# Table of Contents

### Preface .................................................................................................................. 25

### Getting Started

- Alcatel-Lucent 7750 SR-Series
- 7450 ESS-Series
- 7710 SR-Series
- 7950 SR-Series Services Configuration Process ....................................................... 29

### Services Command Reference

#### Services Overview

- Introduction .................................................................................................................. 34
- Service Types ................................................................................................................. 35
- Service Policies ............................................................................................................. 36
- Multipoint Shared Queuing .......................................................................................... 37
- Alcatel-Lucent Service Model ..................................................................................... 42
- Service Entities ............................................................................................................. 43
- Customers ....................................................................................................................... 44
- Service Access Points (SAPs). ..................................................................................... 44
- SAP Encapsulation Types and Identifiers ..................................................................... 46
- Ethernet Encapsulations ................................................................................................. 46
- Default SAP on a Dot1q Port ......................................................................................... 49
- Services and SAP Encapsulations .................................................................................. 50
- SAP Configuration Considerations .............................................................................. 51
- G.8032 Protected Ethernet Rings .................................................................................. 52
- Service Distribution Points (SDPs) ................................................................................ 53
- SDP Binding ................................................................................................................... 54
- Spoke and Mesh SDPs .................................................................................................... 56
- SDP Using BGP Route Tunnel ....................................................................................... 56
- SDP Keepalives ............................................................................................................ 57
- SDP Administrative Groups ......................................................................................... 57
- SDP Selection Rules ....................................................................................................... 59
- SAP & MPLS Binding Loopback with MAC Swap ......................................................... 59
- Class-Based Forwarding ................................................................................................. 65
- Multi-Service Sites ....................................................................................................... 69
- G.8031 Protected Ethernet Tunnels .............................................................................. 70
- OAM Considerations ..................................................................................................... 74
- QoS Considerations ....................................................................................................... 74
- Mirroring and Lawful Intercept Considerations ............................................................ 75
- Support Service and Solution Combinations ............................................................... 75
- LAG Emulation using Ethernet Tunnels ........................................................................ 76
- G.8032 Ethernet Ring Protection Switching ................................................................. 77
- Overview of G.8032 Operation ..................................................................................... 78
- Ethernet Unnumbered Interfaces .................................................................................. 83
- Ethernet Ring Sub-Rings ............................................................................................... 84
  - Virtual and Non-Virtual Channel ............................................................................... 85
  - Lag Support ................................................................................................................ 90
  - OAM Considerations ................................................................................................. 91
# Table of Contents

Support Service and Solution Combinations ......................................................... 91
Internal Objects Created for L2TP and NAT ......................................................... 93
Pseudowire Shaping for Layer 2 and Layer 3 Services ........................................... 94
Service Creation Process Overview ........................................................................ 96
Deploying and Provisioning Services ..................................................................... 97
    Phase 1: Core Network Construction ............................................................... 97
    Phase 2: Service Administration .................................................................... 97
    Phase 3: Service Provisioning . ....................................................................... 97
Configuration Notes ............................................................................................. 98
    General .......................................................................................................... 98
    Configuring Global Service Entities with CLI ................................................ 99
    Service Model Entities ................................................................................... 99
    Basic Configuration ....................................................................................... 101
    Common Configuration Tasks ....................................................................... 103
        Configuring Customers ............................................................................. 103
        Customer Information ............................................................................. 103
        Configuring Multi-Service-Sites .............................................................. 105
        Configuring an SDP .................................................................................. 107
        SDP Configuration Tasks ....................................................................... 107
        Configuring an SDP .................................................................................. 108
        Configuring a Mixed-LSP SDP ................................................................ 110
Ethernet Connectivity Fault Management (ETH-CFM) ........................................... 112
    Facility MEPS ............................................................................................... 116
        Common Actionable Failures .................................................................. 118
        General Detection, Processing and Reaction ........................................... 120
        Port-Based MEP ....................................................................................... 122
        LAG Based MEP ...................................................................................... 130
        Tunnel Based MEP ................................................................................... 138
        Router Interface MEP .............................................................................. 149
        Hardware Support .................................................................................... 152
    ETH-CFM and MC-LAG .................................................................................. 154
        ETH-CFM and MC-LAG Default Behavior .............................................. 154
        Linking ETH-CFM to MC-LAG State ....................................................... 155
    ETH-CFM Features ....................................................................................... 164
        CCM Hold Timers ..................................................................................... 164
        CCM Interval ............................................................................................ 165
        MEP and MIP Support ............................................................................. 166
        Configuring ETH-CFM Parameters ......................................................... 168
    Service Management Tasks ............................................................................. 173
        Modifying Customer Accounts ............................................................... 173
        Deleting Customers ................................................................................. 175
        Modifying SDPs ....................................................................................... 176
        Deleting SDPs .......................................................................................... 177
    Global Services Command Reference .............................................................. 179

VLL Services

    VLL SAP, Pseudowire and SDP Types .............................................................. 282
    ATM VLL (Apipe) Services ............................................................................. 283
    ATM VLL For End-to-End ATM Service ......................................................... 283
    ATM Virtual Trunk Over IP/MPLS Packet-Switched Network ............................ 285
<table>
<thead>
<tr>
<th>Service Type</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet Pipe (Epipe) Services</td>
<td>300</td>
</tr>
<tr>
<td>Epipe Service Overview</td>
<td>301</td>
</tr>
<tr>
<td>Epipe Up Operational State</td>
<td>302</td>
</tr>
<tr>
<td>Epipe with PBB</td>
<td>303</td>
</tr>
<tr>
<td>Epipe over L2TPv3</td>
<td>304</td>
</tr>
<tr>
<td>Ethernet Interworking VLL</td>
<td>305</td>
</tr>
<tr>
<td>VLL CAC</td>
<td>307</td>
</tr>
<tr>
<td>Ethernet Interworking VLL (Ipipe) Services</td>
<td>314</td>
</tr>
<tr>
<td>Ipipe VLL</td>
<td>314</td>
</tr>
<tr>
<td>IP Interworking VLL Datapath</td>
<td>317</td>
</tr>
<tr>
<td>Extension to IP VLL for Discovery of Ethernet CE IP Address</td>
<td>320</td>
</tr>
<tr>
<td>VLL Ethernet SAP Procedures</td>
<td>320</td>
</tr>
<tr>
<td>IPv6 Support on IP Interworking VLL</td>
<td>324</td>
</tr>
<tr>
<td>IPv6 Datapath Operation</td>
<td>324</td>
</tr>
<tr>
<td>IPv6 Stack Capability Signaling</td>
<td>327</td>
</tr>
<tr>
<td>Services Configuration for MPLS-TP</td>
<td>329</td>
</tr>
<tr>
<td>SDPs</td>
<td>329</td>
</tr>
<tr>
<td>VLL Spoke SDP Configuration</td>
<td>330</td>
</tr>
<tr>
<td>Epipe VLL Spoke-SDP Termination on IES, VPRN and VPLS</td>
<td>333</td>
</tr>
<tr>
<td>Pseudowire Switching</td>
<td>335</td>
</tr>
<tr>
<td>Pseudowire Switching with Protection</td>
<td>336</td>
</tr>
<tr>
<td>Pseudowire Switching Behavior</td>
<td>339</td>
</tr>
<tr>
<td>Static-to-Dynamic Pseudowire Switching</td>
<td>341</td>
</tr>
<tr>
<td>Ingress VLAN Swapping</td>
<td>342</td>
</tr>
<tr>
<td>Ingress VLAN Translation</td>
<td>343</td>
</tr>
<tr>
<td>Pseudowire Redundancy</td>
<td>344</td>
</tr>
<tr>
<td>Dynamic Multi-Segment Pseudowire Routing</td>
<td>345</td>
</tr>
<tr>
<td>Overview</td>
<td>345</td>
</tr>
</tbody>
</table>
Table of Contents

- Pseudowire Routing .................................................................................................................. 350
- Configuring VLLs using Dynamic MS-PWs .............................................................................. 353
- Pseudowire Redundancy ............................................................................................................ 356
- VCCV OAM for Dynamic MS-PWs ............................................................................................ 358
- VCCV-Ping on Dynamic MS-PWs ............................................................................................... 358
- VCCV-Trace on Dynamic MS-PWs ............................................................................................. 359
- Example Dynamic MS-PW Configuration ................................................................................... 360
- VLL Resilience with Two Destination PE Nodes ........................................................................ 363
- Master-Slave Operation .............................................................................................................. 365
- Epipe Using BGP-MH Site Support for Ethernet Tunnels ............................................................ 373
- Operational Overview ................................................................................................................ 375
- Detailed Operation ...................................................................................................................... 376
- BGP-MH Site Support for Ethernet Tunnels Operational-Group Model ................................... 380
- BGP-MH Specifics for MH Site Support for Ethernet Tunnels .................................................... 380
- PW Redundancy for BGP MH Site Support for Ethernet Tunnels ............................................ 380
- T-LDP Status Notification Handling Rules of BGP-MH Epipes ................................................. 381
- Access Node Resilience Using MC-LAG and Pseudowire Redundancy ..................................... 392
- VLL Resilience for a Switched Pseudowire Path ....................................................................... 394
- Pseudowire Redundancy Service Models .................................................................................... 397
- Redundant VLL Service Model .................................................................................................. 397
- VLL Endpoint Active Transmit Object Selection Rules ............................................................... 399
- T-LDP Status Notification Handling Rules ................................................................................ 401
- Processing Endpoint SAP Active/Standby Status Bits ................................................................. 401
- Processing and Merging ............................................................................................................. 401
- High-Speed Downlink Packet Access (HSDPA) Off Load Fallback over ATM ............................ 403
- Primary Spoke-SDP Fallback to Secondary SAP ......................................................................... 404
- Reversion to Primary Spoke SDP Path ......................................................................................... 404
- MC-APS and MC-LAG ............................................................................................................... 405
- Failure Scenarios ....................................................................................................................... 407
- VLL Using G.8031 Protected Ethernet Tunnels ......................................................................... 408
- BGP Virtual Private Wire Service (VPWS) ................................................................................ 409
- Single-Homed BGP VPWS ........................................................................................................ 409
- Dual-Homed BGP VPWS ........................................................................................................... 410
- VLL Service Considerations ....................................................................................................... 420
- SDPs ........................................................................................................................................ 420
- SDP Statistics for VPLS and VLL Services .................................................................................. 421
- SAP Encapsulations and Pseudowire Types .............................................................................. 422
- PWE3 N-to-1 Cell Mode ............................................................................................................. 423
- PWE3 AAL5 SDU Mode .............................................................................................................. 423
- PWE3 N-to-1 Cell Mode ............................................................................................................. 425
- PWE3 AAL5 SDU Mode .............................................................................................................. 425
- QoS Policies ............................................................................................................................... 426
- Filter Policies ............................................................................................................................. 426
- MAC Resources ......................................................................................................................... 426
- Configuring a VLL Service with CLI .......................................................................................... 427
- Basic Configurations .................................................................................................................. 429
- Common Configuration Tasks ..................................................................................................... 429
- Configuring VLL Components .................................................................................................... 430
- Creating an Apipe Service .......................................................................................................... 430
- Creating a Cpipe Service ............................................................................................................. 439
# Table of Contents

- EVPN for VXLAN in R-VPLS Services .............................................. 704
- Interaction of EVPN and VXLAN with Existing VPLS Features ................. 706
- Configuring a EVPN Service with CLI .......................................... 707
- EVPN Configuration Examples .................................................... 708
- EVPN Command Reference ....................................................... 711

## Virtual Private LAN Service

- VPLS Service Overview .......................................................... 727
- VPLS Packet Walkthrough ...................................................... 728
- VPLS Features ......................................................................... 731
- VPLS Enhancements .............................................................. 731
- VPLS over MPLS ....................................................................... 732
- VPLS MAC Learning and Packet Forwarding .................................. 733
  - MAC Learning Protection ..................................................... 733
  - DEI in IEEE 802.1ad .......................................................... 736
- VPLS Using G.8031 Protected Ethernet Tunnels .............................. 737
- Pseudowire Control Word ........................................................ 738
- Table Management .................................................................... 739
  - FIB Size ............................................................................. 739
  - FIB Size Alarms .................................................................... 739
  - Local and Remote Aging Timers ............................................. 740
  - Disable MAC Aging .......................................................... 740
  - Disable MAC Learning ........................................................ 740
  - Unknown MAC Discard ..................................................... 740
  - VPLS and Rate Limiting ..................................................... 741
  - MAC Move .......................................................................... 741
  - Auto-Learn MAC Protect ..................................................... 742
- Split Horizon SAP Groups and Split Horizon Spoke SDP Groups ............. 747
- VPLS and Spanning Tree Protocol ............................................. 748
  - Spanning Tree Operating Modes ........................................... 748
  - Multiple Spanning Tree ....................................................... 750
  - MSTP for QinQ SAPs .......................................................... 752
  - Provider MSTP .................................................................... 752
  - Enhancements to the Spanning Tree Protocol .............................. 754
- Egress Multicast Groups ............................................................ 757
- Egress Multicast Group Provisioning ............................................ 757
- VPLS Redundancy ...................................................................... 769
  - Spoke SDP Redundancy for Metro Interconnection ....................... 769
  - Spoke SDP Based Redundant Access ....................................... 771
  - Inter-Domain VPLS Resiliency Using Multi-Chassis Endpoints ....... 772
  - Support for Single Chassis Endpoint Mechanisms ....................... 776
  - Using B-VPLS for Increased Scalability and Reduced Convergence Times ........................................................................... 780
  - MAC Flush Additions for PBB VPLS ....................................... 782
- VPLS Access Redundancy .......................................................... 785
  - STP-Based Redundant Access to VPLS .................................... 785
  - Redundant Access to VPLS Without STP ................................... 786
- Object Grouping and State Monitoring ....................................... 787
  - VPLS Applicability — Block on VPLS a Failure ......................... 787
- MAC Flush Message Processing ................................................. 789
- Dual Homing to a VPLS Service ................................................ 791
### Table of Contents

- MC-Ring and VPLS .......................................................... 792
- ACL Next-Hop for VPLS ................................................ 793
- SDP Statistics for VPLS and VLL Services ......................... 794
- RADIUS Auto-Discovery (feature deprecated) .................... 795
  - Auto SDPs and Auto SDP Bindings ................................ 795
  - Manual SDPs and Manual SDP Bindings ......................... 795
- BGP Auto-Discovery for LDP VPLS .................................. 798
  - BGP AD Overview ....................................................... 798
  - Information Model .................................................... 798
  - FEC Element for T-LDP Signaling ................................ 800
  - BGP-AD and Target LDP (T-LDP) Interaction .................... 801
  - SDP Usage ............................................................... 803
  - Automatic Creation of SDPs ....................................... 803
  - Manually Provisioned SDP .......................................... 803
  - Automatic Instantiation of Pseudowires (SDP Bindings) .... 804
  - Mixing Statically Configured and Auto-Discovered Pseudowires in a VPLS ........................ 805
  - Resiliency Schemes .................................................. 805
- BGP VPLS ................................................................. 806
  - Pseudowire Signaling Details ..................................... 807
  - Supported VPLS Features .......................................... 809
  - BGP VPLS Configuration Procedure ............................... 810
- BGP Multi-Homing for VPLS ......................................... 813
  - Information Model and Required Extensions to L2VPN NLRI . 814
  - Supported Services and Multi-Homing Objects ................ 815
  - Blackhole Avoidance ................................................ 816
  - BGP Multi-Homing for VPLS Inter-Domain Resiliency .......... 817
- Multicast-Aware VPLS .................................................. 818
  - PIM Snooping for VPLS .............................................. 818
  - Multicast Listener Discovery (MLD) Snooping and MAC-Based Multicast Forwarding ............. 820
  - PIM and IGMP Snooping Interaction ............................... 821
  - VPLS Multicast-Aware High Availability Features ........... 821
- RSVP and LDP P2MP LSP for Forwarding VPLS/B-VPLS BUM and IP Multicast Packets .................. 822
- Routed VPLS and I-VPLS .............................................. 824
  - IES or VPRN IP Interface Binding ................................. 824
  - Assigning a Service Name to a VPLS Service .................. 824
  - Service Binding Requirements .................................... 825
  - Bound Service Name Assignment .................................. 825
  - Binding a Service Name to an IP Interface ...................... 825
  - Bound Service Deletion or Service Name Removal .............. 826
  - IP Interface Attached VPLS Service Constraints .............. 826
  - IP Interface and VPLS Operational State Coordination ....... 827
- IP Interface MTU and Fragmentation ................................ 828
- Unicast IP Routing into a VPLS Service ........................... 828
- ARP and VPLS FIB Interactions ..................................... 829
  - Routed VPLS Specific ARP Cache Behavior ...................... 830
  - The allow-ip-int-binding VPLS Flag ............................... 831
  - Routed VPLS SAPs Only Supported on Standard Ethernet Ports .......... 831
  - Routed VPLS SAPs Only Supported on FP2 (or later) Based Systems or IOM/IMM .................. 831
  - Network Ports Restricted to FP2-Based Systems or IOMs ...... 831
  - LAG Port Membership Constraints ................................. 832
**Table of Contents**

- Routed VPLS Feature Restrictions .......................................................... 833
- Routed I-VPLS Feature Restrictions .......................................................... 833
- IES IP Interface VPLS Binding and Chassis Mode Interaction ......................... 834
- VPRN IP Interface VPLS Binding and Forwarding Plane Constraints ................. 834
- Route Leaking Between Routing Contexts .................................................. 834
- Ingress LAG and FP1 to Routed VPLS Discards ......................................... 835
- IPv4 Multicast Routing Support ............................................................... 836
- BGP Auto Discovery (BGP-AD) for Routed VPLS Support ............................. 837
- Routed VPLS Caveats ................................................................................. 838
  - VPLS SAP Ingress IP Filter Override .................................................... 838
  - IP Interface Defined Egress QoS Reclassification ................................. 838
  - VPLS Egress Remarking and Egress Routed Packets ............................. 839
  - 7450 Mixed Mode Chassis ..................................................................... 839
  - IPv4 Multicast Routing ......................................................................... 839
  - Routed VPLS Supported Routing Related Protocols .................................. 839
  - Spanning Tree and Split Horizon ......................................................... 840
- VPLS Service Considerations ..................................................................... 841
  - SAP Encapsulations ............................................................................... 841
  - VLAN Processing .................................................................................... 841
- Ingress VLAN Swapping ............................................................................. 842
  - Service Auto-Discovery using Multiple VLAN Registration Protocol (MVRP) ........................................................................ 843
  - Configure the MVRP Infrastructure using an M-VPLS Context .............. 844
  - Instantiate Related VLAN FIBs and Trunks in MVRP Scope ................. 844
  - MVRP Activation of Service Connectivity .......................................... 847
  - MVRP Control Plane .............................................................................. 850
  - STP-MVRP Interaction .......................................................................... 850
- Configuring a VPLS Service with CLI .......................................................... 853
  - Basic Configuration ............................................................................... 854
  - Common Configuration Tasks .................................................................. 856
- Configuring VPLS Components .................................................................... 857
  - Configuring Egress Multicast Groups .................................................... 858
  - Creating a VPLS Service ........................................................................ 859
  - Enabling Multiple MAC Registration Protocol (MMRP) ....................... 860
  - Configuring GSMP Parameters .............................................................. 869
  - Configuring a VPLS SAP ....................................................................... 870
  - Applying an Egress Multicast Group to a VPLS Service SAP ............... 882
  - Configuring SAP Subscriber Management Parameters ..................... 883
  - MSTP Control over Ethernet Tunnels .................................................... 884
  - Configuring SDP Bindings ..................................................................... 885
  - Configuring Overrides on Service SAPs ............................................... 886
- Configuring VPLS Redundancy ................................................................... 898
  - Creating a Management VPLS for SAP Protection ............................... 898
  - Creating a Management VPLS for Spoke SDP Protection .................... 901
  - Configuring Load Balancing with Management VPLS ....................... 904
  - Configuring Selective MAC Flush ......................................................... 909
  - Configuring Multi-Chassis Endpoints .................................................. 910
- ATM/Frame Relay PVC Access and Termination on a VPLS Service .......... 914
- Configuring BGP Auto-Discovery ............................................................... 916
  - Configuration Steps ............................................................................... 916
  - LDP Signaling ....................................................................................... 919
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>PBB and BGP-AD</td>
<td>1230</td>
</tr>
<tr>
<td>PBB ELINE Service</td>
<td>1230</td>
</tr>
<tr>
<td>Non-Redundant PBB Epipe Spoke Termination</td>
<td>1230</td>
</tr>
<tr>
<td>PBB Using G.8031-Protected Ethernet Tunnels</td>
<td>1231</td>
</tr>
<tr>
<td>Solution Overview</td>
<td>1231</td>
</tr>
<tr>
<td>Detailed Solution Description</td>
<td>1233</td>
</tr>
<tr>
<td>Detailed PBB Emulated LAG Solution Description</td>
<td>1236</td>
</tr>
<tr>
<td>Support Service and Solution Combinations</td>
<td>1238</td>
</tr>
<tr>
<td>Periodic MAC Notification</td>
<td>1239</td>
</tr>
<tr>
<td>MAC Flush</td>
<td>1240</td>
</tr>
<tr>
<td>PBB Resiliency for B-VPLS Over Pseudowire Infrastructure</td>
<td>1240</td>
</tr>
<tr>
<td>Extensions for PBB VPLS</td>
<td>1245</td>
</tr>
<tr>
<td>TCN Event</td>
<td>1245</td>
</tr>
<tr>
<td>PBB Blackholing</td>
<td>1247</td>
</tr>
<tr>
<td>Access Multi-Homing for Native PBB (B-VPLS over SAP Infrastructure)</td>
<td>1250</td>
</tr>
<tr>
<td>Solution Description for I-VPLS Over Native PBB Core</td>
<td>1251</td>
</tr>
<tr>
<td>Solution Description for PBB Epipe over G.8031 Ethernet Tunnels</td>
<td>1255</td>
</tr>
<tr>
<td>BGP Multi-homing for I-VPLS</td>
<td>1259</td>
</tr>
<tr>
<td>Access Multi-Homing over MPLS for PBB Epipe</td>
<td>1260</td>
</tr>
<tr>
<td>PBB and IGMP Snooping</td>
<td>1263</td>
</tr>
<tr>
<td>PBB QoS</td>
<td>1264</td>
</tr>
<tr>
<td>Transparency of Customer QoS Indication through PBB Backbone</td>
<td>1265</td>
</tr>
<tr>
<td>Egress B-SAP per ISID Shaping</td>
<td>1271</td>
</tr>
<tr>
<td>B-SAP Egress ISID Shaping Configuration</td>
<td>1271</td>
</tr>
<tr>
<td>Provisioning Model</td>
<td>1273</td>
</tr>
<tr>
<td>Egress Queue Scheduling</td>
<td>1275</td>
</tr>
<tr>
<td>B-SAP per-ISID Shaping Configuration Example</td>
<td>1277</td>
</tr>
<tr>
<td>PBB OAM</td>
<td>1280</td>
</tr>
<tr>
<td>Mirroring</td>
<td>1281</td>
</tr>
<tr>
<td>OAM Commands</td>
<td>1281</td>
</tr>
<tr>
<td>CFM Support</td>
<td>1281</td>
</tr>
<tr>
<td>Configuration Examples</td>
<td>1282</td>
</tr>
<tr>
<td>PBB ELAN and ELINE</td>
<td>1282</td>
</tr>
<tr>
<td>PBB ELAN with MMRP - M:1 model</td>
<td>1283</td>
</tr>
<tr>
<td>PBB using G.8031 Protected Ethernet Tunnels</td>
<td>1283</td>
</tr>
<tr>
<td>PBB MAC Flush</td>
<td>1286</td>
</tr>
<tr>
<td>MC-LAG Multihoming for Native PBB</td>
<td>1287</td>
</tr>
<tr>
<td>Access Multi-Homing over MPLS for PBB Epipe</td>
<td>1289</td>
</tr>
<tr>
<td>ETH-CFM Configuration on MTU1</td>
<td>1291</td>
</tr>
<tr>
<td>ETH-CFM Configuration on AG1</td>
<td>1292</td>
</tr>
<tr>
<td>Ethernet Virtual Private Networks (EVPN)</td>
<td>1293</td>
</tr>
<tr>
<td>EVPN for VXLAN Tunnels in a Layer-2 DC GW</td>
<td>1294</td>
</tr>
<tr>
<td>EVPN for VXLAN tunnels in a Layer-2 DC with Integrated Routing Bridging Connectivity on the DC GW</td>
<td>1295</td>
</tr>
<tr>
<td>VXLAN</td>
<td>1296</td>
</tr>
<tr>
<td>VXLAN ECMP and LAG</td>
<td>1298</td>
</tr>
<tr>
<td>VXLAN VPLS Tag Handling</td>
<td>1299</td>
</tr>
<tr>
<td>VXLAN MTU Considerations</td>
<td>1299</td>
</tr>
<tr>
<td>VXLAN QoS</td>
<td>1299</td>
</tr>
<tr>
<td>BGP-EVPN Control Plane for VXLAN Overlay Tunnels</td>
<td>1301</td>
</tr>
</tbody>
</table>
# Internet Enhanced Service

IES Service Overview ................................................. 1348
IES Features .......................................................... 1349
IP Interfaces ........................................................... 1349
QoS Policy Propagation Using BGP (QPPB) ....................... 1350
QPPB ................................................................. 1353
QPPB and GRT Lookup .............................................. 1358
Object Grouping and State Monitoring .......................... 1361
Subscriber Interfaces ............................................... 1363
IPv6 Enhanced Subscriber Management (ESM) ................. 1363
RADIUS Accounting .................................................. 1364
SAPs ................................................................. 1367
Encapsulations ...................................................... 1367
ATM SAP Encapsulations for IES ................................. 1367
Pseudowire SAPs .................................................... 1368
Encapsulation ....................................................... 1369
Pseudowire SAP Configuration ................................... 1370
QoS for Pseudowire Ports and Pseudowire SAPs .............. 1371
Shaping and Bandwidth Control ................................. 1372
Last Mile Packet Size Adjustment .............................. 1373
Redundancy with Pseudowire SAPs ............................... 1374
Routing Protocols .................................................... 1376
CPE Connectivity Check ............................................ 1376
QoS Policies ........................................................ 1377
Filter Policies ....................................................... 1377
Spoke SDPs .......................................................... 1378
SRRP ................................................................. 1380
SRRP Messaging ..................................................... 1386
SRRP and Multi-Chassis Synchronization ....................... 1388
SRRP Instance ....................................................... 1389
Subscriber Subnet Owned IP Address Connectivity .......... 1392
Subscriber Subnet SRRP Gateway IP Address Connectivity .. 1392
Receive SRRP Advertisement SAP and Anti-Spoof ............ 1392
BFD with SRRP/VRRP ............................................... 1392
Configuring an IES Service with CLI ......................... 1393
Basic Configuration ................................................ 1394
Common Configuration Tasks ................................. 1395
Configuring IES Components ................................... 1396
Configuring an IES Service ..................................... 1396

## EVPN for VXLAN in VPLS Services

- Resiliency and BGP Multi-Homing ................................ 1306
- Use of bgp-evpn, bgp-ad, and Sites in the Same VPLS Service .................................................. 1306
- Use of the unknown-mac-route ................................ 1308
- Proxy-ARP Table .................................................. 1309
- BGP-EVPN MAC-Mobility ........................................ 1309
- Conditional Static MAC and Protection ........................ 1311

## EVPN for VXLAN in R-VPLS Services

- Interaction of EVPN and VXLAN with Existing VPLS Features .................................................. 1315
- Conditional Static MAC and Protection ........................ 1311

## IP Interfaces

- Use of the unknown-mac-route ................................ 1308
- Proxy-ARP Table .................................................. 1309
- BGP-EVPN MAC-Mobility ........................................ 1309
- Conditional Static MAC and Protection ........................ 1311

## SRRP

- Subscriber Subnet SRRP Gateway IP Address Connectivity .......... 1392
- Subscriber Subnet Owned IP Address Connectivity ............ 1392

## Filter Policies

- Subscriber Subnet Owned IP Address Connectivity ............ 1392
- BFD with SRRP/VRRP ............................................... 1392

## QoS Policies

- Subscriber Subnet Owned IP Address Connectivity ............ 1392
- BFD with SRRP/VRRP ............................................... 1392

## Configuring an IES Service with CLI

- Basic Configuration ................................................ 1394
- Common Configuration Tasks ................................. 1395
- Configuring IES Components ................................... 1396
- Configuring an IES Service ..................................... 1396
# Table of Contents

## Virtual Private Routed Network Service

**VPRN Service Overview** .................................................. 1607
Routing Prerequisites ...................................................... 1609
Core MP-BGP Support ...................................................... 1610
Route Distinguishers ....................................................... 1611
eiBGP Load Balancing ..................................................... 1611
Route Reflector ............................................................... 1614
CE to PE Route Exchange .................................................. 1615
Constrained Route Distribution (RT Constraint) ................. 1618
Constrained VPN Route Distribution Based on Route Targets.. 1618
Configuring the Route Target Address Family .................... 1618
Originating RT Constraint Routes .................................... 1618
Receiving and Re-Advertising RT Constraint Routes ........... 1619
Using RT Constraint Routes ............................................. 1620
BGP Fast Reroute in a VPRN .............................................. 1623
BGP Fast Reroute in a VPRN Configuration .......................... 1624
**VPRN Features** ............................................................ 1625
**IP Interfaces** ............................................................... 1625
QoS Policy Propagation Using BGP (QPPB) ......................... 1626
QPPB ............................................................... 1628
QPPB and GRT Lookup ................................................... 1633
Object Grouping and State Monitoring .............................. 1636
VPRN IP Interface Applicability ....................................... 1636
Subscriber Interfaces ...................................................... 1638
SAPs ............................................................... 1639
Encapsulations .............................................................. 1639
ATM SAP Encapsulations for VPRN Services ....................... 1639
QoS Policies ............................................................... 1640
Filter Policies ............................................................. 1640
DSCP Marking .............................................................. 1641
Default DSCP Mapping Table ........................................... 1643
CE to PE Routing Protocols .............................................. 1644
PE to PE Tunneling Mechanisms ....................................... 1644
Per VRF Route Limiting .................................................. 1644
Table of Contents

Spoke SDPs .......................................................... 1645
T-LDP Status Signaling for Spoke-SDPs Terminating on IES/VPRN ................. 1646
Spoke SDP Redundancy into IES/VPRN ................................ 1647
IP-VPNs .............................................................. 1648
    Using OSPF in IP-VPNs ........................................... 1648
IPCP Subnet Negotiation ............................................ 1649
Cflowd for IP-VPNs ................................................... 1650
Inter-AS VPRNs ....................................................... 1651
Carrier Supporting Carrier (CsC) .................................... 1654
    Terminology ......................................................... 1654
    CSC Connectivity Models ........................................ 1656
    CSC-PE Configuration and Operation ......................... 1657
Traffic Leaking to GRT ............................................... 1661
Traffic Leaking from VPRN to GRT for IPv6 ................................ 1662
RIP Metric Propagation in VPRNs .................................... 1663
NTP Within a VPRN Service ........................................ 1664
PTP Within a VPRN Service .......................................... 1664
Service Label Mode of a VPRN ...................................... 1665
    Configuring the Service Label Mode ............................ 1666
    Restrictions and Usage Notes .................................... 1667
Multicast in IP-VPN Applications .................................... 1668
    Use of Data MDTs .................................................. 1670
    Multicast Protocols Supported in the Provider Network ...... 1671
    Provider Tunnel Support ......................................... 1675
    MVPN Sender-only/Receiver-only ............................... 1679
    Multicast VPN Extranel .......................................... 1681
Non-Congruent Unicast and Multicast Topologies for Multicast VPN. .............. 1683
Multicast Auto RP Discovery ........................................ 1683
IPv6 MVPN Support .................................................. 1684
NG-MVPN Multicast Source Geo-Redundancy ................................ 1686
    Multicast Core Diversity for Rosen MDT_SAFI MVPNs ....... 1689
    Inter-AS MVPN ...................................................... 1691
VPRN Off-Ramp ....................................................... 1695
    DDoS Off-Ramping Through Flowspec ................................ 1696
Configuring a VPRN Service with CLI ................................ 1697
    Basic Configuration .............................................. 1698
    Common Configuration Tasks ..................................... 1700
Configuring VPRN Components ....................................... 1701
    Creating a VPRN Service ......................................... 1701
    Configuring Global VPRN Parameters .......................... 1702
    Configuring VPRN Protocols - PIM ............................. 1704
Configuring IPsec Parameters ....................................... 1720
Service Management Tasks .......................................... 1721
    Modifying VPRN Service Parameters ............................ 1721
    Deleting a VPRN Service ........................................ 1722
    Disabling a VPRN Service ........................................ 1723
    Re-enabling a VPRN Service ..................................... 1724
VPRN Services Command Reference .................................. 1725
    Common Service Commands ...................................... 2618
Table of Contents

Index ........................................................................................................................................... 2631
List of Figures

Services Overview
Figure 1: Unicast Service Queue Mapping to Multiple Destination Based Hardware Queues ........... 38
Figure 2: Unicast Service Queuing With Shared Queuing Enabled ............................................. 39
Figure 3: Multipoint Queue Behavior with Shared Queuing Enabled ........................................... 40
Figure 4: Multipoint Shared Queuing Using First Pass Unicast Queues ...................................... 41
Figure 5: Service Entities ........................................................................................................... 43
Figure 6: Service Access Point (SAP) ......................................................................................... 44
Figure 7: Service Access Point (SAP) ......................................................................................... 45
Figure 8: Multiple SAPs on a Single Port/Channel ....................................................................... 47
Figure 9: Multiple SAPs on a Single Port .................................................................................... 47
Figure 10: Multiple SAPs on a Single Port/Channel ................................................................... 48
Figure 11: GRE Service Distribution Point (SDP) Pointing from ALA-A to ALA-B ....................... 54
Figure 12: GRE Service Distribution Point (SDP) Pointing From ALA-A to ALA-B ....................... 55
Figure 13: GRE Service Distribution Point (SDP) Pointing from ALA-A to ALA-B ....................... 55
Figure 14: Ingress Loopback ....................................................................................................... 60
Figure 15: Egress Loopback ......................................................................................................... 61
Figure 16: Active Loopback Mode ............................................................................................... 63
Figure 17: Class-Based Forwarding over SDP LSPs ...................................................................... 66
Figure 18: Ethernet Protected Ethernet Tunnel Example ............................................................... 71
Figure 19: PBB G.8031 Protected Ethernet Tunnel Example ....................................................... 71
Figure 20: PBB Fate-Independent Ethernet Tunnels ....................................................................... 73
Figure 21: PBB Fate Sharing Ethernet Tunnels ............................................................................ 73
Figure 22: 0-1 G.8032 Ring in the Initial State ............................................................................... 78
Figure 23: 0-1 G.8032 Ring in the Protecting State ......................................................................... 79
Figure 24: 0-3 Ring Example ....................................................................................................... 81
Figure 25: 0-4 G.8032 Sub-Ring .................................................................................................... 84
Figure 26: 0-5 Sub-Ring Configuration Example ............................................................................ 85
Figure 27: 0-6 Sub-Ring Homed to VPLS .................................................................................... 88
Figure 28: 0-7 Multi Ring Hierarchy ............................................................................................. 90
Figure 29: Service Creation and Implementation Flow ................................................................. 96
Figure 30: Ethernet OAM Model for Broadband Access - Residential ......................................... 114
Figure 31: Ethernet OAM Model for Broadband Access - Wholesale ......................................... 114
Figure 32: Fault Handling Non-Member Port ............................................................................... 124
Figure 33: Port-Based MEP Example ......................................................................................... 125
Figure 34: Fault Handling LAG MEP ......................................................................................... 131
Figure 35: LAG MEP Example .................................................................................................... 132
Figure 36: Tunnel Concepts and Encapsulation .......................................................................... 140
Figure 37: Tunnel MEP Example ............................................................................................... 142
Figure 38: Router MEP Example ............................................................................................... 149
Figure 39: Independent Processing UP MEP Example ............................................................... 154
Figure 40: Independent Processing Down MEP Example ............................................................ 155
Figure 41: ETH-CFM and MC-LAG Example .............................................................................. 158

VLL Services
Figure 42: ATM VLL for End-to-End ATM Service .................................................................... 284
<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>43</td>
<td>VT Application Example</td>
</tr>
<tr>
<td>44</td>
<td>Mobile Infrastructure</td>
</tr>
<tr>
<td>45</td>
<td>RFC 4553 (SAToP) MPLS PSN Encapsulation</td>
</tr>
<tr>
<td>46</td>
<td>CESoPSN Packet Format for an MPLS PSN</td>
</tr>
<tr>
<td>47</td>
<td>MEF8 PSN Encapsulation</td>
</tr>
<tr>
<td>48</td>
<td>CESoPSN MPLS Encapsulation</td>
</tr>
<tr>
<td>49</td>
<td>Epine/VLL Service</td>
</tr>
<tr>
<td>50</td>
<td>L2TPv3 SDP Illustration</td>
</tr>
<tr>
<td>51</td>
<td>Application of Ethernet Interworking VLL Example</td>
</tr>
<tr>
<td>52</td>
<td>MC-Ring in a Combination with VLL Service</td>
</tr>
<tr>
<td>53</td>
<td>Application of a Frame Relay VLL Example</td>
</tr>
<tr>
<td>54</td>
<td>Frame Relay-to-ATM Network Interworking (FRF.5) VLL</td>
</tr>
<tr>
<td>55</td>
<td>IP Interworking VLL (Ipipe)</td>
</tr>
<tr>
<td>56</td>
<td>IP Interworking VLL (Ipipes)</td>
</tr>
<tr>
<td>57</td>
<td>IP Interworking VLL Datapath</td>
</tr>
<tr>
<td>58</td>
<td>IP Interworking VLL Datapath</td>
</tr>
<tr>
<td>59</td>
<td>IP Interworking VLL Datapath</td>
</tr>
<tr>
<td>60</td>
<td>Data Path for Ethernet CE to PPP Attached CE</td>
</tr>
<tr>
<td>61</td>
<td>Pseudowire Service Switching Node</td>
</tr>
<tr>
<td>62</td>
<td>VLL Resilience with Pseudowire Redundancy and Switching</td>
</tr>
<tr>
<td>63</td>
<td>Ingress VLAN Swapping</td>
</tr>
<tr>
<td>64</td>
<td>Ingress VLAN Translation</td>
</tr>
<tr>
<td>65</td>
<td>Dynamic MS-PW Overview</td>
</tr>
<tr>
<td>66</td>
<td>Figure 2 MS-PW Addressing using FEC129 Type 2</td>
</tr>
<tr>
<td>67</td>
<td>Advertisement of PE Addresses by PW Routing</td>
</tr>
<tr>
<td>68</td>
<td>Signaling of Dynamic MS-PWs using T-LDP</td>
</tr>
<tr>
<td>69</td>
<td>Mapping of All to SAP</td>
</tr>
<tr>
<td>70</td>
<td>VLL Using Dynamic MS-PWs, Inter-AS Scenario</td>
</tr>
<tr>
<td>71</td>
<td>Pseudowire Redundancy</td>
</tr>
<tr>
<td>72</td>
<td>Dynamic MS-PW Example</td>
</tr>
<tr>
<td>73</td>
<td>VLL Resilience</td>
</tr>
<tr>
<td>74</td>
<td>Master-Slave Pseudowire Redundancy</td>
</tr>
<tr>
<td>75</td>
<td>Example of SAP OAM Interaction with Master-Slave Pseudowire Redundancy</td>
</tr>
<tr>
<td>76</td>
<td>VLL Resilience</td>
</tr>
<tr>
<td>77</td>
<td>VLL Resilience with Pseudowire Switching</td>
</tr>
<tr>
<td>78</td>
<td>BGP-MH Site Support for Ethernet Tunnels</td>
</tr>
<tr>
<td>79</td>
<td>G.8031 for Slave Operation</td>
</tr>
<tr>
<td>80</td>
<td>Full Redundancy G.8031 Epine &amp; BGP-MH</td>
</tr>
<tr>
<td>81</td>
<td>Sample Topology Full Redundancy</td>
</tr>
<tr>
<td>82</td>
<td>Access Node Resilience</td>
</tr>
<tr>
<td>83</td>
<td>VLL Resilience with Pseudowire Redundancy and Switching</td>
</tr>
<tr>
<td>84</td>
<td>Redundant VLL Endpoint Objects</td>
</tr>
<tr>
<td>85</td>
<td>HSDPA Off Load Fallback over ATM</td>
</tr>
<tr>
<td>86</td>
<td>HSDPA Off Load Fallback with MC-APS</td>
</tr>
<tr>
<td>87</td>
<td>Ethernet Failure At Cell Site</td>
</tr>
<tr>
<td>88</td>
<td>Single-Homed BGP-VPWS Example</td>
</tr>
<tr>
<td>89</td>
<td>Dual-Homed BGP VPWS with Single Pseudowire</td>
</tr>
<tr>
<td>90</td>
<td>Dual-homed BGP VPWS with Active/Standby Pseudowires</td>
</tr>
<tr>
<td>91</td>
<td>BGP VPWS Update Extended Community Format</td>
</tr>
<tr>
<td>Figure</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>92</td>
<td>BGP VPWS NLRI</td>
</tr>
<tr>
<td>93</td>
<td>BGP VPWS NLRI TLV Extension Format</td>
</tr>
<tr>
<td>94</td>
<td>Circuit Status Vector TLV Type</td>
</tr>
<tr>
<td>95</td>
<td>SDP Statistics for VPLS and VLL Services</td>
</tr>
<tr>
<td>96</td>
<td>SDPs — Uni-Directional Tunnels</td>
</tr>
<tr>
<td>97</td>
<td>VLL Resilience with Pseudowire Redundancy and Switching</td>
</tr>
<tr>
<td>98</td>
<td>VLL Resilience with Pseudowire Redundancy and Switching</td>
</tr>
<tr>
<td>99</td>
<td>VLL Resilience</td>
</tr>
<tr>
<td>100</td>
<td>VLL Resilience with Pseudowire Switching</td>
</tr>
<tr>
<td>101</td>
<td>Single-Homed BGP VPWS Configuration Example</td>
</tr>
<tr>
<td>102</td>
<td>Example of Dual-Homed BGP VPWS with Single Pseudowire</td>
</tr>
<tr>
<td>103</td>
<td>Example of Dual-homed BGP VPWS with Active/Standby Pseudowires</td>
</tr>
<tr>
<td>104</td>
<td>Layer-2 DC PE with VPLS to the WAN</td>
</tr>
<tr>
<td>105</td>
<td>GW IRB on the DC PE for an L2 EVPN/VXLAN DC</td>
</tr>
<tr>
<td>106</td>
<td>VXLAN Frame Format</td>
</tr>
<tr>
<td>107</td>
<td>EVPN-VXLAN Required Routes and Communities</td>
</tr>
<tr>
<td>108</td>
<td>VPLS Service Architecture</td>
</tr>
<tr>
<td>109</td>
<td>Access Port Ingress Packet Format and Lookup</td>
</tr>
<tr>
<td>110</td>
<td>Network Port Egress Packet Format and Flooding</td>
</tr>
<tr>
<td>111</td>
<td>Access Port Egress Packet Format and Lookup</td>
</tr>
<tr>
<td>112</td>
<td>MAC Learning Protection</td>
</tr>
<tr>
<td>113</td>
<td>DE Bit in the 802.1ad S-TAG</td>
</tr>
<tr>
<td>114</td>
<td>Auto-Learn-Mac-Protect Operation</td>
</tr>
<tr>
<td>115</td>
<td>Auto-Learn-Mac-Protect Example</td>
</tr>
<tr>
<td>116</td>
<td>Access Resiliency</td>
</tr>
<tr>
<td>117</td>
<td>HVPLS with Spoke Redundancy</td>
</tr>
<tr>
<td>118</td>
<td>HVPLS Resiliency Based on AS Pseudowires</td>
</tr>
<tr>
<td>119</td>
<td>Multi-Chassis Pseudowire Endpoint for VPLS</td>
</tr>
<tr>
<td>120</td>
<td>MC-EP in Passive Mode</td>
</tr>
<tr>
<td>121</td>
<td>MAC Flush in the MC-EP Solution</td>
</tr>
<tr>
<td>122</td>
<td>MC-EP with B-VPLS</td>
</tr>
<tr>
<td>123</td>
<td>MC-EP with B-VPLS Failure Scenario</td>
</tr>
<tr>
<td>124</td>
<td>MC-EP with B-VPLS Mac Flush Solution</td>
</tr>
<tr>
<td>125</td>
<td>Dual Homed MTU-s in Two-Tier Hierarchy H-VPLS</td>
</tr>
<tr>
<td>126</td>
<td>Dual Homed CE Connection to VPLS</td>
</tr>
<tr>
<td>127</td>
<td>Application 1 Diagram</td>
</tr>
<tr>
<td>128</td>
<td>SDP Statistics for VPLS and VLL Services</td>
</tr>
<tr>
<td>129</td>
<td>BGP AD NLRI versus IP VPN NLRI</td>
</tr>
<tr>
<td>130</td>
<td>Generalized Pseudowire-ID FEC Element</td>
</tr>
<tr>
<td>131</td>
<td>BGP-AD and T-LDP Interaction</td>
</tr>
<tr>
<td>132</td>
<td>BGP VPLS Solution</td>
</tr>
<tr>
<td>133</td>
<td>BGP Multi-Homing for VPLS</td>
</tr>
<tr>
<td>134</td>
<td>BGP MH-NLRI for VPLS Multi-Homing</td>
</tr>
<tr>
<td>135</td>
<td>BGP MH Used in an HVPLS Topology</td>
</tr>
<tr>
<td>136</td>
<td>IPv4 Multicast with a Router VPLS service</td>
</tr>
</tbody>
</table>
List of Figures

Figure 137: Ingress VLAN Swapping ............................................................... 842
Figure 138: Infrastructure for MVRP Exchanges ........................................... 843
Figure 139: Service Instantiation with MVRP - QinQ to PBB Example ................. 847
Figure 140: SDPs — Uni-Directional Tunnels ................................................ 887
Figure 141: Example Configuration for Protected VPLS SAP ........................ 899
Figure 142: Example Configuration for Protected VPLS Spoke SDP ................... 902
Figure 143: Example Configuration for Load Balancing Across Two Protected VPLS Spoke SDPs 904
Figure 144: ATM/Frame Relay PVC Access and Termination on a VPLS Example 914
Figure 145: ATM/Frame Relay PVC Access and Termination on a VPLS Example 914
Figure 146: BGP AD Configuration Example ................................................. 916
Figure 147: BGP-AD CLI Command Tree ...................................................... 917
Figure 148: BGP AD Triggering LDP Functions ............................................. 919
Figure 149: Show Router LDP Session Output .............................................. 920
Figure 150: Show Router LDP Bindings FEC-Type Services ......................... 920
Figure 151: PW-Template CLI Tree ............................................................. 921
Figure 152: PW-Template-Binding CLI Syntax ............................................ 922
Figure 153: BGP VPLS Example ................................................................. 923
Figure 154: Policy-Based Forwarding For Deep Packet Inspection .................... 927

IEEE 802.1ah Provider Backbone Bridging
Figure 155: Large HVPLS Deployment ....................................................... 1191
Figure 156: Large PBB-VPLS Deployment ................................................... 1192
Figure 157: QinQ Payload in Provider Header Example ................................ 1193
Figure 158: PBB Mapping to VPLS Constructs ............................................ 1194
Figure 159: PBB Packet Walkthrough ...................................................... 1198
Figure 160: Control and User B-VPLS with FIDs ......................................... 1202
Figure 161: Sample Partial Mesh network ................................................ 1204
Figure 162: Unicast Paths for Low-path-id and High-path-id ......................... 1205
Figure 163: Multicast Paths for Low-path-id and High-path-id ..................... 1206
Figure 164: Static MACs Example .............................................................. 1210
Figure 165: Static ISIDs Example ............................................................. 1211
Figure 166: ISID Policy Example ............................................................... 1214
Figure 167: Sample Network ................................................................. 1215
Figure 168: Customer Services Transported in 1 B-VPLS (M:1 Model) .......... 1223
Figure 169: Flood Containment Requirement in M:1 Model .......................... 1224
Figure 170: Inter-Domain Topology ......................................................... 1227
Figure 171: Limiting the Scope of MMRP Advertisements ......................... 1227
Figure 172: Mobile Backhaul Use Case .................................................... 1232
Figure 173: PBB-EPipe with B-VPLS over Ethernet Tunnel ......................... 1233
Figure 174: G.8031 P2P Tunnels and LAG-Like Loadsharing Co-Existence ........ 1234
Figure 175: Ethernet Tunnel Overlay ......................................................... 1236
Figure 176: TCN Triggered PBB Flush-ALI-But-Mine Procedure ..................... 1243
Figure 177: PBB Flush-All-But-Mine Procedure ......................................... 1246
Figure 178: PBB Blackholing Issue — MC LAG ......................................... 1247
Figure 179: MAC Flush Using LDP Signaling - Failure of MC LAG Link ............ 1248
Figure 180: MAC Flush Using LDP Signaling - Active Pseudowire Transition ...... 1249
Figure 181: Access Dual-Homing into PBB BEBs - Topology View .................. 1250
Figure 182: PBB Active Topology and Access Multi-Homing ....................... 1251
Figure 183: Access Multi-Homing - Link Failure ...................................... 1253
List of Figures
## List of Tables

### Getting Started
Table 1: Configuration Process ................................................................. 29

### Services Overview
Table 2: MAC-SWAP Configuration and Options ........................................ 62
Table 3: Defect Conditions and Priority Settings ....................................... 118
Table 4: Facility MEP Support Overview .................................................... 152

### VLL Services
Table 5: VLL, SAP, Pseudowire and SDP Types ........................................ 282
Table 6: Behavior and Relative Priorities ................................................. 289
Table 7: Mobile Infrastructure Definitions ............................................... 294
Table 8: Unstructured Payload Defaults .................................................... 294
Table 9: Structured Number of Frames Defaults ....................................... 378
Table 10: SAP MEP Signaling .................................................................. 446
Table 11: Supported SAP Types ................................................................. 446
Table 12: Default QinQ and TopQ SAP Dot1P Evaluation ............................. 622
Table 13: Bottom Position QinQ and TopQ SAP Dot1P Evaluation ................. 623

### Virtual Private LAN Service
Table 14: SAP Chain Creation ................................................................. 765
Table 15: SAP Chain Creation ................................................................. 766
Table 16: SAP Chain Creation ................................................................. 766
Table 17: Ingress Routed to VPLS Next-Hop Behavior ................................. 830
Table 18: Egress Routed VPLS Next-Hop Behavior ..................................... 830
Table 19: MSTP and MVRP Interaction Table ............................................. 850
Table 20: SAP BPDU Encapsulation States ............................................... 878
Table 21: Spoke SDP BPDU Encapsulation States ....................................... 895
Table 22: Default QinQ and TopQ SAP Dot1P Evaluation ............................ 1106
Table 23: Bottom Position QinQ and TopQ SAP Dot1P Evaluation ............... 1108

### IEEE 802.1ah Provider Backbone Bridging
Table 24: B-VPLS Control Planes ......................................................... 1200
Table 25: SPB Ethernet OAM Operation Summary ..................................... 1208
Table 26: SPBM ISID Policies Table ......................................................... 1212

### Internet Enhanced Service
Table 27: QPPB Interactions with SAP Ingress QoS ................................... 1359
Table 28: RADIUS Accounting Table ...................................................... 1365
Table 29: Packet Sizes Used for Pseudowire SAPs ................................... 1374
Table 30: SRRP State Effect on Subscriber Hosts Associated with Group IP Interface ..................................................... 1382
Table 31: Default Dot1P Explicit Marking Actions ..................................... 1570
Table 32: QinQ Mark Top Only Explicit Marking Actions ............................ 1570

### Virtual Private Routed Network Service
Table 36: BGP Fast Reroute Scenarios (VPRN Context) ............................. 1623
List of Tables

Table 37: QPPB Interactions with SAP Ingress QoS .................................................. 1634
Table 38: DSCP/FC Marking ................................................................................. 1641
Table 39: Service Labels Distributed in Service Label per Next-Hop Mode ................. 1666
Table 40: Supported Configuration Combinations .................................................... 1673
Table 41: Supported Configuration Combinations .................................................... 1673
Table 42: Bottom Position QinQ and TopQ SAP Dot1P Evaluation .......................... 2008
Table 43: Show Service Egress Label Output Fields .................................................. 2181
Preface

About This Guide

This guide describes Layer 2 and Layer 3 VPN services and associated functions provided by Alcatel-Lucent’s family of routers and presents examples to configure and implement various protocols and services.

This document is organized into functional chapters and provides concepts and descriptions of the implementation flow, as well as Command Line Interface (CLI) syntax and command usage.

Audience

This manual is intended for network administrators who are responsible for configuring the routers. It is assumed that the network administrators have an understanding of networking principles and configurations. Protocols, standards, and services described in this manual.

List of Technical Publications

The 7950 SR documentation set is composed of the following books:

- 7950 SR Basic System Configuration Guide
  This guide describes basic system configurations and operations.
- 7950 SR System Management Guide
  This guide describes system security and access configurations as well as event logging and accounting logs.
- 7950 SR Interface Configuration Guide
  This guide describes XMA Control Module (XCM), XRS Media Adaptor (XMA), port and Link Aggregation Group (LAG) provisioning.
- 7950 SR Router Configuration Guide
  This guide describes logical IP routing interfaces and associated attributes such as an IP address, as well as IP and MAC-based filtering, and VRRP and Cflowd.
- 7950 SR Routing Protocols Guide
This guide provides an overview of routing concepts and provides configuration examples for RIP, OSPF, IS-IS, BGP, and route policies.

- **7950 SRS MPLS Guide**
  This guide describes how to configure Multiprotocol Label Switching (MPLS) and Label Distribution Protocol (LDP).

- **7950 SR Services Guide**
  This guide describes how to configure service parameters such as service distribution points (SDPs), customer information, and user services.

- **7950 SR OAM and Diagnostic Guide**
  This guide describes how to configure features such as service mirroring and Operations, Administration and Management (OAM) tools.

- **7950 SR Quality of Service Guide**
  This guide describes how to configure Quality of Service (QoS) policy management.
Technical Support

If you purchased a service agreement for your router and related products from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance. If you purchased an Alcatel-Lucent service agreement, contact your Alcatel-Lucent sales representative.

http://support.alcatel-lucent.com

Product manuals and documentation updates are available at alcatel-lucent.com. If you are a new user and require access to this service, contact your Alcatel-Lucent sales representative.

http://www.alcatel-lucent.com/myaccess

Report documentation errors, omissions and comments to:

ipd_online_feedback@alcatel-lucent.com

Include document name, version, part number and page(s) affected.
Preface
In This Chapter

This book provides process flow information to configure provision services.

Alcatel-Lucent 7950 SR-Series Services Configuration Process

Table 1 lists the tasks necessary to configure Layer 2 and Layer 3 services and configure mirroring.
This guide is presented in an overall logical configuration flow. Each section describes a software area and provides CLI syntax and command usage to configure parameters for a functional area.

Table 1: Configuration Process

<table>
<thead>
<tr>
<th>Area</th>
<th>Task</th>
<th>Chapter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global entities</td>
<td>fet</td>
<td></td>
</tr>
<tr>
<td>VLL services</td>
<td>Ethernet Pipe (Epipe) Services on page 246</td>
<td></td>
</tr>
<tr>
<td>VPLS service</td>
<td>Virtual Private LAN Service on page 539</td>
<td></td>
</tr>
<tr>
<td>IES service</td>
<td>Internet Enhanced Service on page 1053</td>
<td></td>
</tr>
<tr>
<td>VPRN service</td>
<td>Virtual Private Routed Network Service on page 1187</td>
<td></td>
</tr>
<tr>
<td>Reference</td>
<td>List of IEEE, IETF, and other proprietary entities.</td>
<td>Standards and Protocol Support on page 1787</td>
</tr>
</tbody>
</table>
In This Chapter

This chapter provides the command reference trees for the 7950 SR services.

Topics include:

- Global Services Commands
  - Customer Commands on page 155
  - Pseudowire (PW) Commands on page 157
- Service Configuration Commands
  - Epipe Service Configuration Commands on page 381
  - VPLS Service Configuration Commands on page 712
  - IES Service Configuration Commands on page 1091
SERVICES OVERVIEW

In This Section

This section provides an overview of the 7950 SR service model and service entities. Additional details on the individual subscriber services can be found in subsequent chapters.

Topics in this section include:

• Introduction on page 34
  → Service Types on page 35
  → Service Policies on page 36
• Alcatel-Lucent Service Model on page 39
• Service Entities on page 40
  → Customers on page 41
  → Service Access Points (SAPs) on page 41
  → Service Distribution Points (SDPs) on page 48
• Multi-Service Sites on page 61
• G.8032 Ethernet Ring Protection Switching on page 62
• Ethernet Unnumbered Interfaces on page 68
• Mobile Solutions on page 2039
• Internal Objects Created for L2TP and NAT on page 77
• Service Creation Process Overview on page 78
• Deploying and Provisioning Services on page 79
• Configuration Notes on page 80
Introduction

A service is a globally unique entity that refers to a type of connectivity service for either Internet or VPN connectivity. Each service is uniquely identified by a service ID and an optional service name within a service area. The 7950 SR service model uses logical service entities to construct a service. In the service model, logical service entities provide a uniform, service-centric configuration, management, and billing model for service provisioning.

In the 7950 SR services can provide Layer 2/bridged service or Layer 3/IP routed connectivity between a service access point (SAP) on one router and another service access point (a SAP is where traffic enters and exits the service) on the same (local) router or another router (distributed). A distributed service spans more than one router.

Distributed services use service distribution points (SDPs) to direct traffic to another 7950 SR through a service tunnel. SDPs are created on each participating router, specifying the origination address (the router participating in the service communication) and the destination address of another router. SDPs are then bound to a specific customer service. Without the binding process, far-end router is not able to participate in the service (there is no service without associating an SDP with a service).
Service Types

The 7950 SR offers the following types of services which are described in more detail in the referenced chapters:

- Virtual Leased Line (VLL) services:
  - Ethernet pipe (Epipe) — A Layer 2 point-to-point VLL service for Ethernet frames. See Ethernet Pipe (Epipe) Services on page 246.

- Virtual Private LAN Service (VPLS) — A Layer 2 multipoint-to-multipoint VPN. See Virtual Private LAN Service on page 539. VPLS includes Hierarchical VPLS (H-VPLS) which is an enhancement of VPLS which extends Martini-style signaled or static virtual circuit labeling outside the fully meshed VPLS core.

- Internet Enhanced Service (IES) — A direct Internet access service where the customer is assigned an IP interface for Internet connectivity. See Internet Enhanced Service on page 1053.

- Virtual Private Routed Network (VPRN) — A Layer 3 IP multipoint-to-multipoint VPN service as defined in RFC 2547bis. See Virtual Private Routed Network Service on page 1187.
Service Policies

Common to all 7950 SR connectivity services are policies that are assigned to the service. Policies are defined at a global level and then applied to a service on the router. Policies are used to define service enhancements. The types of policies that are common to all 7950 SR connectivity services are:

- **SAP Quality of Service (QoS) policies** which allow for different classes of traffic within a service at SAP ingress and SAP egress.

  QoS ingress and egress policies determine the QoS characteristics for a SAP. A QoS policy applied to a SAP specifies the number of queues, queue characteristics (such as forwarding class, committed, and peak information rates, etc.) and the mapping of traffic to a forwarding class. A QoS policy must be created before it can be applied to a SAP. A single ingress and a single egress QoS policy can be associated with a SAP.

- **Filter policies** allow selective blocking of traffic matching criteria from ingressing or egressing a SAP.

  Filter policies, also referred to as access control lists (ACLs), control the traffic allowed in or out of a SAP based on MAC or IP match criteria. Associating a filter policy on a SAP is optional. Filter policies are identified by a unique filter policy ID. A filter policy must be created before it can be applied to a SAP. A single ingress and single egress filter policy can be associated with a SAP.

- **Scheduler policies** define the hierarchy and operating parameters for virtual schedulers.

  Schedulers are divided into groups based on the tier each scheduler is created under. A tier is used to give structure to the schedulers within a policy and define rules for parent scheduler associations.

- **Accounting policies** define how to count the traffic usage for a service for billing purposes.

  The routers provide a comprehensive set of service-related counters. Accounting data can be collected on a per-service, per-forwarding class basis, which enables network operators to accurately measure network usage and bill each customer for each individual service using any of a number of different billing models.
Ingress Service Queuing

Normal or service queuing is the default mode of operation for SAP ingress queuing. Service queuing preserves ingress forwarding bandwidth by allowing a service queue defined in an ingress SAP QoS policy to be represented by a group of hardware queues. A hardware queue is created for each switch fabric destination to which the logical service queue must forward packets. For a VPLS SAP with two ingress unicast service queues, two hardware queues are used for each destination forwarding engine the VPLS SAP is forwarding to. If three switch fabric destinations are involved, six queues are allocated (two unicast service queues multiplied by three destination forwarding complexes equals six hardware queues). Figure 1 demonstrates unicast hardware queue expansion. Service multipoint queues in the ingress SAP QoS policy are not expanded to multiple hardware queues, each service multipoint queue defined on the SAP equates to a single hardware queue to the switch fabric.

When multiple hardware queues represent a single logical service queue, the system automatically monitors the offered load and forwarding rate of each hardware queue. Based on the monitored state of each hardware queue, the system imposes an individual CIR and PIR rate for each queue that provides an overall aggregate CIR and PIR reflective of what is provisioned on the service queue.
Multicast Queue is Represented by a Single Hardware Queue (Single Pass)

Unicast Queue is Represented by Multiple SF Destination Hardware Queues

Figure 1: Unicast Service Queue Mapping to Multiple Destination Based Hardware Queues
Alcatel-Lucent Service Model

In the Alcatel-Lucent service model, the service edge routers are deployed at the provider edge. Services are provisioned on the service routers and transported across an IP and/or IP/MPLS provider core network in encapsulation tunnels created using generic router encapsulation (GRE) or MPLS label switched paths (LSPs).

The service model uses logical service entities to construct a service. The logical service entities are designed to provide a uniform, service-centric configuration, management, and billing model for service provisioning. Some benefits of this service-centric design include:

- Many services can be bound to a single customer.
- Many services can be bound to a single tunnel.
- Tunnel configurations are independent of the services they carry.
- Changes are made to a single logical entity rather than multiple ports on multiple devices. It is easier to change one tunnel rather than several services.
- The operational integrity of a logical entity (such as a service tunnel and service end points) can be verified rather than dozens of individual services improving management scaling and performance.
- QoS policies, filter policies, and accounting policies are applied to each service instead of correlating parameters and statistics from ports to customers to services.

Service provisioning uses logical entities to provision a service where additional properties can be configured for bandwidth provisioning, QoS, security filtering, accounting/billing to the appropriate entity.
The basic logical entities in the service model used to construct a service are:

- **Customers** (see page 41)
- **Service Access Points (SAPs)** (see page 41)
- **Service Distribution Points (SDPs)** (see page 48) (for distributed services only)

![Figure 2: Service Entities](image-url)
Customers

The most basic required entity is the customer ID value which is assigned when the customer account is created. To provision a service, a customer ID must be associated with the service at the time of service creation.

Service Access Points (SAPs)

Each service type is configured with at least one service access point (SAP). A SAP identifies the customer interface point for a service on an Alcatel-Lucent router. The SAP configuration requires that slot, XMA/MDA, and port information be specified. The slot, XMA/MDA, and port parameters must be configured prior to provisioning a service (see the Cards, XMAs, MDAs, and Ports sections of the OS Interface Guide).

A SAP is a local entity to the router and is uniquely identified by:

- The physical Ethernet port
- The encapsulation type
- The encapsulation identifier (ID)

Depending on the encapsulation, a physical port or channel can have more than one SAP associated with it. SAPs can only be created on ports or channels designated as “access” in the physical port configuration. SAPs cannot be created on ports designated as core-facing “network” ports as these ports have a different set of features enabled in software.

![Figure 3: Service Access Point (SAP)](image)

A SAP can also be associated with a pseudowire port rather than an access port. Such SAPs are called pseudowire SAPs. It is only applicable to IES or VPRN services. Pseudowire ports...
represent pseudowires in enhanced subscriber management (ESM). For a description of pseudowire ports, see the SR OS Triple Play Guide.
SAP Encapsulation Types and Identifiers

The encapsulation type is an access property of a service Ethernet port or SONET/SDH or TDM channel. The appropriate encapsulation type for the port or channel depends on the requirements to support multiple services on a single port/channel on the associated SAP and the capabilities of the downstream equipment connected to the port/channel. For example, a port can be tagged with IEEE 802.1Q (referred to as dot1q) encapsulation in which each individual tag can be identified with a service. A SAP is created on a given port or channel by identifying the service with a specific encapsulation ID.

Ethernet Encapsulations

The following lists encapsulation service options on Ethernet ports:

- **Null** — Supports a single service on the port. For example, where a single customer with a single service customer edge (CE) device is attached to the port. The encapsulation ID is always 0 (zero).
- **Dot1q** — Supports multiple services for one customer or services for multiple customers (Figure 4). For example, the port is connected to a multi-tenant unit (MTU) device with multiple downstream customers. The encapsulation ID used to distinguish an individual service is the VLAN ID in the IEEE 802.1Q header.
- **QinQ** — The QinQ encapsulation type adds a IEEE 802.1Q tag to the 802.1Q tagged packets entering the network to expand the VLAN space by tagging tagged packets, producing a double tagged frame.

![Figure 4: Multiple SAPs on a Single Port/Channel](OSSG003)

---

7950 SR OS Services Guide Page 43
Default SAP on a Dot1q Port

This feature introduces default SAP functionality on Dot1q-encapsulated ports. This is similar to the functionality provided by Q1* SAP on QinQ encapsulated ports, meaning that on Dot1q-encapsulated ports where a default SAP is configured, all packets with q-tags not matching any explicitly defined SAPs will be assigned to this SAP. SAPs with default QinQ encapsulation are supported in VPLS, Epipe, IES and VPRN services. Snooping is supported for QinQ SAPs. In this context, the character “*” indicates default which means allow through. A 0 value means that it should not be there which allows the Qtag to be missing.

One of the applications where this feature can be applicable is an access connection of a customer who uses the whole port to access Layer 2 services. The internal VLAN tags are transparent to the service provider. This can be provided by a null encapsulated port. A dedicated VLAN (not used by the user) can be used to provide CPE management.

In this type of environment, logically two SAPs exist, a management SAP and a service SAP. The management SAP can be created by specifying a VLAN tag which is reserved to manage the CPE. The service SAP covers all other VLANs and behaves as a SAP on a null-encapsulated port.

There are a few constraints related for the use of default SAP on a Dot1q-encapsulated port:

- This type of SAP is supported only on VPLS and Epipe services and cannot be created in IES and VPRN services as it cannot preserve VLAN tag markings.
- For VPLS SAPs with STP enabled, STP listens to untagged and null-tagged BPDUs only. All other tagged BPDUs are forwarded like other customer packets. This is the same behavior as null-encapsulated ports.
- IGMP snooping is not supported on a default SAP. This would require remembering VLAN tags per hosts. By not allowing IGMP snooping of this SAP, all IGMP packets will be transparently forwarded.
- This type of SAP is mutually exclusive with a SAP defined by explicit null encapsulation (for example, 1/1/1:0). This avoids conflict as to which SAP untagged frames should be associated.
## Services and SAP Encapsulations

<table>
<thead>
<tr>
<th>Port Type</th>
<th>Encapsulation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet</td>
<td>Null</td>
</tr>
<tr>
<td>Ethernet</td>
<td>Dot1q</td>
</tr>
<tr>
<td>Ethernet</td>
<td>QinQ</td>
</tr>
</tbody>
</table>
SAP Configuration Considerations

When configuring a SAP, consider the following:

- A SAP is a local entity and only locally unique to a given device. The same SAP ID value can be used on another 7950 SR.
- There are no default SAPs.
- The default administrative state for a SAP at creation time is administratively enabled.
- When a SAP is deleted, all configuration parameters for the SAP will also be deleted. For Internet Enhanced Service (IES), the IP interface must be shutdown before the SAP on that interface may be removed.
- A SAP is owned by and associated with the service in which it is created in each router.
- A port/channel with a dot1q or BCP-dot1q encapsulation type means the traffic for the SAP is identified based on a specific IEEE 802.1Q VLAN ID value. The VLAN ID is stripped off at SAP ingress and the appropriate VLAN ID placed on at SAP egress. As a result, VLAN IDs only have local significance, so the VLAN IDs for the SAPs for a service need not be the same at each SAP.
- If a port/channel is administratively shutdown, all SAPs on that port/channel will be operationally out of service.
- A SAP cannot be deleted until it has been administratively disabled (shutdown).
- Each SAP can have one each of the following policies assigned:
  → Ingress filter policy
  → Egress filter policy
  → Ingress QoS policy
  → Egress QoS policy
  → Accounting policy
  → Ingress scheduler policy
  → Egress scheduler policy
G.8032 Protected Ethernet Rings

Ethernet ring protection switching offers ITU-T G.8032 specification compliance to achieve resiliency for Ethernet Layer 2 networks. G.8032 (Ethernet-ring) is built on Ethernet OAM and often referred to as Ring Automatic Protection Switching (R-APS).

For further information on Ethernet rings, see G8032 Ethernet Ring Protection Switching on page 62.
Service Distribution Points (SDPs)

- SDP Binding on page 49
- Spoke and Mesh SDPs on page 50
- SDP Using BGP Route Tunnel on page 50
- SDP Keepalives on page 51
- SDP Administrative Groups on page 51
- SDP Selection Rules on page 53
- SAP & MPLS Binding Loopback with MAC Swap on page 53
- Class-Based Forwarding on page 59
- Virtual and Non-Virtual Channel on page 70
- Lag Support on page 75

A service distribution point (SDP) acts as a logical way to direct traffic from one router to another through a uni-directional (one-way) service tunnel. The SDP terminates at the far-end device which directs packets to the correct service egress SAPs on that device. A distributed service consists of a configuration with at least one SAP on a local node, one SAP on a remote node, and an SDP binding the service to the service tunnel.

An SDP has the following characteristics:

- An SDP is locally unique to a participating routers. The same SDP ID can appear on other Alcatel-Lucent routers.
- An SDP uses the system IP address to identify the far-end edge router.
- An SDP is not specific to any one service or any type of service. Once an SDP is created, services are bound to the SDP. An SDP can also have more than one service type associated with it.
- All services mapped to an SDP use the same transport encapsulation type defined for the SDP (either GRE or MPLS).
- An SDP is a management entity. Even though the SDP configuration and the services carried within are independent, they are related objects. Operations on the SDP affect all the services associated with the SDP. For example, the operational and administrative state of an SDP controls the state of services bound to the SDP.

An SDP from the local device to a far-end router requires a return path SDP from the far-end SR-SeriesESS-Series back to the local router. Each device must have an SDP defined for every remote router to which it wants to provide service. SDPs must be created first, before a distributed service can be configured.
SDP Binding

To configure a distributed service from ALA-A to ALA-B, the SDP ID (1) (shown in Figure 5) must be specified in the service creation process in order to “bind” the service to the tunnel (the SDP). Otherwise, service traffic is not directed to a far-end point and the far-end device(s) cannot participate in the service (there is no service). To configure a distributed service from ALA-B to ALA-A, the SDP ID (5) must be specified.

Figure 5: GRE Service Distribution Point (SDP) Pointing from ALA-A to ALA-B
Spoke and Mesh SDPs

When an SDP is bound to a service, it is bound as either a spoke SDP or a mesh SDP. The type of SDP indicates how flooded traffic is transmitted.

A spoke SDP is treated like the equivalent of a traditional bridge “port” where flooded traffic received on the spoke SDP is replicated on all other “ports” (other spoke and mesh SDPs or SAPs) and not transmitted on the port it was received.

All mesh SDPs bound to a service are logically treated like a single bridge “port” for flooded traffic where flooded traffic received on any mesh SDP on the service is replicated to other “ports” (spoke SDPs and SAPs) and not transmitted on any mesh SDPs.

SDP Using BGP Route Tunnel

SDP is enhanced to use BGP route tunnel to extend inter-AS support for L2VPN services. An SDP can be configured based on service transport method (for example, GRE or MPLS tunnel). MPLS SDP support is enhanced to allow a BGP route tunnel to reach the far-end PE.

A single method of tunneling is allowed per SDP (for example, LDP, RSVP-TE LSP or BGP route tunnel). BGP route tunnel method is excluded if multi-mode transport is enabled for an SDP.

For the inter-AS far-end PE, next-hop for BGP route tunnel must be one of the local ASBR. The LSP type selected to reach the local ASBR (BGP labeled route next-hop) must be configured under the BGP global context. LDP must be supported to provide transport LSP to reach the BGP route tunnel next-hop.

Only BGP route labels can be used to transition from ASBR to the next-hop ASBR. The global BGP route tunnel transport configuration option must be entered to select an LSP to reach the PE node from ASBR node. On the last BGP segment, both “BGP+LDP” and LDP routes may be available to reach the far-end PE from the ASBR node. LDP LSP must be preferred due to higher protocol priority. This leads to just one label besides other labels in stack to identify VC/VPN at far-end PE nodes.
SDP Keepalives

SDP keepalives actively monitor the SDP operational state using periodic Alcatel-Lucent SDP ping echo request and echo reply messages. Alcatel-Lucent SDP ping is a part of Alcatel-Lucent’s suite of service diagnostics built on an Alcatel-Lucent service-level OA&M protocol. When SDP ping is used in the SDP keepalive application, the SDP echo request and echo reply messages are a mechanism for exchanging far-end SDP status.

Configuring SDP keepalives on a given SDP is optional. SDP keepalives for a particular SDP have the following configurable parameters:

- Admin up/admin down state
- Hello time
- Message length
- Max drop count
- Hold down time

SDP keepalive echo request messages are only sent when the SDP is completely configured and administratively up and SDP keepalives is administratively up. If the SDP is administratively down, keepalives for the SDP are disabled.

SDP keepalive echo request messages are sent out periodically based on the configured Hello Time. An optional message length for the echo request can be configured. If max drop count echo request messages do not receive an echo reply, the SDP will immediately be brought operationally down.

If a keepalive response is received that indicates an error condition, the SDP will immediately be brought operationally down.

Once a response is received that indicates the error has cleared and the hold down time interval has expired, the SDP will be eligible to be put into the operationally up state. If no other condition prevents the operational change, the SDP will enter the operational state.

For information about configuring keepalive parameters, refer to.

SDP Administrative Groups

This feature introduces the support of SDP administrative groups, referred to as SDP admin groups. SDP admin groups provide a way for services using a pseudowire template to automatically include or exclude specific provisioned SDPs. SDPs sharing a specific characteristic or attribute can be made members of the same admin group.
The user first creates the admin groups that are to be used by SDPs on this node:

```
config>service>sdp-group>group-name group-name value group-value create
```

A maximum of 32 admin groups can be created. The `no` option is only allowed if the group-name is not referenced in a pw-template or SDP.

The group value ranges from zero (0) to 31. It is uniquely associated with the group name at creation time. If the user attempts to configure another group name for a group value that is already assigned to an existing group name, the SDP admin group creation is failed. The same happens if the user attempts to configure an SDP admin group with a new name but associates it to a group value already assigned to an existing group name.

Next, the user configures the SDP membership in admin groups:

```
config>service>sdp>sdp-group
```

The user can enter a maximum of one (1) admin group name at once. The user can execute the command multiple times to add membership to more than one admin group. The admin group name must have been configured or the command is failed. Admin groups are supported on an SDP of type GRE and of type MPLS (BGP/RSVP/LDP). They are also supported on an SDP with the `mixed-lsp-mode` option enabled.

The user then selects which admin groups to include or exclude in a given pseudowire template:

```
config>service>pw-template>sdp-include group-name
config>service>pw-template>sdp-exclude group-name
```

The admin group name must have been configured or the command is failed. The user can execute the command multiple times to include or exclude more than one admin group. The `sdp-include` and `sdp-exclude` commands can only be used with the `use-provisioned-sdp` option. If the same group name is included and excluded within the same pseudowire template, only the exclude option will be enforced.

Any changes made to the admin group `sdp-include` and `sdp-exclude` constraints will only be reflected in existing spoke SDPs after the following command has been executed:

```
tools>perform>service>eval-pw-template>allow-service-impact
```

When the service is bound to the pseudowire template, the SDP selection rules will enforce the admin group constraints specified in the `sdp-include` and `sdp-exclude` commands.

```
config>service>vpls:bgp>pw-template-binding policy-id
config>service:epipe:spoke-sdp-fec>pw-template-bind policy-id
```
Note that the group value is what is used to uniquely identify an SDP admin group throughout the network in the 5620 SAM. The node will send both the group name and value to 5620 SAM, or other SNMP device, at the creation of the SDP admin group. In all other operations in the node, such as adding an SDP to an admin group or including/excluding an SDP admin group in a service context, only the group name is sent to the 5620 SAM or the SNMP device.

SDP admin groups can be enabled on all 7x50 services that make use of the pseudowire template (BGP-AD VPLS service, BGP-VPLS service, BGP-VPWS and FEC129 VLL service). In the latter case, Release 11.0.R1 provides support at the T-PE nodes only.

---

**SDP Selection Rules**

In the current SDP selection process, all provisioned SDPs with the correct far-end IP address, the correct tunnel-far-end IP address, and the correct service label signaling are considered. The SDP with the lowest admin metric is selected. If more than one SDP with the same lowest metric are found, then the SDP with the highest sdp-id is selected. The type of SDP, GRE or MPLS (BGP/RSVP/LDP) is not a criterion in this selection.

The selection rule with SDP admin groups is modified such that the following admin-group constraints are applied up front to prune SDPs that do not comply:

- If one or more sdp-include statement is part of the pw-template, then an SDP that is a member of one or more of the included groups will be considered. With the sdp-include statement, there is no preference for an SDP that belongs to all included groups versus one that belongs to one or fewer of the included groups. All SDPs satisfying the admin-group constraint will be considered and the selection above based on the lowest metric and highest sdp-id is applied.
- If one or more sdp-exclude statement is part of the pw-template, then an sdp that is a member of any of the excluded groups will not be considered.

---

**SAP & MPLS Binding Loopback with MAC Swap**

SAPs and MPLS SDP bindings within Ethernet services, Epipe and VPLS, may be placed into a loopback mode that allows all packets that arrive on the looped entity to be reflected back into the service. The function is specific to the entity on which the loopback is configured and is non-disruptive to other SAPs and SDP bindings on the same port or LAG.

Epipe and PBB Epipe service constructs support both ingress and egress loopbacks on Ethernet SAPs or MPLS SDP bindings.

VPLS and I-VPLS service constructs support both in ingress and egress loopback on Ethernet SAPs or MPLS SDP bindings.
Do not enable this functionality in the core PBB context because there is no ISID awareness. If this feature is enabled within the core PBB context ALL traffic that arrives on the B-SAP or B-MPLS binding will be looped back into the PBB context without regard for ISID or customer specific MAC headers.

An ingress loopback configured on the entity will have the following effects on forwarding for the entity:

- Traffic arriving on the entity will be looped back to the same entity, via the fabric.
- Traffic that is attempting to egress that entity from another SAP or SDP binding within the service will be blocked.

Essentially an ingress loopback function will isolate the SAP or MPLS SDP binding from the rest of the service. The Figure 6 uses a simple Epipe service to illustrate the various touch points and processing that occurs on a packet that is processed by an ingress loopback as it moves through the network element.

![Figure 6: Ingress Loopback](image)
An egress loopback configured on the entity will have the following effects on the forwarding for the entity.

- Traffic that arrives on any service SAP or SDP binding that arrives on the egress that is in loopback will be looped back into the service.
- Any traffic that is attempting to gain access to the service from that entity (ingress the network element from the entity) will be dropped.

In the case of the egress loopback the SAP or MPLS SDP binding is not isolated from the rest of the service it remains part of the service and reflects traffic back into the service. Extreme care must be used when considering the application of an egress loopback in a VPLS or I-VPLS service. Since a VPLS service rely on MAC based forwarding any packet that arrives at an egress loopback will be reflected back into the service and use MAC based forwarding to apply the proper forwarding decision. If this is a live multipoint service with active endpoints this could have very negative effects on the service and the clients connected to this service. Even if the forwarding database is primed any broadcast, unknown or multicast that arrives in the service will arrive on the egress loopback and will be reflected back into the service causing at the very least duplication of all of this type of traffic.

Figure 7 uses a simple Epipe service to illustrate the various touch points and processing that occurs on a packet that is processed by an egress loopback as it moves through the network element. Egress processing will not perform queuing functions on the egress it will only perform the functions of the forwarding plane like remarking.

![Figure 7: Egress Loopback](image)

The operational state of the SAP or MPLS SDP binding will not change as a result of the loopback function. This means a SAP or MPLS SDP binding that is operationally up will not change state strictly because of the loopback be started or stopped. Of course control protocols that are attempting to gain access via the entity that is not allowing packets to enter the service will eventually time out.
Care must be taken when considering the use of control protocols in a service with enabled loopbacks. The operator must be very aware of the impact that interrupting control protocols can have on the state of the SAP. When SAPs are dynamically created using a protocol or a protocol is required to maintain the operational state of the SAP, interruption of this control protocol will cause the SAP to fail. Other SAPs linking their state to a failed SAP will react to that failure as well. This loopback function is per Ethernet SAP or MPLS SDP binding. This means that all traffic that is not extracted and sent to the CPM prior to the loopback process will all be looped back to in the direction it was received, or in the case of VPLS, back into the service. All service based control protocols that are included with this service should be removed to ensure the loopback process is handling the packets and not some other function on the node that can extract the control protocol but never respond because the service is block. However, there may be instances where an operator would want to continue to run control protocols for the service during a loopback. For example, Down MEPs on an Ethernet SAP could continue to process ETH-CFM packets if the loopback is on the mate Ethernet SAP and was configured as an egress loopback.

By default no MAC swap functions are performed. Options are available to allow for various MAC swap functions. Table 2 lists the various options and functions based on the configured mac-swap and associated options.

Table 2: MAC-SWAP Configuration and Options

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Reflection with Inbound DA</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Action</strong></td>
<td><strong>Options</strong></td>
</tr>
<tr>
<td>mac-swap</td>
<td>no options</td>
</tr>
<tr>
<td>mac-swap</td>
<td>mac</td>
</tr>
<tr>
<td>mac-swap</td>
<td>mac + all</td>
</tr>
<tr>
<td>none</td>
<td>none</td>
</tr>
</tbody>
</table>

Only the outer Layer 2 header can be manipulated.

In order for the loopback function to operate the service, the SAP/ MPLS SDP binding, the port or LAG must be operational. In the case of a LAG the LAG must have members port that are operational. If the port over which the entity is configured is not operational or the LAG has no configured members the loopback function will not loopback traffic.
In order to configure this functionality the operator is required to use the tools hierarchy. In this specific case, the loopback tools supporting this functionality may be configured through CLI or through SNMP. However, these commands are never resident in the configuration. This means the loopback will survive high availability events that cause one CPM to change from standby to active, as well as ISSU function or IOM resets (hard or soft). However the function will not survive a complete node reboot.

In the case on SNMP it is possible to configure a static mac address for the mac swap function without actually invoking the mac-swap. This is not possible through the CLI.

This function requires a minimum of IOM3/IMM.

This feature is mutually exclusive with functions that use mirroring.

Figure 8 shows an example for placing sap 1/1/10:2.2 in service id 2 (an epipe) in an active loopback mode with a mac-swap for all broadcast and multicast destined packets.

```
show service id 2 base
```

```
Service Basic Information

Service Id        : 2                   Vpn Id            : 0
Service Type      : Epipe
Name              : (Not Specified)
Description       : (Not Specified)
Customer Id       : 1                   Creation Origin   : manual
Last Status Change: 07/08/2013 09:57:02
Last Mgmt Change  : 07/08/2013 09:56:49
Admin State       : Up                  Oper State        : Up
MTU               : 1514
Vc Switching      : False
SAP Count         : 2                   SDP Bind Count    : 0
Per Svc Hashing   : Disabled
Force QTag Fwd    : Disabled
```

**Figure 8: Active Loopback Mode**
### Service Access & Destination Points

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Type</th>
<th>AdmMTU</th>
<th>OprMTU</th>
<th>Adm</th>
<th>Opr</th>
</tr>
</thead>
<tbody>
<tr>
<td>sap:1/1/2:2.2</td>
<td>qinq</td>
<td>1522</td>
<td>1522</td>
<td>Up</td>
<td>Up</td>
</tr>
<tr>
<td>sap:1/1/10:2.2</td>
<td>qinq</td>
<td>1522</td>
<td>1522</td>
<td>Up</td>
<td>Up</td>
</tr>
</tbody>
</table>

tools perform service id 2 loopback start sap 1/1/10:2.2 ingress mac-swap mac 00:00:00:00:00:88

### Service Ethernet Loopback Points

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Svc ID</th>
<th>Type</th>
<th>Swap</th>
<th>Swap</th>
<th>Oper</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP 1/1/10:2.2 qinq</td>
<td>2</td>
<td>ingr</td>
<td>SA&lt;-&gt;DA</td>
<td>Static</td>
<td>up</td>
</tr>
</tbody>
</table>

No. of Service ethernet loopback points: 1

tools dump service id 2 loopback sap 1/1/10:2.2

### Service ID 2 SAP 1/1/10:2.2 Loopback

- Identifier (SAP): 1/1/10:2.2 qinq
- Service ID: 2
- Type: Ingress
- MAC Swap:
  - Unicast: SA<->DA
  - Multicast/Broadcast: Static
  - Static MAC: 00:00:00:00:00:88
- SAP Oper State: Up

### Sap Statistics

- Last Cleared Time: N/A
- Packets CPM Ingress: 491790
- Octets CPM Ingress: 46721290

### Forwarding Engine Stats

- Dropped: 0
- Off. HiPrio: 0
- Off. LowPrio: 0
- Off. Uncolor: 0
- Off. Managed: 0

### Queueing Stats (Ingress QoS Policy 1)

- Dro. HiPrio: 0
- Dro. LowPrio: 0
- For. InProf: 0
- For. OutProf: 0
To stop the loopback, a simple `stop` command is required.

```
tools perform service id 2 loopback stop sap 1/1/10:2.2
```

---

## Class-Based Forwarding

- [Application of Class-Based Forwarding over RSVP LSPs on page 59](#)
- [Operation of Class-Based Forwarding over RSVP LSPs on page 60](#)

---

### Application of Class-Based Forwarding over RSVP LSPs

Class based forwarding over RSVP LSPs allows a service packet to be forwarded over a specific RSVP LSP, part of an SDP, based on its ingress determined forwarding class. The LSP selected depends on the operational status and load-balancing algorithms used for ECMP and LAG spraying.

**Figure 9: Class-Based Forwarding over SDP LSPs**

*Figure 9* illustrates the use of class-based forwarding to direct packets of a service to specific RSVP or static LSPs that are part of the same SDP based on the packets' forwarding class. The forwarding class of the packet is the one assigned to the packet as a result of applying the ingress QoS policy to the service SAP. The VLL service packets are all classified into the “*ef*” forwarding class and those that are destined to PE2 are forwarded over LSP1. Multicast and broadcast are classified into the “*be*” class and are forwarded over LSP2.

This feature allows service providers to dedicate specific LSPs with a determined level of traffic engineering and protection to select service packets. For example, packets of a VoIP service are assigned the “*ef*” class to expedite their forwarding but are also sent over carefully traffic-engineered and FRR-protected LSP paths across the service provider network.
Operation of Class-Based Forwarding over RSVP LSPs

The 7950 SR class-based forwarding feature applies to a set of LSPs that are part of the same SDP. Each LSP must be configured as part of an SDP specifying the forwarding classes it will support. A forwarding class can only be assigned to one LSP in a given SDP, meaning that only one LSP within an SDP will support a given class of service. However, multiple classes of services can be assigned to an LSP. Both RSVP and static LSPs are allowed. All subclasses will be assigned to the same LSP as the parent forwarding class.

When a service packet is received at an ingress SAP, it is classified into one of the eight 7950 SR forwarding classes. If the packet will leave the SR on an SDP that is configured for class-based forwarding, the outgoing LSP will be selected based on the packet's forwarding class. Each SDP has a default LSP. The default LSP is used to forward a received packet that was classified at the ingress SAP into a forwarding class for which the SDP does not have an explicitly-configured LSP association. It is also used to forward a received packet if the LSP supporting its forwarding class is down. Note that the SDP goes down if the default LSP is down.

Class-based forwarding can be applied to all services supported by the 7950 SR. For VPLS services, explicit FC-to-LSP mappings are used for known unicast packets. Multicast and broadcast packets use the default LSP. There is a per-SDP user configuration that optionally overrides this behavior to specify an LSP to be used for multicast/broadcast packets.

VLL service packets are forwarded based on their forwarding class only if shared queuing is enabled on the ingress SAP. Shared queuing must be enabled on the VLL ingress SAP if class-forwarding is enabled on the SDP the service is bound to. Otherwise, the VLL packets will be forwarded to the LSP which is the result of hashing the VLL service ID. Since there are eight entries in the ECMP table for an SDP, one LSP ID for each forwarding class, the resulting load balancing of VLL service ID is weighted by the number of times an LSP appears on that table. For instance, if there are eight LSPs, the result of the hashing will be similar to when class based forwarding is disabled on the SDP. If there are fewer LSPs, then the LSPs which were mapped to more than one forwarding class, including the default LSP, will have proportionally more VLL services forwarding to them.

Note that only user packets are forwarded based on their forwarding class. OAM packets are forwarded in the same way as an SDP with class-based forwarding disabled. In other words, LSP ping and LSP trace messages are queued in the queue corresponding to the forwarding class specified by the user and are forwarded over the LSP being tested. Service and SDP OAM packets, such as, service ping, VCCV ping, and SDP ping, are queued in the queue corresponding to the forwarding class specified by the user and forwarded over the first available LSP.

Class-based forwarding is not supported for protocol packets tunnelled through an SDP. All packets are forwarded over the default LSP.

Class-based forwarding is not supported on a spoke SDP used for termination on an IES or VPRN service. All packets are forwarded over the default LSP.
Multi-Service Sites

A customer site can be designated a multi-service site where a single scheduler policy is applied to all SAPs associated with the site while retaining per-service and per-forwarding class shaping and policing. The SAPs associated with the multi-service site can be on a single port or on a single slot. The SAPs in a multi-service site cannot span slots.

Multi-service sites are anchor points to create an ingress and egress virtual scheduler hierarchy. When a site is created, it must be assigned to a chassis slot. When scheduler policies are defined for ingress and egress, the scheduler names contained in each policy are created according to the parameters defined in the policy. Multi-service customer sites exist for the sole purpose of creating a virtual scheduler hierarchy and making it available to queues on multiple Service Access Points (SAPs).

The scheduler policy association with the customer site normally prevents the scheduler policy from being deleted until after the scheduler policy is removed from the customer site.

When the multi-service customer site is created, an ingress and egress scheduler policy association does not exist. This does not prevent the site from being assigned to a chassis slot or prevent service SAP assignment. After the site has been created, the ingress and egress scheduler policy associations can be assigned or removed at any time.

Each customer site must have a unique name within the context of the customer. Modifications made to an existing site immediately affect all SAPs associated with the site. Changing a scheduler policy association can cause new schedulers to be created and existing queues on the SAPs to no longer be orphaned. Existing schedulers on the site may cease to exist, causing queues relying on that scheduler to be orphaned.
G.8032 Ethernet Ring Protection Switching

Ethernet ring protection switching offers ITU-T G.8032 specification compliance to achieve resiliency for Ethernet Layer 2 networks. Similar to G.8031 linear protection (also called Automatic Protection Switching (APS)), G.8032 (Ethernet-ring) is built on Ethernet OAM and often referred to as Ring Automatic Protection Switching (R-APS).

Ethernet-rings are supported on VPLS SAPs (VPLS, I-VPLS, B-VPLS). VPLS services supporting Rings SAPs can connect to other rings and Ethernet service using VPLS and R-VPLS SAPs. Ethernet-rings enable rings for core network or access network resiliency. A single point of interconnection to other services is supported. The Ethernet-ring service is a VLAN service providing protection for ring topologies and the ability to interact with other protection mechanisms for overall service protection. This ensures failures detected by Ethernet-ring only result in R-APS switchover when the lower layer cannot recover and that higher layers are isolated from the failure.

Rings are preferred in data networks where the native connectivity is laid out in a ring or there is a requirement for simple resilient LAN services. Due to the symmetry and the simple topology, rings are viewed a good solution for access and core networks where resilient LANS are required. The Alcatel-lucent implementation can be used for interconnecting access rings and to provide traffic engineered backbone rings.

Ethernet-rings use one VID per control per ring instance and use one (typically) or multiple VIDs for data instances per control instance. A dedicated control VLAN (ERP VLAN) is used to run the protocol on the control VID. G.8032 controls the active state for the data VLANs (ring data instances) associated with a control instance. Multiple control instances allow logically separate rings on the same topology. The Alcatel-lucent implementation supports DOT1q, QinQ and PBB encapsulation for data ring instances. The control channel supports dot1q and QinQ encapsulation. Note that the control channel can support DOT1q while the data channels use queuing if the global `configure>system>ethernet>new-qinq-untagged-sap` command is enabled.
Overview of G.8032 Operation

R-APS messages that carry the G.8032 protocol are sent on dedicated protocol VLAN called ERP VLAN (or Ring Control Instance). In a revertive case, G.8032 Protocol ensures that one Ring Protection Link (RPL) owner blocks the RPL link. R-APS messages are periodically sent around in both directions to inform other nodes in the Ring about the blocked port in the RPL owner node. In non-revertive mode any link may be the RPL. Y.1731 Ethernet OAM CC is the basis of the RAPs messages. Y.1731 CC messages are typically used by nodes in the ring to monitor the health of each link in the ring in both directions. However CC messages are not mandatory. Other link layer mechanisms could be considered – for example LOS (Loss of Signal) when the nodes are directly connected.

Initially each Ring Node blocks one of its links and notifies other nodes in the ring about the blocked link. Once a ring node in the ring learns that another link is blocked, the node unblocks its blocked link possibly causing FDB flush in all links of the ring for the affected service VLANs, controlled by the ring control instance. This procedure results in unblocking all links but the one link and the ring normal (or idle) state is reached. In revertive mode the RPL link will be the link that is blocked when all links are operable after the revert time. In non-revertive mode the RPL link is no different that other ring links. Revertive mode offers predictability particularly when there are multiple ring instances and the operator can control which links are block on the different instances. Each time there is a topology change that affects Reachability, the nodes may flush the FDB and MAC learning takes place for the affected service VLANs, allowing forwarding of packets to continue. Figure 10 depicts this operational state:

![Figure 10: 0-1 G.8032 Ring in the Initial State](image)

When a ring failure occurs, a node or nodes detecting the failure (enabled by Y.1731 OAM CC monitoring) send R-APS message in both directions. This allows the nodes at both ends of the failed link to block forwarding to the failed link preventing it from becoming active. In revertive mode, the RPL Owner then unblocks the previously blocked RPL and triggers FDB flush for all
nodes for the affected service instances. The ring is now in protecting state and full ring connectivity is restored. MAC learning takes place to allow Layer 2 packet forwarding on a ring. The following picture depicts the failed link scenario.

![Figure 11: 0-1 G.8032 Ring in the Protecting State](image)

Once the failed link recovers, the nodes that blocked the link again send the R-APS messages indicating no failure this time. This in turn triggers RPL Owner to block the RPL link and indicate the Blocked RPL link the ring in R-APS message, which when received by the nodes at the recovered link cause them to unblock that link and restore connectivity (again all nodes in the ring perform FBD Flush and MAC learning takes place). The ring is back in the normal (or idle) state.

Within each path, Y.1731 Maintenance Entity Group (MEG) Endpoints (MEPs) are used to exchange R-APS specific information (specifically to co-ordinate switchovers) as well as optionally fast Continuity Check Messages (CCM) providing an inherent fault detection mechanism as part of the protocol. Failure detection of a ring path by one of the mechanisms triggers to activate the protection links. Upon failure, re-convergence times are a dependent on the failure detection mechanisms. In the case of Y.1731, the CCM transmit interval determines the response time. The 7x507210 SAS supports message timers as low as 10 milliseconds (also 100 ms) so the restoration times are comparable to SONET/SDH. Alternatively, 802.3ah (Ethernet in the First Mile) or simple Loss of Signal can act as a trigger for a protection switch where appropriate. In case of direct connectivity between the nodes, there is no need to use Ethernet CC messaging for liveliness detection.

Revertive and non-revertive behaviors are supported. The Ring protection link (RPL) is configured and Ethernet-rings can be configured to revert to the RPL upon recovery.

G.8032 supports multiple data channels (VIDs) or instances per ring control instance (R-APS tag). G.8032 also supports multiple control instances such that each instance can support RPLs on
different links providing for a load balancing capability however once services have been assigned to one instance the rest of the services that need to be interconnected to those services must be on the same instance. In other words each data instance is a separate data VLAN on the same physical topology. When there is any one link failure or any one node failure in the ring, G.8032 protocols are capable of restoring traffic between all remaining nodes in these data instances.

Ethernet R-APS can be configured on any port configured for access mode using dot1q, q-in-q encapsulation enabling support for Ethernet R-APS protected services on the service edge towards the customer site, or within the Ethernet backbone. ELINE, ELAN, and ETREE services can be afforded Ethernet R-APS protection and, although the Ethernet Ring providing the protection uses a ring for protection the services are configured independent of the Ring properties. The intention of this is to cause minimum disruption to the service during Ethernet R-APS failure detection and recovery.

In the implementation, the Ethernet Ring is built from a VPLS service on each node with VPLS SAPs that provides Ring path with SAPs. As a result, most of the VPLS SAP features are available on Ethernet rings if desired. This results in a fairly feature rich ring service.

The control tag defined under each Ethernet-ring is used for encapsulating and forwarding the CCMs and the G.8032 messages used for the protection function. If a failure of a link or node affects an active Ethernet ring segment, the services will fail to receive the CCMs exchanged on that segment or will receive a fault indication from the Link Layer OAM module. CCMs are optional but MEPs are always configured to provide G.8032 control.

For fault detection using CCMs three CC messages plus a configurable hold-off timer must be missed for a fault to be declared on the associated path. The latter mechanism is required to accommodate the existence of additional, 50 ms resiliency mechanism in the optical layer. After it receives the fault indication, the protection module will declare the associated ring link down and the G.8032 state machine will send the appropriate messages to open the RPL and flush the learned addresses.

Flushing is triggered by the G.8032 state machine and the 7x50 implementation allows flooding of traffic during the flushing interval to expedite traffic recovery.

Figure 12 illustrates a resilient Ring Service. In the example a PBB ring (solid line) using VID 500 carries 2 service VLANs on I-SID 1000 and 1001 for Service VIDs (Dot1q 100 and QinQ 400.1 respectively.) The RPL for the PBB ring is between A and B where B is the RPL owner. Also illustrated is a QinQ service on the (dotted line) ring that uses Dot1q VID 600 for the ring to connect service VLAN 100.50. The two rings have RPLs on different nodes which allow a form of load balancing. The example serves to illustrate that service encapsulations and ring encapsulation can be mixed in various combinations. Also note that neither of the rings is closed loop. A ring can restore connectivity when any one node or link fails to all remaining nodes within the 50 ms transfer time (signaling time after detection).
Sample Configuration:

```bash
configure eth-ring 1
  description "Ring PBB BLUE on Node B"
  revert-time 100
  guard-time 5
  ccm-hold-time down 100 up 200
  rpl-node owner
  path a 6/6/1 raps-tag 100 // CC Tag 100
    description "To A ring link"
    rpl-end
    eth-cfm
    mep 1 domain 1 association 1 direction down
      // Control MEP
    no shutdown
    exit
  exit
  no shutdown // would allow protect switching
  // in absence of the "force" cmd
  exit
  path b 6/6/2 raps-tag 100 // Tag 100
    description "to D Ring Link"
    eth-cfm
    mep 1 domain 1 association 1 direction down
    no shutdown
    exit
    no shutdown
    no shutdown
    exit
  service
  vpls 10 customer 1 create // Ring APS SAPs
    description "Ring Control VID 100"
    sap 6/6/1:100 eth-ring 1 create
```
// TAG for the Control Path a
exit
  sap 6/6/2:100 eth-ring 1 create // TAG for the Control Path b
  exit
no shutdown
exit
service
  vpls 40 customer 1 b-vpls create // Data Channel on Ring
description "Ethernet Ring 1 VID 500"
  sap 6/6/1:500 eth-ring 1 create // TAG for the Data Channel Path a
  exit
  sap 6/6/2:500 eth-ring 1 create // TAG for the Data Channel Path b
  exit
exit
service vpls 1000 i-vpls // CPE traffic
sap 3/1/1:100 create // CPE SAP
  pbb
    backbone-vpls 40 isid 1000
    exit
  exit
no shutdown
exit
service vpls 1001 i-vpls // CPE traffic
sap 3/1/2:400.1 create // CPE SAP
  pbb
    backbone-vpls 40 isid 1001
    exit
  exit
no shutdown
exit
Ethernet Unnumbered Interfaces

The ability to configure Ethernet Unnumbered interfaces has been added to support some service types for IPv4. The unnumbered interface capability has been available for other interface types on SR OS. Unnumbered Ethernet allows point-to-point interfaces to borrow the address from other interfaces such as system or loopback interfaces.

This feature enables unnumbered interfaces for some routing protocols (IS-IS and OSPF). Support for routing is dependent on the respective routing protocol and service. This feature also adds support for both dynamic and static ARP for unnumbered Ethernet interfaces to allow interworking with unnumbered interfaces that may not support dynamic ARP.

The use of unnumbered interface has no effect on IPv6 routes but the unnumbered command must only be used in cases where IPv4 is active (IPv4 only and mixed IPv4/IPv6 environments). When using an unnumbered interface for IPv4, the loopback address used for the unnumbered interface must have IPv4 address. Also, interface type for the unnumbered interface will automatically be point-to-point.
Ethernet Ring Sub-Rings

Ethernet Sub-Rings offer a dual redundant way to interconnect rings. The 7x50 supports Sub-Rings connected to major rings and a sub-ring connected to a VPLS (LDP based) for access rings support in VPLS networks. Figure 13 illustrates a Major ring and Sub Ring scenario. In this scenario, any link can fail in either ring (ERP1 or ERP2) and each ring is protected. Furthermore, the sub ring (ERP2) relies on the major Ring (ERP1) as part of its protection for the traffic from C and D. The nodes C and D are configured as inter connection nodes.

Figure 13: 0-4 G.8032 Sub-Ring

Sub-Rings and Major Rings run similar state machines for the ring logic, however there are some differences. When Sub-Rings protect a link, the flush messages are propagated to the major ring. (A special configuration allows control of this option on the 7x50.) When major rings change topology, the flush is propagated around the major ring and does not continue to any sub-rings. The reason for this is that Major Rings are completely connected but Sub-Rings are dependent on another ring or network for full connectivity. The topology changes need to be propagated to the other ring or network usually. Sub-Rings offer the same capabilities as major rings in terms of control and data so that all link resource may be utilized.
Virtual and Non-Virtual Channel

The 7x50 platform supports both the virtual channel and non-virtual channel for sub-ring control communication. In the virtual channel mode, a dedicated VID, other than the major ring RAPs control channel is configured as a data instance on the major ring. This allows the sub-ring control messages and state machine logic to behave similar to a major ring. In the non-virtual channel mode, the sub-ring is only connected by the RAPs control channels on the sub-ring itself. This mode offers slightly less redundancy in the RAPs messaging than the virtual channel mode since sub-ring RAPs messages are not propagated across the major ring. When non-virtual link is configured, the protocol allows RPL messages over the sub-ring blocked link.

![Diagram](image-url)
Sub-ring configuration is similar to major ring configuration and consists of three parts: Ethernet-ring instance configuration, control VPLS configuration and data VPLS configuration (data instance or data channel). The Ethernet-ring configuration of a sub-ring is tied to a major ring and only one path is allowed. Note that a split horizon group is mandatory to ensure that Sub-Ring control messages from the major ring are only passed to the sub-ring control.

The data VPLS can be configured on the major ring, and in the example, shares the same VID (SAP encapsulation) on both the major ring and the sub-ring to keep data on the same VLAN ID everywhere. (Note that just like other services in the 7x50 the encapsulation VID is controlled by SAP configuration and the association to the controlling ring is by the Ethernet-ring, ring-id.)

The following illustrates a sample sub-ring configuration on Node C:

```
eth-ring 2
  description "Ethernet Sub Ring on Ring 1"
  sub-ring virtual-link // Using a virtual link
    interconnect ring-id 1 // Link to Major Ring 1
      propagate-topology-change
      exit
  exit
  path a 1/1/3 raps-tag 100 // Ring control uses VID 100
  eth-cfm
    mep 9 domain 1 association 4
    ccm-enable
    control-mep
    no shutdown
    exit
  exit
  no shutdown
  exit
```

Note that if the sub-ring been configured as a non-virtual-link, the sub-ring configuration above and on all the other sub-ring nodes for this sub-ring would become:

```
sub-ring non-virtual-link // Not using a virtual link

# Control Channel for the Major Ring ERP1 illustrates that Major ring control is still separate from Sub-ring control
vpls 10 customer 1 create
  description "Control VID 10 for Ring 1 Major Ring"
  stp shutdown
  sap 1/1/1:10 eth-ring 1 create
    stp shutdown
    exit
  sap 1/1/4:10 eth-ring 1 create
    stp shutdown
    exit
    no shutdown
    exit

# Data configuration for the Sub-Ring
vpls 11 customer 1 create
```
description "Data on VID 11 for Ring 1"
stp shutdown
sap 1/1/1:11 eth-ring 1 create // VID 11 used for ring
  stp shutdown
exit
stp shutdown
exit
stp shutdown
exit
sap 1/1/4:11 eth-ring 1 create
  stp shutdown
exit
stp shutdown
exit
sap 1/1/3:11 eth-ring 2 create // Sub-ring data
  stp shutdown
exit
sap 3/2/1:1 create
description "Local Data SAP"
  stp shutdown
  no shutdown
exit
# Control Channel for the Sub-Ring using a virtual link. This is
# a data channel as far as Ring 1 configuration. Other Ring 1
# nodes also need this VID to be configured.

vpls 100 customer 1 create
description "Control VID 100 for Ring 2 Interconnection"
split-horizon-group "s1" create //Ring Split horizon Group
exit
stp shutdown
sap 1/1/1:100 split-horizon-group "s1" eth-ring 1 create
  stp shutdown
exit
stp shutdown
exit
sap 1/1/4:100 split-horizon-group "s1" eth-ring 1 create
  stp shutdown
exit
stp shutdown
exit
no shutdown
exit
exit

Note that had the sub-ring been configured as a non-virtual-link the configuration above would become:

vpls 100 customer 1 create
description "Control VID 100 for Ring 2 Interconnection"
sap 1/1/3:100 eth-ring 2 create
  stp shutdown
exit
no shutdown
exit
The 7x50 platform allows for a special configuration of the non-virtual link sub-ring that can be homed to a VPLS service illustrated in Figure 15. This is an economical way to have a redundant ring connection to a VPLS service. This is currently supported only for dot1Q and QinQ sub-rings and only on LDP based VPLS. The primary application for this is access rings that require resiliency. This configuration shows the configuration for a sub-ring at an interconnection node without a virtual channel and interconnected to a VPLS. A VPLS service 1 is used to terminate the ring control. The Ethernet ring data SAP appears in the associated LDP based VPLS service 5.

The following illustrates a sample sub-ring configuration for VPLS (at PE1):

```
eth-ring 1
    description "Ethernet Ring 1"
guard-time 20
no revert-time
rpl-node nbr
sub-ring non-virtual-link
    interconnect vpls // VPLS is interconnection type
    propagate-topology-change
```
exit
exit
path a 1/1/3 raps-tag 1.1
  description "Ethernet Ring : 1 Path on LAG"
  eth-cfm
  mep 8 domain 1 association 8
    ccm-enable
    control-mep
    no shutdown
exit
exit
exit
no shutdown
exit
no shutdown
exit

# Configuration for the ring control interconnection termination:
vpls 1 customer 1 create
  description "Ring 1 Control termination"
  stp shutdown
  sap 1/1/3:1.1 eth-ring 1 create //path a control
    stp shutdown
exit
no shutdown
exit

# Configuration for the ring data into the LDP based VPLS Service
vpls 5 customer 1 create
  description "VPLS Service at PE1"
  stp
    no shutdown
exit
  sap 1/1/3:2.2 eth-ring 1 create
    stp shutdown
exit
  sap 1/1/5:1 create
exit
  mesh-sdp 5001:5 create //sample LDP MPLS LSPs
exit
  mesh-sdp 5005:5 create
exit
  mesh-sdp 5006:5 create
exit
no shutdown
exit
Ethernet-rings and sub-rings offer a way to build a scalable resilient Ethernet transport network. Figure 16 illustrates a hierarchical ring network using PBB where dual homed services are connected to a PBB based Ethernet ring network. The major rings are connected by sub-rings to the top level major ring. These sub-rings require virtual channel and will not work with non-virtual channel. Ring flushing is contained to major rings, or in the case of a sub-ring link or node failure, to the sub-ring and the directly attached major rings.

---

**Lag Support**

Ethernet-rings support LAG on Ethernet rings SAPS. However, the use of LAG impact the response time for resiliency. In many cases, the use of multiple ring instances each on a single link may be more suitable from a resiliency and QoS standpoint than using LAG on Ethernet rings in a given topology. If sub 100ms response is not required, LAG is an option for Ethernet-rings.
OAM Considerations

Ethernet CFM is enabled by configuring MEPs on each individual path under an Ethernet ring. Only down MEPs can be configured on each of them and optionally, CCM sessions can be enabled to monitor the liveliness of the path using interval of 10 or 100 msec. Different CCM intervals can be supported on the path a and path b in an Ethernet ring. CFM is optional if hardware supports Loss of Signal (LOS) for example, which is controlled by configuring `no-ccm-enable`.

Up MEPs on service SAPs which multicast into the service and monitor the active path may be used to monitor services.

When Ethernet ring is configured on two ports located on different XMAs, the SAP queues and virtual schedulers will be created with the actual parameters on each XMA.

Ethernet ring CC messages transmitted over the SAP queues using the default egress QoS policy will use NC (network class) as a forwarding class. If user traffic is assigned to the NC forwarding class, it will compete for the same bandwidth resources with the Ethernet CCMs. As CCM loss could lead to unnecessary switching of the Ethernet ring, congestion of the queues associated with the NC traffic should be avoided. The operator must configure different QoS Policies to avoid congestion for the CCM forwarding class by controlling the amount of traffic assigned into the corresponding queue.

Details of the Ethernet ring applicability in the services solution can be found in the respective Layer 2 sections of the Services Guide.

Support Service and Solution Combinations

The Ethernet rings are supported Layer 2 service, VPLS, I-VPLS, R-VPLS and B-VPLS instances. The following considerations apply:

- Only ports in access mode can be configured as Ethernet-ring paths. The ring ports can be located on the same or different XCMs or XMAs.
- Dot1q and QinQ ports are supported as Ethernet-ring path members.
- A mix of regular and multiple Ethernet-ring SAPs and pseudowires can be configured in the same services.
Internal Objects Created for L2TP and NAT

Some services such as L2TP LNS (L2TP Network Server) and NAT (Network Address Translation) automatically create service objects for internal use. In particular, an IES service with ID 2147483648 is created. In that service, or in configured VPRN services, service objects such as interfaces, SAPs and related objects can be automatically created for internal use.

Named objects reserved for internal use have a name that starts with “_tmnx_”. Objects with a numeric identifier created for internal use have an identifier from a reserved range.

The general rules for objects reserved for internal use:

- Will appear in CLI show commands and MIB walks output;
- Will appear in the output of `info detail` commands but will never be in the output of `admin save [detail]`.

It may be possible to enter the CLI node of such an object, but it is not possible to change anything. It may also be possible to set the value of one of its objects to the current value with SNMP, but it will never be possible to change any value.
**Service Creation Process Overview**

Figure 17 displays the overall process to provision core and services.

Figure 17: Service Creation and Implementation Flow
Deploying and Provisioning Services

The service model provides a logical and uniform way of constructing connectivity services. The basic steps for deploying and provisioning services can be broken down into three phases.

Phase 1: Core Network Construction

Before the services are provisioned, the following tasks should be completed:

- Build the IP or IP/MPLS core network.
- Configure routing protocols.
- Configure MPLS LSPs (if MPLS is used).
- Construct the core SDP service tunnel mesh for the services.

Phase 2: Service Administration

Perform preliminary policy and SDP configurations to control traffic flow, operator access, and to manage fault conditions and alarm messages, the following tasks should be completed:

- Configure group and user access privileges.
- Build templates for QoS, filter and/or accounting policies needed to support the core services.

Phase 3: Service Provisioning

- Provision customer account information.
- If necessary, build any customer-specific QoS, filter or accounting policies.
- Provision the services on the 7950 XRS-Series routers by defining SAPs, binding policies to the SAPs, and then binding the service to appropriate SDPs as necessary. Refer to Configuring Customers on page 84 and Configuring an SDP on page 87.
Configuration Notes

This section describes service configuration caveats.

General

Service provisioning tasks can be logically separated into two main functional areas, core tasks and tasks and are typically performed prior to provisioning a service.

Core tasks include the following:

- Create customer accounts
- Create template QoS, filter, scheduler, and accounting policies
- Create SDPs

Service tasks include the following:

- Create Epipe, IES, Ipipe, VPLS or VPRN services.
- Bind SDPs
- Configure interfaces (where required) and SAPs
- Create exclusive QoS and filter policies
Configuring Global Service Entities with CLI

This section provides information to create accounts and configure Service Distribution Points (SDPs) using the command line interface.

Topics include:

- Service Model Entities on page 81
- Configuring Customers on page 84
  - Configuring Multi-Service-Sites on page 86
- Configuring an SDP on page 87
- Service Management Tasks on page 149

Service Model Entities

The Alcatel-Lucent service model uses logical entities to construct a service. The service model contains four main entities to configure a service.

- SDPs on page 87
- Services:
  - Ethernet Pipe (Epipe) Services on page 246
  - VPLS on page 651
  - IES on page 1081
- Service Access Points (SAPs)
  - Ethernet Pipe (Epipe) Services on page 246
  - VPLS SAP on page 668
  - IES SAP on page 1086
Basic Configuration

The most basic service configuration must have the following:

- A customer ID
- A service type
- A service ID

An optional service name can also be configured in addition to the service ID. Service names are optional. All services are required to assign a service ID to initially create a service. However, either the service ID or the service name can be used to identify and reference a given service once it is initially created.

- A SAP identifying a port and encapsulation value
- An interface (where required) identifying an IP address, IP subnet, and broadcast address
- For distributed services: an associated SDP

The following example provides an Epipe service configuration displaying the SDP and Epipe service entities. SDP ID 2 was created with the far-end node 10.10.10.104. Epipe ID 6000 was created for customer ID 6 which uses the SDP ID 2.

```
A:ALA-B>config>service# info detail
#------------------------------------------
...  
sdp 2 gre create
    description "GRE-10.10.10.104"
    far-end 10.10.10.104
    signaling tldp
    no vlan-vc-etype
    keep-alive
    path-mtu 4462
    keep-alive
        shutdown
        hello-time 10
        hold-down-time 10
        max-drop-count 3
        timeout 5
        no message-length
    exit
    no shutdown
    exit
...
epipe 6000 customer 6 vpn 6000 create
    service-name “customer-ABC-NW” (R8.0)
    service-mtu 1514
    sap 1/1/2:0 create
        no multi-service-site
        ingress
            no scheduler-policy
            qos 1
        exit
    egress
```
no scheduler-policy
qos 1
exit
no collect-stats
no accounting-policy
no shutdown
exit
spoke-sdp 2:6111 create
  ingress
    no vc-label
    no filter
  exit
  egress
    no vc-label
    no filter
  exit
  no shutdown
  exit
  no shutdown
  exit
...
#------------------------------------------
A:ALA-B>config>service#
Common Configuration Tasks

This section provides a brief overview of the tasks that must be performed to configure a customer account and an SDP.

Configuring Customers

The most basic customer account must have a customer ID. Optional parameters include:

- Description
- Contact name
- Telephone number
- Multi-service site

Customer Information

Use the following CLI syntax to create and input customer information:

**CLI Syntax:**

```
config>service# customer customer-id create
    contact contact-information
    description description-string
    phone phone-number
```
The following displays a basic customer account configuration.

A:ALA-12>config>service# info
-------------------------------------------
...  
customer 5 create
    description "Alcatel Customer"
    contact "Technical Support"
    phone "650 555-5100"
    exit
...  
-------------------------------------------
A:A:ALA-12>config>service#
Configuring Multi-Service-Sites

Multi-service sites create a virtual scheduler hierarchy and making it available to queues on multiple Service Access Points (SAPs). The ingress and egress scheduler-policy commands on the SAP are mutually exclusive with the SAP multi-service-site command. The multi-service customer site association must be removed from the SAP before local scheduler polices may be applied.

After a multi-service site is created, it must be assigned to a chassis slot or port. Use the following CLI syntax to configure customer multi-service sites.

**CLI Syntax:**
```
cfg>service# customer customer-id
    multi-service-site customer-site-name
        assignment {port port-id | card slot}
        description description-string
        egress
            agg-rate-limit agg-rate
            scheduler-policy scheduler-policy-name
        ingress
            scheduler-policy scheduler-policy-name
        tod-suite tod-suite-name
```

The following displays a customer’s multi-service-site configuration.

```
A:ALA-12>config>service# info
-------------------------------------------
..  customer 5 create
    multi-service-site "EastCoast" create
        assignment card 4
        ingress
            scheduler-policy "alpha1"
        exit
    exit
    multi-service-site "WestCoast" create
        assignment card 3
        egress
            scheduler-policy "SLA1"
        exit
    exit
    description "Alcatel Customer"
    contact "Technical Support"
    phone "650 555-5100"
    exit
..  -------------------------------------------
A:ALA-12>config>service#
```
Configuring an SDP

The most basic SDP must have the following:

- A locally unique SDP identification (ID) number.
- The system IP address of the originating and far-end routers.
- An SDP encapsulation type, either GRE or MPLS.

SDP Configuration Tasks

This section provides a brief overview of the tasks that must be performed to configure SDPs and provides the CLI commands.

Consider the following SDP characteristics:

- SDPs can be created as either GRE or MPLS.
- Each distributed service must have an SDP defined for every remote router to provide VLL, VPLS, and VPRN services.
- A distributed service must be bound to an SDP. By default, no SDP is associated with a service. Once an SDP is created, services can be associated to that SDP.
- An SDP is not specific or exclusive to any one service or any type of service. An SDP can have more than one service bound to it.
- The SDP IP address must be a 7950 SR system IP address.
- In order to configure an MPLS SDP, LSPs must be configured first and then the LSP-to-SDP association must be explicitly created.
- In the SDP configuration, automatic ingress and egress labeling (targeted LDP) is enabled by default. Ingress and egress VC labels are signaled over a TLDP connection between two 7950 SR routers.

Note that if signaling is disabled for an SDP, then services using that SDP must configure ingress and egress vc-labels manually.

To configure a basic SDP, perform the following steps:

1. Specify an originating node.
2. Create an SDP ID.
3. Specify an encapsulation type.
4. Specify a far-end node.
Configuring an SDP

Use the following CLI syntax to create an SDP and select an encapsulation type. If you do not specify GRE or MPLS, the default encapsulation type is GRE.

**NOTE**: When you specify the far-end ip address, you are creating the tunnel. In essence, you are creating the path from Point A to Point B. When you configure a distributed service, you must identify an SDP ID. Use the show service sdp command to display the qualifying SDPs.

When specifying MPLS SDP parameters, you must specify an LSP or enable LDP. There cannot be two methods of transport in a single SDP except if the mixed-lsp option is selected. If an LSP name is specified, then RSVP is used for dynamic signaling within the LSP.

LSPs are configured in the `config>router>mpls` context. See the OS MPLS Guide for configuration and command information.

Use the following CLI syntax to create a GRE SDP or an MPLS SDP:

**CLI Syntax:**

```
config>service>sdp  sdp-id [gre | mpls] create
adv-mtu-override
derscription description-string
far-end ip-address
keep-alive
   hello-time seconds
   hold-down-time seconds
   max-drop-count count
message-length octets
timeout timeout
no shutdown
   ldp (only for MPLS SDPs)
   lsp lsp-name [lsp-name](only for MPLS SDPs)
path-mtu octets
signaling {off | tldp}
no shutdown
```
The following displays a GRE SDP, an LSP-signalled MPLS SDP, and an LDP-signalled MPLS SDP configuration.

A:ALA-12>config>service# info
-------------------------------------------
... sdp 2 create
description "GRE-10.10.10.104"
far-end 10.10.10.104
keep-alive
   shutdown
exit
no shutdown
exit
sdp 8 mpls create
description "MPLS-10.10.10.104"
far-end 10.10.10.104
lsp "to-104"
keep-alive
   shutdown
exit
no shutdown
exit
sdp 104 mpls create
description "MPLS-10.10.10.94"
far-end 10.10.10.94
ldp
keep-alive
   shutdown
exit
no shutdown
exit
...
-------------------------------------------
A:ALA-12>config>service#
Configuring a Mixed-LSP SDP

Use the following command to configure an SDP with mixed-LSP mode of operation:

```plaintext
config>service>sdp mpls>mixed-lsp-mode
```

The primary is backed up by the secondary. Two combinations are possible: primary of RSVP is backed up by LDP and primary of LDP is backed up by 3107 BGP.

The `no` form of this command disables the mixed-LSP mode of operation. The user first has to remove one of the LSP types from the SDP configuration or the command will fail.

The user can also configure how long the service manager must wait before it must revert the SDP to a higher priority LSP type when one becomes available by using the following command:

```plaintext
config>service>sdp mpls>mixed-lsp-mode>sdp-revert-time seconds
```

A special value of the timer dictates that the SDP must never revert to another higher priority LSP type unless the currently active LSP type is down:

```plaintext
config>service>sdp mpls>mixed-lsp-mode>sdp-revert-time infinite
```

The BGP LSP type is allowed. The `bgp-tunnel` command can be configured under the SDP with the `lsp` or `ldp` commands.

**Mixed-LSP Mode of Operation**

The mixed LSP SDP allows for a maximum of two LSP types to be configured within an SDP. A primary LSP type and a backup LSP type. An RSVP primary LSP type can be backed up by an LDP LSP type.

An LDP LSP can be configured as a primary LSP type which can then be backed up by a BGP LSP type.

At any given time, the service manager programs only one type of LSP in the linecard that will activate it to forward service packets according to the following priority order:

1. RSVP LSP type. Up to 16 RSVP LSPs can be entered by the user and programmed by the service manager in ingress linecard to load balance service packets. This is the highest priority LSP type.

2. LDP LSP type. One LDP FEC programmed by service manager but ingress linecard can use up to 16 LDP ECMP paths for the FEC to load balance service packets when ECMP is enabled on the node.

3. BGP LSP type. One RFC 3107-labeled BGP prefix programmed by the service manager. The ingress linecard can use more than one next-hop for the prefix.
In the case of the RSVP/LDP SDP, the service manager will program the NHLFE(s) for the active LSP type preferring the RSVP LSP type over the LDP LSP type. If no RSVP LSP is configured or all configured RSVP LSPs go down, the service manager will re-program the linecard with the LDP LSP if available. If not, the SDP goes operationally down.

When a higher priority type LSP becomes available, the service manager reverts back to this LSP at the expiry of the sdp-revert-time timer or the failure of the currently active LSP, whichever comes first. The service manager then re-programs the linecard accordingly. If the infinite value is configured, then the SDP reverts to the highest priority type LSP only if the currently active LSP failed.

Note however, that LDP uses a tunnel down damp timer which is set to three seconds by default. When the LDP LSP fails, the SDP will revert to the RSVP LSP type after the expiry of this timer. For an immediate switchover this timer must be set to zero. Use the configure>router>ldp>tunnel-down-damp-time command.

If the value of the sdp-revert-time timer is changed, it will take effect only at the next use of the timer. Any timer which is outstanding at the time of the change will be restarted with the new value.

If class based forwarding is enabled for this SDP, the forwarding of the packets over the RSVP LSPs will be based on the FC of the packet as in current implementation. When the SDP activates the LDP LSP type, then packets are forwarded over the LDP ECMP paths using the regular hash routine.

In the case of the LDP/BGP SDP, the service manager will prefer the LDP LSP type over the BGP LSP type. The service manager will re-program the linecard with the BGP LSP if available otherwise it brings down the SDP operationally.

Also note the following difference in behavior of the LDP/BGP SDP compared to that of an RSVP/LDP SDP. For a given /32 prefix, only a single route will exist in the routing table: the IGP route or the BGP route. Thus, either the LDP FEC or the BGP label route is active at any given time. The impact of this is that the tunnel table needs to be re-programmed each time a route is deactivated and the other is activated. Furthermore, the SDP revert-time cannot be used since there is no situation where both LSP types are active for the same /32 prefix.
Ethernet Connectivity Fault Management (ETH-CFM)

Ethernet Connectivity Fault Management (ETH-CFM) is defined in two similar standards: IEEE 802.1ag and ITU-T Y.1731. They both specify protocols, procedures, and managed objects to support transport fault management, including discovery and verification of the path, detection and isolation of a connectivity fault for each Ethernet service instance. CFM functionalities are supported on SR and ESS platforms.

The configuration is split into multiple areas. There is the base ETH-CFM configuration which defines the different Management constructs and administrative elements. This is performed in the ETH-CFM context. The individual management points are configure within the specific service contexts in which they are applied.

The different service types support a subset of the features from the complete ETH-CFM suite.

ETH-CC used for continuity is available to all MEPs configured within a service and all facility MEPs.

The troubleshooting tools ETH-LBM/LBR, LTM/LTR ETH-TST defined by the IEEE 802.1ag specification and the ITU-T Y.1731 recommendation are applicable to all MEPs (MIPs where appropriate).

The advanced notification function AIS defined by the ITU-T Y.1731 is supported on Epipe services and may be terminated by a MEP on a Layer 3 service interface.

The advanced performance functions, 1DM, DMM/DMR and SLM/SLR are supported on all service MEPs, not on facility MEPs.

For a description of the individual features and functions that are supported refer to the applicable OAM Diagnostics Guide.

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Callout</th>
</tr>
</thead>
<tbody>
<tr>
<td>1DM</td>
<td>One way Delay Measurement (Y.1731)</td>
</tr>
<tr>
<td>AIS</td>
<td>Alarm Indication Signal</td>
</tr>
<tr>
<td>CCM</td>
<td>Continuity check message</td>
</tr>
<tr>
<td>CFM</td>
<td>Connectivity fault management</td>
</tr>
<tr>
<td>DMM</td>
<td>Delay Measurement Message (Y.1731)</td>
</tr>
<tr>
<td>DMR</td>
<td>Delay Measurement Reply (Y.1731)</td>
</tr>
<tr>
<td>LBM</td>
<td>Loopback message</td>
</tr>
<tr>
<td>LBR</td>
<td>Loopback reply</td>
</tr>
<tr>
<td>Acronym</td>
<td>Callout (Continued)</td>
</tr>
<tr>
<td>---------</td>
<td>---------------------</td>
</tr>
<tr>
<td>LTM</td>
<td>Linktrace message</td>
</tr>
<tr>
<td>LTR</td>
<td>Linktrace reply</td>
</tr>
<tr>
<td>ME</td>
<td>Maintenance entity</td>
</tr>
<tr>
<td>MA</td>
<td>Maintenance association</td>
</tr>
<tr>
<td>MA-ID</td>
<td>Maintenance association identifier</td>
</tr>
<tr>
<td>MD</td>
<td>Maintenance domain</td>
</tr>
<tr>
<td>MEP</td>
<td>Maintenance association end point</td>
</tr>
<tr>
<td>MEP-ID</td>
<td>Maintenance association end point identifier</td>
</tr>
<tr>
<td>MHF</td>
<td>MIP half function</td>
</tr>
<tr>
<td>MIP</td>
<td>Maintenance domain intermediate point</td>
</tr>
<tr>
<td>OpCode</td>
<td>Operational Code</td>
</tr>
<tr>
<td>RDI</td>
<td>Remote Defect Indication</td>
</tr>
<tr>
<td>TST</td>
<td>Ethernet Test (Y.1731)</td>
</tr>
<tr>
<td>SLM</td>
<td>Synthetic Loss Message (Y.1731)</td>
</tr>
<tr>
<td>SLR</td>
<td>Synthetic Loss Reply (Y.1731)</td>
</tr>
</tbody>
</table>
ETH-CFM capabilities may be deployed in many different Ethernet service architectures. The Ethernet based SAPs and SDP bindings provide the endpoint on which the management points may be created. The basic functions can be used in different services, VPLS, Ipipe, Epipe and even in IES, VPRN and the base router instance interfaces. Of course, Layer 3 services are boundaries for Layer 2 ETH-OAM functions. The ETH-CFM functionality is also applicable to broadband access networks. Two models of broadband access are shown below to illustrate how ETH-CFM could be deployed in these cases. (Figure 18 and Figure 19).
As shown in Figure 18 and Figure 19, the following functions are supported:

- CFM can be enabled or disabled on a SAP or SDP bindings basis.
- The eight ETH-CFM levels are suggested to be broken up numerically between customer 7-5, service provider 4-3 and Operator 2-1. Level 0 is meant to monitor direct connections without any MIPs and should be reserved for port-based facility MEPs. These can be configured, deleted or modified.
- Up and/or down MEP with an MEP-ID on a SAP and SDP binding for each MD level can be configured, modified, or deleted. Each MEP is uniquely identified by the MA-ID, MEP-ID tuple.
  - MEP creation on a SAP is allowed only for Ethernet ports (with null, q-tags, qinq encapsulations).
- MIP creation on a SAP and SDP binding for each MD level can be enabled and disabled. MIP creation is automatic or manual when it is enabled. When MIP creation is disabled for an MD level, the existing MIP is removed.
  - MIP creation is not supported on mesh SDP bindings.
Facility MEPs

Facility MEPs have been introduced to improve scalability, reduce operational overhead, and provide fate sharing without requiring service MEPs. This allows for fault notification for Epipe services that share a common transport. Facility MEPs recognize failure based solely on ETH-CFM detection mechanisms.

There are a total of four facility MEPs, as described below:

- Port (physical) — Detects port failure where LoS may be hidden by some intervening network
- LAG (logical) — Validates the connectivity of the LAG entity
- Tunnel (logical) — Enables fate sharing of a MEP configured on a QinQ encapsulated access LAG and outer VLAN-ID.
- Router IP Interface (logical) — Validates the Layer 2 connectivity between IP endpoints (troubleshooting only – no CCM functions)

In general, a Facility MEP detects failure conditions using ETH-CFM at the Ethernet Transport layer. The detection is based solely on the MEP entering a fault state as a result of ETH-CC. Conditions outside the scope of ETH-CFM do not directly influence the state of the MEP. However, these outside influences have indirect influence. For example, upon a failure of a port, CCM messages cannot reach the destination. This condition causes the MEP to enter a fault state after the 3.5*interval expires, with the only exception being the acceptance of AIS on a Tunnel MEP. AIS received on all other facilities MEPs are discarded silently when normal level matching targets the local facility MEP.

Facility MEPs are supported as part of a down MEP only. Facility MEPs validate the point to point Ethernet transport between two end points. Facility MEPs do not validate switching functions that are not part of the point to point Ethernet transport. Instead, service MEPs validate switching functions that are not part of the point to point Ethernet transport.

A facility MEP allows for the scaling improvements using fate sharing and leveraging OAM mapping. The OAM mapping functions are part of the fault propagation functions and allow ETH-CFM to move from alarms only to network actions. Service based MEPs are not required to generate AIS in reaction to a facility MEP fault. OAM mapping and fault generation, either the R8.0 function or the AIS function as part of a facility MEP) are only available on Epipe services. There is no equivalent AIS generation as part of the facility fault for VPLS, IES, and VPRN. There is no service MEP required to have the SAP transition in the VPLS, IES, and VPRN service context. Normal SAP transition functions do not occur when these services are configured to accept the tunnel fault, or in reaction to a facility fault, where the underlying port or LAG transitions the SAP.

Note: Do not exceed the platform-specific scaling limits. Since a single facility fault may trigger the generation of many service level faults, ensure the specific ETH-CFM processing power of the
network element and any configured rate controlling features for the service are not exceed. Exceeding the network element scaling properties may lead to OAM packet loss during processing and result in undesirable behavior.

The implementation of facility MEPs must adhere to all platform-specific specifications. For example, sub-second enabled CCM MEPs are supported on port based MEPs. However, any platform restrictions preventing the sub-second enabled MEPs override this capability and require the operator to configure CCM intervals that are supported for that specific platform.

Facility MEPs are created in the same manner as service MEPs, both related to the ETH-CFM domain and association. However, the association used to build the facility MEP does not include a bridge-identifier. The CLI ensures that a bridge id is not configured when the association is applied to a facility MEP.

Service MEPs and Facility MEPs may communicate with each other, as long as all the matching criteria are met. Since facility MEPs use the standard ETH-CFM packets, there is nothing contained in the packet that would identify an ETH-CFM packet as a facility MEP or Service MEP.

Only facility MEPs of 1 second and above are supported on the ports that are involved in an Eth-Ring (G.8032).
Common Actionable Failures

It is important to note that AIS operates independently from the **low-priority-defect** setting. The **low-priority-defect** setting configuration parameter affects only the ETH-CFM fault propagation and alarming outside the scope of AIS. Any fault in the MEP state machine generates AIS when it is configured. Table 3 illustrates the ETH-CC defect condition groups, configured low-priority-defect setting, priority and defect as it applies to fault propagation.

Table 3: Defect Conditions and Priority Settings

<table>
<thead>
<tr>
<th>Defect</th>
<th>Low Priority Defect</th>
<th>Description</th>
<th>Causes</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>DefNone</td>
<td>n/a</td>
<td>No faults in the association</td>
<td>Normal operations</td>
<td>n/a</td>
</tr>
<tr>
<td>DefRDICCM</td>
<td>allDef</td>
<td>Remote Defect Indication</td>
<td>Feedback mechanism to inform unidirectional faults exist. It provides the feedback loop to the node with the unidirectional failure conditions</td>
<td>1</td>
</tr>
<tr>
<td>DefMACStatus (default)</td>
<td>macRemErrXcon</td>
<td>MAC Layer</td>
<td>Remote MEP is indicating a remote port or interface not operational.</td>
<td>2</td>
</tr>
<tr>
<td>DefRemoteCCM</td>
<td>remErrXon</td>
<td>No communication from remote peer.</td>
<td>MEP is not receiving CCM from a configured peer. The timeout of CCM occurs at 3.5x the local CC interval. As per the specification, this value is not configurable.</td>
<td>3</td>
</tr>
<tr>
<td>DefErrorCCM</td>
<td>errXcon</td>
<td>Remote and local configures do not match required parameters.</td>
<td>Caused by different interval timer, domain level issues (lower value arriving at a MEP configured with a higher value), MEP receiving CCM with its MEPID</td>
<td>4</td>
</tr>
<tr>
<td>DefXconn</td>
<td>Xcon</td>
<td>Cross Connected Service</td>
<td>The service is receiving CCM packets from a different association. This could indicate that two services have merged or there is a configuration error on one of the SAP or bindings of the service, incorrect association identification.</td>
<td>5</td>
</tr>
</tbody>
</table>
A facility MEP may trigger two distinct actions as a result of fault. Epipe services generate AIS that have been configured to do so as a result of a failure. The level of the AIS is derived from the facility MEP. Multiple client-meg-levels can be configured under the facility MEP to allow for operational efficiency in the event a change is required. However, only the lowest AIS level is generated for all the linked and applicable services. VPLS, IES and VRPN SAPs transition the SAP state that are configured to react to the facility MEP state. In addition, Epipe services may also take advantages of OAM and mapping functions.

Before implementing facility MEPs, it is important to understand the behavior of AIS and Fault propagation. Alcatel-Lucent advises that you strongly considered the following recommendations listed below before enabling or altering the configuration of any facility MEP. These steps must be tested on each individual network prior to building a maintenance operational procedure (MOP).

- Do not configure AIS on the facility MEP until the ETH-CCM has been verified. For instance, when a local MEP is configured with AIS prior to the completion of the remote MEP, the AIS is immediately generated when the MEP enters a fault state for all services linked to that facility MEP.
- Disable the client-meg-level configuration parameter when changes are being made to existing functional facility MEPs for AIS. Doing this stops the transmit function but maintains the ability to receive and understand AIS conditions from the network.
- Set the low-priority-defect parameter to noXconn in order to prevent the MEP from entering a defect state, triggering SAP transitions and OAM mapping reactions.

It is important to consider and select what types of fault conditions causes the MEP to enter a faulty state when using fault propagation functions.

The ccm-hold-timers supported on port-based MEPs configured with a sub-second interval. The ccm-hold-timers prevents the MEP from entering a failed state for 3.5 times the CCM interval plus the additional hold timer.
General Detection, Processing and Reaction

All Facility MEPs that support CCM functions must only have one remote MEP peer. Facilities MEPs validate point-to-point logical or physical Ethernet transports. Configure service MEPs if multipoint-service validation is required.

There are three distinct functions for a Facility MEP:

- General Detection: Determines that a fault has occurred. In this case, the MEP performs its normal functions such as: recognizing the fault condition, maintaining the local errors and reporting based on low-priority-setting, and taking no further action. This is the default.

- Fault Processing: By default, there is no action taken as a result of a MEP state machine transition beyond alarming. In order to take action which may include a SAP operational state change, generation of AIS, or fault propagation and mapping, the appropriate facility fault configuration parameter must be configured and enabled. The general reaction to a fault is described below. More details are including the section describing the functions of the individual facility MEPs.

  → Port—Affects link operational status of the port. Facility failure changes the operational state to Link Up. This indicates that the port has been brought down as a result of OAM MEP Fault. This operational state has the equivalent function to port down condition.

  → LAG—Affects link operational status of the LAG. Facility failure changes the operational state of the LAG to DOWN. This indicates that the LAG has been brought down as a result of OAM MEP Fault.

  → Tunnel MEP—Enters faulty state and will further impact the operational state of the SAPs linked to the tunnel MEP state.

    - Epipe SAP remains operationally up, SAP's flag set to `OamTunnelMEPFault`
    - Ipipe SAP remains operationally up, SAP's flag set to `OamTunnelMEPFault`
    - VPLS, IES and VPLS SAPs transition to operationally down, the SAP's flag is set to `OamTunnelMEPFault`

      SAP operational states and flags are affect only by the `tunnel-fault` configuration option.

  → Router IP Interface— Affects operational status of the IP Interface.
• Propagation: Services appropriately linked to the Facility MEP take the following service specific actions:
  → Epipe generates AIS or use Fault Propagation and OAM mappings.
  → VPLS does not propagate fault using AIS unless service-based MEPs are configured and contain MEP-specific AIS configuration. SAP transitions will occur when the facility MEP failure is recognized by the service.
  → IES and VPRN, as Layer 3 functions, act as boundaries for Layer 2 fault processing. No propagation functions occur beyond what is currently available as part of fault propagation, SAP down.

• AIS-enable configuration options: Epipe services support the ais-enable configuration option under the SAP hierarchy level. This structure, outside of the MEP context, creates a special link between the Epipe service SAP and the facility MEP. If a facility MEP enters a fault state, all Epipe service SAPs with this configuration generate lowest-level AIS at the level configured under the facility MEP. As with fault propagation, AIS generation is restricted to Epipe services only. The actions taken by the other services is described in more detail in the relevant facility MEP sections.

NOTE: Facility MEPs do not support the generation of AIS to an explicitly configured endpoint. An explicitly configure endpoint abstracts multiple endpoints within its context, for example, pseudowire (PW) redundancy. Although the linkage of a facility MEP to an Epipe and AIS generation triggered as a result of the facility MEP failure can be configured AIS generation is not supported and will be unpredictable. When an explicit endpoint is configured service based MEPs are required when AIS generation is the desired behavior.
Port-Based MEP

There is an increase in services that share the same facilities, and that service-based ETH-CFM, although very granular, comes at an operational and scalability cost. Configuring a MEP on a physical port allows ETH-CFM to detect Ethernet transport failures, raise a facility alarm, and perform local fault processing. A facility event is coordinated to the services or functions using the affected port.

Port-based facility MEPs are able to run all supported on-demand and SAA, 802.1ag and ITU-T Y.1731 ETH-CFM functions.

The port-based MEP is intended to validate physical connectivity to the peer MEP, provide on-demand and scheduled troubleshooting, and performance management functions.

Port facility MEPs are advantageous in cases where port-to-port connectivity issues are obscured, similar to the deployment use cases for IEEE 802.3 Clause 57 – Operation, Administration and Maintenance (formerly 802.3ah). Clause 57 specification limits the transmit rate to 10pps, or a send rate of 100ms. In order to detect port failure conditions between two peers faster, a port-based facility MEP may be configured to utilize the supported sub-second CCM intervals. Also, 1 second and above timers are available for configuration for cases where aggressive timers are not necessary. Note that all platform-specific requirements must be met for the desired interval. Since both ETH-CFM and IEEE 802.3 Clause 57 attempt to control the port state in event of protocol failure, these two functions are mutually exclusive and can not be configured on the same port.

Port-level ETH-CFM PDUs are sent untagged because they are not specific to any service or VLAN. The ETH-CFM packets generated from a port-based facility MEP must use an ETH-CFM level of 0 or 1. Any ETH-CFM PDU that arrives untagged on a port matching the level for the port based facility MEP will be terminated and processed by the port based MEP.

Do not use MEPs configured with level 0 to validate logical transport or services. Consideration should be given to blocking all non-customer (5-7) levels at the entry point of the network.

It is not expected that faults from other parts of the network will be propagate and terminated on a port-based facility MEP. This type of facility MEP provides a one-to-one validation with a single remote MEP across on a physical port, allowing locally detected faults to be propagated to the endpoints of the network.

A physical port may only have a single port based facility MEP. Since the purpose of the MEP is to control the port state, more than one is not required per port. The MEP must be configured with the direction-down option.

Port based MEPs are supported in both the IEEE 802.1ag and ITU-T Y.1731 contexts. Therefore, the Y.1731 context must be configured in order to run functions beyond those that are described as part of the IEEE 802.1ag specification.
When a port enters the link up operational state due to ETH-CFM, the MEP continues to transmit and received in order to properly clear the condition. However, when the port fails for reasons that are not specific to ETH-CFM, it stops transmit and receive functions until the condition is cleared. This is different than the behavior of a service MEP, because facility MEPS only supports Down MEPS, while some service-based MEPS support UP and Down MEPS. In the case of UP MEPS, a single port failure may not prevent all the CCMs from egressing the node. So the operational method for service-based MEPS remains the same: continuing to increase the counter for CCM transmit in the event of port failure, regardless of the reason. The transmit ETH-CCM counters do not apply to sub-second CCM-enabled MEPS.

There are two types of port in the context of port-based facility MEPS. The first type are ports that are not part of a LAG, referred to as non-member ports. The second type of ports are ports that are part of a LAG, referred to member ports, and have slightly different reactions to fault. MEPS configured directly on either type of port will act the same. However, a MEP configured on a non-member port and a MEP configured on a member port handle fault propagation differently.

When a port-based facility MEP causes the port to enter the operational state Link Up, normal processing occurs for all higher level functions. If the port is a member port, unless the entire LAG enters a non-operational state, the SAP configured on the LAG remains operational. A facility MEP on a member port has no direct influence on the SAP. The purpose of a facility MEP on a member port is to provide feedback to the LAG. The LAG performs the normal computations in response to a port down condition. A facility MEP configured on a non-member port does have direct control over the SAPs configured on the port. Therefore, when a port fails, all the SAPs transitions to the operation state down. When this occurs, fault may be propagated using AIS for those Epipe services that are AIS-enabled under the SAO. For the services that have MEPS configured on the SAP or the binding, fault propagation occurs. For VPLS, IES and VPRN services, normal reaction to a SAP entering a down state occurs.

When a LAG is administratively shutdown, the member ports are shutdown automatically. As a result, packet reception is interrupted, causing ETH-CFM functions running on physical member ports to lose connectivity. Therefore, the CFM functions on member ports are somewhat tied to the LAG admin status in this case.

It is important to note that LAG convergence time is not affected by a facility MEP on a member port once the port has entered the link up operational state. The ETH-CFM failure of a port-based MEP acts as the trigger to transition the port.

Figure 20 on page 104 provides an example of how an ETH-CFM failure reacts with the various services that share that port. The green Epipe service generates AIS as a result of the port failure using the \texttt{client-meg-level} command configured on the port facility MEP. The multipoint service takes location configured action when the SAP transitions to the down operational state. The blue Epipe service is not affected by the port link up state as a result of ETH-CFM fault.
A debounce function has been implemented to prevent notifying every port state change if a port bounces multiple times within a window. Up to four notifications will be accepted in a three second window. If the third port state is a down state change the fourth will be ignored. If the fourth port state change is a down state change it will be processed. After that no further state changes will be accepted for the duration of the three second timer. This helps ensure that the port is not artificially held in the UP state when it is not operating. Following the processing of that last port state change, the third or fourth, the latest state change will be held and processed at the expiration of the three second hold timer.

**Example: Port-Based MEP Configuration**

The following illustration, Figure 21, provides an example of how port-based MEPs and defect conditions translate into service awareness without service-based MEPs. From the two nodes perspective, they are aware they are directly connected at the port. The two nodes are unaware of any of the cross connections that allow this to occur.
Figure 21: Port-Based MEP Example

Configure port-based MEPS with the `facility-fault` option and `ais-enable client-meg-level` command. When the MEP enters any defect state, an AIS is generated to any Epipe service that has the ais-enable configured under the sap>eth-cfm hierarchy.

NODE1

```
config>eth-cfm# info
----------------------------------------------
domain 10 format none level 0
    association 1 format icc-based name "FacilityPort0"
       ccm-interval 1
       remote-mepid 2
    exit
exit
----------------------------------------------
config>port# info
----------------------------------------------
ethernet
    mode access
    encap-type qinq
    eth-cfm
        mep 1 domain 10 association 1
        ais-enable
        client-meg-level 5
        exit
        facility-fault
        ccm-enable
        mac-address d0:0d:1e:00:00:01
        no shutdown
    exit
exit
exit
no shutdown
----------------------------------------------
config>service>epipe# info
```

SAP 1/1/2:100.31 (ais-enable)
SAP 1/1/10:100.31

SAP 1/1/2:100.31 (ais-enable)
SAP 1/1/10:100.31

= Down MEP

OSGS542
Ethernet Connectivity Fault Management (ETH-CFM)

---
sap 1/1/2:100.31 create
   eth-cfm
   ais-enable
   exit
exit
sap 1/1/10:100.31 create
exit
no shutdown
---

NODE2

config>eth-cfm# info
---
domain 10 format none level 0
   association 1 format icc-based name "FacilityPort0"
   ccm-interval 1
   remote-mepid 1
   exit
exit
---

config>port# info
---
ethernet
   mode access
   encap-type qinq
   eth-cfm
      mep 2 domain 10 association 1
         ais-enable
      client-meg-level 5
      exit
         facility-fault
      ccm-enable
      mac-address d0:0d:1e:00:00:02
      no shutdown
      exit
      exit
      no shutdown
---

config>service>epipe# info
---
sap 1/1/2:100.31 create
   eth-cfm
      ais-enable
   exit
exit
sap 1/1/10:100.31 create
exit
no shutdown
---
There are two different levels of fault to consider: Port State / Operational State driven by the low-priority-defect setting and the generation of AIS driven by any defect state for the MEP, regardless of low-priority-defect.

If the low-priority-defect is left at the default macRemErrXcon setting, then port state may not match on both nodes. If an unidirectional failure is introduced for port-based MEPs, then RDI is received on one of the nodes and the other node would report and react to RemoteCCM (timeout). The RDI defect is below the default low-priority-defect in priority, and the port would remain operationally UP and the port state would remain UP. The MEP that has timed out the peer MEP takes port level action because this defect is higher in priority than the default low-priority-defect. The port state is recorded as Link Up and the Port is operationally down with a Reason Down: ethCfmFault. To avoid this inconsistency, set the low-priority-defect setting to detection unidirectional failures using the allDef option.

The following show commands reveal the condition mentioned above within the network. Node 1 is receiving RDI and Node 2 has timed out its peer MEP.

NODE1

```bash
#show port
===============================================================================
Ports on Slot 1
===============================================================================
| Port | Admin Link Port | Cfg | Oper LAG/ Port | Port | Port | C/QS/S/XFP/ |
| Id   | State          | State | MTU | MTU | Bndl Mode | Encp | Type | MDIMDX |
-------------------------------------------------------------------------------
...snip...
1/1/2 | Up             | Yes | Up | 1522 | 1522 | accs qinq xcme
...snip...
```

```bash
#show port 1/1/2
===============================================================================
Ethernet Interface
===============================================================================
Description : 10/100/Gig Ethernet SFP
Interface : 1/1/2
Link-level : Ethernet
Admin State : up
Oper State : up
Physical Link : Yes
Oper Speed : 1 Gbps
Config Speed : 1 Gbps
Oper Duplex : full
Config Duplex : full
MTU : 1522
...snip...
```

```bash
#show eth-cfm mep 1 domain 10 association 1
===============================================================================
Eth-Cfm MEP Configuration Information
===============================================================================
Md-index : 10
Ma-index : 1
MepId : 1
Port : 1/1/2
Description : {Not Specified}
FngState : fngReset
LowestDefectPri : macRemErrXcon
Direction : Down
Admin : Enabled
CCM-Enable : Disabled
VLAN : 0
ControlMep : False
HighestDefect : none
```
Defect Flags : bDefRDICCM
Mac Address : d0:0d:1e:00:00:01  ControlMep : False
CcmLtmPriority : 7
CcmTx : 1481  CcmSequenceErr : 0
Fault Propagation : disabled  FacilityFault : Notify
MA-CcmInterval : 1  MA-CcmHoldTime : 0ms
Eth-1m Threshold : 3(sec)  MD-Level : 0
Eth-Ais : Enabled  Eth-Ais Rx Ais : No
Eth-Ais Tx Priority* : 7  Eth-Ais Rx Interv* : 1
Eth-Ais Tx Interv* : 1  Eth-Ais Tx Counte* : 3019
Eth-Ais Tx Levels : 5
Eth-Tst : Disabled

# show service sap-using eth-cfm facility

===============================================================================
Service ETH-CFM Facility Information
===============================================================================
SapId SvcId SAP AIS SAP Tunnel SVC Tunnel Fault
-------------------------------------------------------------------------------
1/1/2:100.31 100 Enabled Accept Ignore
-------------------------------------------------------------------------------
No. of Facility SAPs: 1
===============================================================================

NODE2
# show port

===============================================================================
Ports on Slot 1
===============================================================================
Port Admin Link Port Cfg Oper LAG/ Port Port Port C/QS/S/XFP/
Id State State MTU MTU Bndl Mode Encp Type MDIMDX
-------------------------------------------------------------------------------
1/1/2 Up Yes Link Up 1522 1522 - accs qinq xcme

# show port 1/1/2

Ethernet Interface

Description : 10/100/Gig Ethernet SFP
Interface : 1/1/2  Oper Speed : N/A
Link-level : Ethernet  Config Speed : 1 Gbps
Admin State : up  Oper Duplex : N/A
Oper State : down  Config Duplex : full
Reason Down : ethCfmFault
Physical Link : Yes  MTU : 1522

# show eth-cfm mep 2 domain 10 association 1

===============================================================================
Eth-Cfm MEP Configuration Information
===============================================================================
Md-index : 10  Direction : Down
Ma-index : 1  Admin : Enabled
MepId : 2  CCM-Enable : Enabled
Port : 1/1/2  VLAN : 0
### Description
- (Not Specified)

### FngState
- fngDefectReported

### LowestDefectPri
- macRemErrXcon

### Defect Flags
- bDefRemoteCCM

### Mac Address
- d0:0d:1e:00:00:02

### CcmLtmPriority
- 7

### CcmTx
- 5336

### Fault Propagation
- disabled

### MA-CcmInterval
- 1

### Eth-10m Threshold
- 3(sec)

### Eth-Ais:
- Enabled

### Eth-Ais Tx Priority
- 7

### Eth-Ais Tx Interval
- 1

### Eth-Ais Tx Levels
- 5

### Eth-Tst:
- Disabled

---

```
# show service sap-using eth-cfm facility
```

### Service ETH-CFM Facility Information

<table>
<thead>
<tr>
<th>SapId</th>
<th>SvcId</th>
<th>SAP AIS</th>
<th>SAP Tunnel</th>
<th>SVC Tunnel</th>
<th>Fault</th>
<th>Fault</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1/2:100.31</td>
<td>100</td>
<td>Enabled</td>
<td>Accept</td>
<td>Ignore</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

No. of Facility SAPs: 1
LAG Based MEP

LAG bundled ports provide both protection and scalability. Down MEPS configured on a LAG validate the connectivity of the LAG. Failure of this MEP causes the LAG to enter an operational down state. SAPs connected to the operationally down LAG transitions to operationally down. This triggers the configured reaction and processing similar to that of the port-based facility MEP. AIS is generated for those Epipe services with AIS enabled under the SAP. Local processing occurs for VPLS, IES and VPRN services that have experienced the SAP failure as a result of the LAG based SAP. Furthermore, fault propagation is invoked for any SAP with fault propagation operations enabled as a result of the failed LAG based SAP. LAG-based MEPS must be configured with a direction down.

LAG ETH-CFM PDUs are sent untagged because they are not specific to any service or VLAN. When running the combination of LAG-based MEPS and port-based MEPS, domain-level nesting rules must be adhered to for proper implementation, and is enforced by the CLI on the local node. As stated earlier, do not configure logical non-port-based MEPS, including service-based MEPS, to use level 0 for the ETH-CFM packets.

LAG-based MEPS are supported in both the IEEE 802.1ag and ITU-T Y.1731 contexts. Therefore, the Y.1731 context must be configured in order to run functions beyond those that are described as part of the IEEE 802.1ag standard. Since the recognition of fault is determined entirely by the ETH-CFM function, timeout conditions for the MEP occurs in 3.5 times the CCM interval. The LAG admin state or other failures that causes the LAG to completely fail, does not directly influence the MEP. The state of the MEP can only be influenced by the ETH-CFM function, specifically ETH-CC.

Since the LAG-based MEP selects a single member port to forward ETH-CFM packets, port-based facilities MEPS must be deployed to validate the individual member ports. Functional tests that require the ability to test individual member ports need to be performed from the port-based MEPS. The LAG-based MEPS validate only the LAG entity.

Figure 22 on page 111, provides an example how an ETH-CFM failure reacts with the various services that share that LAG. There is only one way the LAG state can trigger the propagation of failure, and that is using ETH-AIS. The carrier must enable CCM at the LAG level and a ETH-CCM defect condition exists. The red Epipe service generates AIS as a result of the LAG failure using the client-meg-level parameter configured on the LAG facility MEP. The green multipoint service takes location-configured action when the SAP transitions to the down operational state.
LAG-based MEP are supported for MultiChassis LAG (MC-LAG) configurations.

A LAG facility MEP must not be configured with **facility-fault** when it is applied to an MC-LAG. Traffic will black hole when the LAG Facility MEP enters a defect state. The LAG enters an operational down state but the MC-LAG does not switch over to the peer node. This restriction does not include Tunnel Facility MEPs which are applied to a LAG with an outer VLAN. Tunnel facility MEPs do not control the operational state of the LAG because they are outer VLAN specific.
Example: LAG MEP Configuration

Figure 23 uses a port-based MEP to validate port-to-port connectivity.

With the introduction of the LAG, the port no longer has direct control over the services SAPs. The ais-enable command has been disabled from the port for this reason. The low-priority-defect condition has been modified to react to all defect conditions “allDef”, avoiding the unidirectional issue demonstrated in the previous port-based MEP example. A LAG MEP is built on top the LAG with the facility-fault option and ais-enable command with the associated client-meg-level. This allows the Epipe services to generate AIS when the LAG MEP enters any defect condition. This example introduce the use of a VPLS service. VPLS, IES and VPRN services do not support the generation of AIS as a result of a facility MEP failure. However, all service SAPs which correspond to the failed facility will transition to a down state. Epipe service also generates AIS in this example.

NODE1

config>eth-cfm# info
--------------------------------------------
domain 1 format none level 1
  association 1 format icc-based name "FacilityLag01"
    ccm-interval 1
    remote-mepid 22
  exit
exit
domain 10 format none level 0
association 1 format icc-based name "FacilityPort0"
    ccm-interval 1
    remote-mepid 2
exit
exit

config>port# info
----------------------------------------------
ethernet
    mode access
    encap-type qinq
    eth-cfm
    mep 1 domain 10 association 1
    facility-fault
    ccm-enable
    low-priority-defect allDef
    mac-address d0:0d:1e:00:00:01
    no shutdown
exit
exit
autonegotiate limited
exit
no shutdown

config>lag# info
----------------------------------------------
mode access
encap-type qinq
eth-cfm
mep 11 domain 1 association 1
ais-enable
client-meg-level 5
exit
ccm-enable
facility-fault
low-priority-defect allDef
no shutdown
exit
port 1/1/2
no shutdown

config>service# info
----------------------------------------------
customer 1 create
description "Default customer"
exit
epipe 100 customer 1 create
sap 1/1/10:100.31 create
exit
sap lag-1:100.31 create
eth-cfm
   ais-enable
exit
exit
no shutdown
exit
vpls 200 customer 1 create
stp
    shutdown
exit
sap 1/1/10:200.20 create
exit
sap lag-1:200.20 create
exit
no shutdown
exit
----------------------------------------------
NODE2
config>eth-cfm# info
----------------------------------------------
domain 1 format none level 1
    association 1 format icc-based name "FacilityLag01"
        ccm-interval 1
        remote-mepid 11
        exit
    exit
domain 10 format none level 0
    association 1 format icc-based name "FacilityPort0"
        ccm-interval 1
        remote-mepid 1
        exit
    exit
----------------------------------------------
config>port# info
----------------------------------------------
ethernet
    mode access
    encap-type qinq
    eth-cfm
        mep 2 domain 10 association 1
            facility-fault
            ccm-enable
            low-priority-defect allDef
            mac-address d0:0d:1e:00:00:02
        no shutdown
        exit
    exit
    autonegotiate limited
    exit
    no shutdown
----------------------------------------------
config>lag# info
----------------------------------------------
mode access
encap-type qinq
eth-cfm
    mep 22 domain 1 association 1
        ais-enable
        client-meg-level 5
        exit
        facility-fault
A fault is introduced that only affects the LAG MEP. The port MEP continues to validate the port, meaning that the port remains operationally up and the lag transitions to operation down. The LAG transition causes all the SAPs tied to the LAG to transition to down. The VPLS service reacts normally with the configured behavior as a result of a SAP down condition. The Epipe SAP also transitions to down, causing the operational state of the Epipe service to transition to down. In this case, AIS is enabled under the SAP in the service those AIS packets will still be generated out the mate SAP.

Output from one of the nodes is included below. Since both react in the same manner, output from both nodes is not shown.

**NODE1**

```bash
#show port
```

<table>
<thead>
<tr>
<th>Port Id</th>
<th>Admin Link Port State</th>
<th>Cfg Oper LAG/ Port State</th>
<th>MTU</th>
<th>MTU</th>
<th>Bndl Mode</th>
<th>Encp Type</th>
<th>C/Q/S/XFP/ MDIMDX</th>
</tr>
</thead>
</table>
show eth-cfm mep 11 domain 1 association 1

-------------------------------------------------------------------
Eth-Cfm MEP Configuration Information
-------------------------------------------------------------------
Md-index           : 1                        Direction         : Down
Ma-index           : 1                        Admin             : Enabled
MepId              : 11                       CCM-Enable        : Disabled
Port               : lag-1                    VLAN              : 0
Description        : (Not Specified)        ControlMep        : False
FngState           : fngDefectReported      ControlMep        : False
LowestDefectPri    : allDef                   HighestDefect     : defRDICCM
Defect Flags       : bDefRDICCM                
Mac Address        : 90:f3:ff:00:01:41        ControlMep        : False
CcmLtmPriority     : 7                        
CcmTx              : 4428                     CcmSequenceErr    : 0
Fault Propagation  : disabled                 FacilityFault     : Notify
MA-CcmInterval     : 1                        MA-CcmHoldTime    : 0ms
Eth-1Dm Threshold  : 3(sec)                   MD-Level          : 1
Eth-Ais:           : Enabled                  Eth-Ais Rx Ais:   : No
Eth-Ais Tx Priorit*: 7                        Eth-Ais Rx Interv*: 1
Eth-Ais Tx Interv*: 1                        Eth-Ais Tx Counte*: 1085
Eth-Ais Tx Levels  : 5
Eth-Tst:           : Disabled

# show service sap-using eth-cfm facility

-------------------------------------------------------------------
Service ETH-CFM Facility Information
-------------------------------------------------------------------
SapId     SvcId     SAP AIS     SAP Tunnel SVC Tunnel Fault
-------------------------------------------------------------------
lag-1:100.31 100    Enabled     Accept     Ignore
lag-1:200.20 200    Disabled    Accept     Ignore
-------------------------------------------------------------------
No. of Facility SAPs: 2

# show eth-cfm cfm-stack-table facility

CFM Stack Table Defect Legend:
R = Rdi, M = MacStatus, C = RemoteCCM, E = ErrorCCM, X = XconCCM, A = AisRx

-------------------------------------------------------------------
CFM Facility Port Stack Table
-------------------------------------------------------------------
Port     Tunnel     Lvl Dir  Md-index     Ma-index     MepId     Mac-address     Defect
-------------------------------------------------------------------
1/1/2     0          0 Down         10           1          d0:0d:1e:00:00:01

CFM Facility LAG Stack Table
-------------------------------------------------------------------
Lag     Tunnel     Lvl Dir  Md-index     Ma-index     MepId     Mac-address     Defect
A:Dut-C# show service id 1 sap 1/1/1 base

Service Access Points (SAP)

| Service Id | 1 |
| SAP        | 1/1/1 |
| Encap      | null |
| Description| (Not Specified) |
| Admin State| Up |
| Oper State | Up |
| Flags      | None |
| Multi Svc Site | None |
| Last Status Change | 02/24/2012 11:37:55 |
| Last Mgmt Change | 02/24/2012 11:31:32 |
| Sub Type   | regular |
| Dot1Q Ethertype | 0x8100 |
| QinQ Ethertype | 0x8100 |
| Split Horizon Group | (Not Specified) |

| Max Nbr of MAC Addr | No Limit |
| Total MAC Addr     | 0 |
| Static MAC Addr    | 0 |
| Admin MTU          | 1514 |
| Oper MTU           | 1514 |
| Ingr IP Fltr-Id    | n/a |
| Egr IP Fltr-Id     | n/a |
| Ingr Mac Fltr-Id   | n/a |
| Egr Mac Fltr-Id    | n/a |
| Ingr IPv6 Fltr-Id  | n/a |
| Egr IPv6 Fltr-Id   | n/a |
| tod-suite          | None |
| qinq-pbit-marking | both |
| Ing Agg Rate Limit | max |
| Egr Agg Rate Limit | max |
| ARP Reply Agent    | Disabled |
| Host Conn Verify   | Disabled |
| Mac Learning       | Enabled |
| Discard Unkwn Srce| Disabled |
| Mac Aging          | Enabled |
| Mac Pinning        | Disabled |
| BPDU Translation   | Disabled |
| L2PT Termination   | Disabled |
| Vlan-translation   | None |
| Acct. Pol          | None |
| Collect Stats      | Disabled |
| Anti Spoofing      | None |
| Dynamic Hosts      | Enabled |
| Avl Static Hosts   | 0 |
| Tot Static Hosts   | 0 |
| Calling-Station-Id | n/a |
| Application Profile| None |
| Oper Group         | (none) |
| Monitor Oper Grp   | (none) |
| Restr MacProt Src  | Disabled |
| Restr MacUnpr Dst  | Disabled |
| Auto Learn Mac Prot| Disabled |
| RestProtSrcMacAct  | Disable |
| Time to RetryReset | never |
| Retries Left       | 3 |
| Mac Move           | Blockable |
| Blockable Level    | Tertiary |
| Egr MCast Grp      | |
| Auth Policy        | None |

ETH-CFM SAP specifics

| Tunnel Faults | n/a |
| AIS           | Disabled |
| MC Prop-Hold-Timer | n/a |
| V-MEP Filtering | Disabled |
Tunnel Based MEP

The concept of a logical tunnel carrying many unique and individual services has been deployed in many networks on QinQ encapsulated access ports where the outer VLAN represents the common transports and the inner VLAN represents the specific service. Typically, the tunnel transparently passes frames from multiple services through some common network. Tunnel MEPs are logically configured on the Port or LAG and outer VLAN for access ports use QinQ Ethernet encapsulation. Service processing is done after the tunnel MEP. This means that any service-based MEPs are required to be a higher level than that of the tunnel MEP. Tunnel MEPs are only supported on LAGs that are configured with QinQ encapsulation and must specify the outer VLAN.

The Tunnel MEP must validate connectivity between the tunnel end points. As with all facility MEPs, this is a point-to-point relationship between the local MEP and one remote MEP. By default, the MEP configured at the tunnel level performs only alarming functions. Actionable functions such as AIS, SAP transition, and fault propagation requires the operator to enable these functions.

The tunnel MEP must first be configured to take action when the MEP enters a fault state, similar to all other facilities MEPs. In order for the individual services to share the fate of the tunnel, each service must accept the facility MEP state. This is service-dependent and depends on the desired goals. Services share the tunnel fate based on the lag-id and the outer VLAN.

Epipe services support the ais-enable configuration option on the SAP. Enabling this option generates AIS in the event the tunnel MEP has entered a fault state as a result of ETH-CC failure, similar to other facility MEPs. However, since the individual SAPs configured within the different services are not directly affected by the tunnel MEP, an additional configuration is necessary to perform local SAP transitions, in the case of VPLS, EIS and VPRN services and OAM mapping functions for Epipe services.

The tunnel-fault service-level command configured on an Epipe allows SAP flags to be set and fault propagation and OAM mapping functions between technology. The operational state of the SAP remains up. The operator needs to determine if the AIS generation of fault propagation is the best approach in their specific network. It is possible to configure both ais-enable and tunnel-fault accept within the Epipe service. However, this may generate multiple ETH-CFM packets, or multiple actions as a result of a single failure.

The tunnel-fault accept service level option is also available under Epipe, VPLS and IES services hierarchy level within the CLI. This allows for a tunnel fault to share fate with these service SAPs. For the non-Epipe services, the SAP enters an operationally down state, and normal processing occurs as a result of the SAP transition. In order to generate any ETH-CC based fault propagation, suspend-cmm or use-int-stat-tlv, this requires service-based MEPs that are actively running CCM with a peer.

The tunnel-fault configuration options occur in two levels of the CLI hierarchy: service level and SAP level. Both of the levels within a service and within the SAP (whose underlying port and outer tag has a tunnel MEP) must be set to accept, in order to have the function enabled. By default
the **tunnel-fault** is set to ignore at the service level and accept at the SAP level. This means that a single **tunnel-fault** accept at the service level will enable fault operations for all SAPs in the service. The operator is free to enable and disable on specific SAPs by choosing the ignore option under the individual SAP. The combination of **accept** at the service level and **ignore** at the SAP level prevents that specific SAP from recognizing fault. AIS generation for Epipe services is not controlled by the **tunnel-fault** configuration options.

Specific to tunnel MEPs, reception of AIS on the tunnel MEP causes AIS to be cut through to all Epipe services that have the ais-enabled command configured under the SAP. During a fault condition, it is important that the AIS configuration under the tunnel MEP not be modified. This causes increased network element CPU processing requirements and in scaled environments transitioning this command during a heavily loaded fault condition, where highly scaled SAPs are linked to the fate of the tunnel MEP, may cause the system to spend more than normal processing time to be spent dealing with this artificially induced clear and fault situation. It is not expected that operators perform these types of tasks in production networks. Reception of AIS will not trigger a fault condition or AIS to be cut through when sub second CCM intervals have been configured on the Tunnel MEP.

Service-based MEPs may also be configured as normal for all services. They perform normal processing tasks, including service-based MEP with fault propagation.

As with all other facility MEPs, use only ETH-CFM functions to cause the Tunnel MEP to enter the fault state. Tunnel MEPs support sub second ccm-intervals on selected hardware. Tunnel MEPs must be configured with a direction of down. UP MEPs are not supported as part of the facility MEP concept.

LAG-based MEPs and LAG-based tunnel MEPs cannot be configured on the same LAG. Port-based MEPs may be configured on the LAG member ports of a tunnel MEP as long as they follow the requirements for port-based MEPs on LAG member ports. All those consideration are applicable here, including nesting and port-level control only without propagation.

Port-based MEPs and Port-based tunnel MEPs cannot be configured on the same port.

LAG-based Tunnel MEPs are supported in MultiChassis LAG (MC-LAG) configuration. However, sub second CCM enabled intervals should not be configured when the LAG-based Tunnel MEP utilizes the transport of an MC-LAG. Only one second and above CCM intervals should be used. Not all platforms support sub second CCM enable Tunnel MEPs.

Tunnel MEPs are meant to propagate fault from one segment to the other for Epipe services. **Figure 24 on page 120** shows how individual Epipes have SAPs connecting to a legacy network. A MEP is configured at the tunnel level and peers with a single remote peer MEP.
This is only one example of a tagged service. The principles of a tunnel MEP may be applied to other service as applicable. Remember that tunnel MEPs are only supported on LAGs that are configured with QinQ encapsulation and must have an outer VLAN.

Individual services can be monitored end-to-end by placing a MEP on the service endpoint at the CPE, denoted by the MEP at level 5 on the individual EVC (customer levels 5-7). The Network Interface Demarcation (NID) typically places a single tag, outer or only, on the customer traffic. This is cross connected to the proper connection in the access network and eventually arrive on the Ethernet Aggregation Switch. The connection between the legacy or access network and the aggregation switch must be either a LAG bundle or MC-LAG in order for tunnel MEPs to be configured.

Since there can be a large number of services transported by a single tunnel, the MEP executing at the tunnel-level reduces network overhead and simplifies the configuration. It is important to note that all services in the tunnel must share a common physical path.

**Figure 24: Tunnel Concepts and Encapsulation**
A SAP is needed in order for the Tunnel MEP to extract the tunnel MEP ETH-CFM packets at the appropriate level. No SAP record is created by default. A service must already exist that includes a SAP in the form lag-id:vid.* or lag-id:vid.0 where the vid matches the outer VLAN in which the tunnel is to monitor. Since the ETH-CFM traffic arrives at the Ethernet aggregation node as a single outer tag with no inner tag, the operator may want to consider the ability to configure the lag-id:vid.0 to accept untagged only frames with the matching outer tag and no inner tag. The global command `configure>system->ethernet>new-qinq-untagged-sap` is available to enable this functionality. By default both the vid.* and vid.0 accepts all packets that match the outer vid and any inner vid. If no SAP record exists for this VLAN, one must be created manually.

Manually creating this SAP requires a service context. Alcatel-Lucent recommends that an Epipe service be configured with this single SAP, preventing any flooding of packets. It is possible to use a VPLS instance and combine many tunnel SAP records into a single service instance. However, configuration errors may result in leakage because of the multipoint nature of a VPLS service. Regardless of the service type chosen, it should be in a shutdown state. Also, normal ETH-CFM rules apply. ETH-CFM packets arriving on the SAP passes all ETH-CFM packets at and below the tunnel MEP to the ETH-CFM application for processing.

The goal of a Tunnel MEP is to validate an attachment circuit and relate the state to services that share the same LAG and outer VLAN to other services across the network. Tunnel MEPs are not intended for propagating fault between two endpoints that share the same LAG and outer VLAN. For this reason, locally switched circuits that share the same LAG and the same outer tag must not use the `ais-enable` function under those SAPs. As an example, lag-1 may have two SAPs associated with it: lag-1:1.1 and lag-1:1.2. These two SAP represent two different endpoints on the same LAG using the same outer VLAN. In this case, if the ais-enable is configured under both SAPs, AIS functionality does not work properly. Normal fault propagation could be used in this case instead. Since the tunnel MEP is validating the common physical path and these two MEPs share the common physical path, there is no reason to propagate fault. Service-based MEPs could be configured on the endpoints in order to validate the connectivity between the two endpoints when this type of model is deployed. However, two SAPs that are connected to different LAGs is a supported configuration. An example of this would be lag-1:1.1 and lag-2:1.1.

Sub second Tunnel MEPs will be monitored for every three seconds to ensure that they are not continuously bouncing and consuming an unfair allocation of ETH-CFM resources. A sub second MEP will only be allowed three operational status changes in a three second window before holding the state for the remaining time in that window. Messages will be paced from Tunnel MEPs. Fault propagation depends on factors such as how busy the node is, or how scaled the node configuration is.

Five percent of the operational/negotiated port speed not physical speed is available for Tunnel MEP control traffic. When applying this to the LAG-based Tunnel MEPs the five percent is derived from the lowest speed of a single member port in the bundle. If this bandwidth percentage required for ETH-CFM is exceeded the ETH-CFM packets will not be able to be sent and failures will occur. As an example, a physical port of 1Gbps that has negotiated an operational speed of 100Mbps with a peer will be allowed to send up to a maximum of 5Mbps of Tunnel MEP control traffic.
Example: Tunnel MEP Configuration

Figure 25 shows how fate can be shared between the Tunnel MEP and the services configured on the same LAG and outer VLAN.

![Figure 25: Tunnel MEP Example](image)

In this example, a single Tunnel, LAG-1 outer VLAN 100, carries three services. Epipe 101, Epipe 102 and VPLS 201 are the service extraction points on the aggregation node. Epipe 100 is the extraction point for the Tunnel MEP eth-cfm traffic. This is a single SAP Epipe that is operationally shutdown. One common configuration error when using Tunnel MEPs is the lack of extraction on the aggregation node, causing unidirectional failures. The aggregation node is sending eth-cfm traffic to the NID, but is not extracting the eth-cfm traffic that the NID is sending.

Epipe 101 is configured to accept the tunnel MEP fate and generate AIS.

Epipe 102 is configured to accept the tunnel MEP state and apply fault propagation rules. If the network-side mate were an SDP binding, then the applicable setting of the LDP status bits are in the header. Since this example uses an Ethernet SAP as the mate, and only tunnel fault-accept is configured with no ais-enable, only the SAP flag is set to indicate an error.

VPLS 201 also shares the fate of the tunnel MEP. The tunnel-fault accept transitions the SAP to operationally down. Any configured event that occurs because of a SAP down for the VPLS also occur.

Only the configuration for the aggregation node is shown below. The NID configuration is not required to show how this function works.

Aggregation node

```
config>eth-cfm# info
----------------------------------------------
domain 2 format none level 2
association 1 format icc-based name "FacilityTun01"
ccm-interval 1
remote-mepid 101
```
exit
exit
----------------------------------------------

config>lag# info
----------------------------------------------
mode access
encap-type qinq
eth-cfm
  mep 100 domain 2 association 1 vlan 100
  description "Tunnel Facility MEP - Do NOT Delete"
  ais-enable
    client-meg-level 5
  exit
  facility-fault
  ccm-enable
  low-priority-defect allDef
  no shutdown
  exit
  exit
  port 1/1/2
  no shutdown
----------------------------------------------

config>service# info
----------------------------------------------
customer 1 create
description "Default customer"
exit
epipe 100 customer 1 create
  shutdown
  description "Tunnel Extraction Service"
  sap lag-1:100.0 create
  exit
  exit
epipe 101 customer 1 create
description "Customer Service 100.31"
  sap 1/1/10:100.31 create
  exit
  sap lag-1:100.31 create
    eth-cfm
      ais-enable
      exit
      exit
      no shutdown
      exit
epipe 102 customer 1 create
description "Customer Service 100.32"
    eth-cfm
      tunnel-fault accept
      exit
      sap 1/1/10:100.32 create
      exit
      sap lag-1:100.32 create
      exit
      no shutdown
      exit
vpls 201 customer 1 create
description "Customer Service 100.51"
stp
  shutdown
exit
eth-cfm
  tunnel-fault accept
exit
sap 1/1/10:100.51 create
exit
sap lag-1:100.51 create
exit
no shutdown
exit

# show eth-cfm mep 100 domain 2 association 1

Eth-Cfm MEP Configuration Information

Md-index           : 2                        Direction         : Down
Ma-index           : 1                        Admin             : Enabled
MepId              : 100                      CCM-Enable        : Enabled
Port               : lag-1                    VLAN              : 100
Description        : Tunnel Facility MEP - Do NOT Delete
FngState           : fngReset                 ControlMep        : False
LowestDefectPri    : allDef                   HighestDefect     : none
Defect Flags       : None                     Defect Flags       : None
Mac Address        : 90:f3:ff:00:01:41        ControlMep        : False
CcmLtmPriority     : 7                        CcmLtmPriority     : 7
CcmTx              : 3958                     CcmTx              : 3958
Fault Propagation  : disabled                 FacilityFault     : Notify
MA-CcmInterval     : 1                        MA-CcmHoldTime    : 0ms
Eth-1Dm Threshold  : 3(sec)                   MD-Level          : 2
Eth-Ais:           : Enabled                  Eth-Ais Rx Ais:   : No
Eth-Ais Tx Priorit*: 7                        Eth-Ais Rx Interv*: 1
Eth-Ais Tx Interva*: 1                        Eth-Ais Tx Counte*: 175
Eth-Ais Tx Levels  : 5                        Eth-Ais Tx Levels  : 5
Eth-Tst:           : Disabled                Eth-Tst:           : Disabled
Redundancy:
  MC-LAG State   : n/a

CcmLastFailur Frame:
  None

XconCcmFailure Frame:
  None

# show eth-cfm cfm-stack-table facility all-tunnel-meps

CFM Stack Table Defect Legend:
R = Rdi, M = MacStatus, C = RemoteCCM, E = ErrorCCM, X = XconCCM, A = AisRx

CFM Facility LAG Stack Table

Lag Tunnel Lvl Dir Md-index Ma-index MepId Mac-address Defect
None
lag-1  100  2 Down  2  1  100  90:f3:ff:00:01:41 -------

# show service sap-using eth-cfm facility

Service ETH-CFM Facility Information

<table>
<thead>
<tr>
<th>SapId</th>
<th>SvcId</th>
<th>SAP AIS</th>
<th>SAP Tunnel</th>
<th>SVC Tunnel</th>
</tr>
</thead>
<tbody>
<tr>
<td>lag-1:100.0</td>
<td>100</td>
<td>Disabled</td>
<td>Accept</td>
<td>Ignore</td>
</tr>
<tr>
<td>lag-1:100.31</td>
<td>101</td>
<td>Enabled</td>
<td>Accept</td>
<td>Ignore</td>
</tr>
<tr>
<td>lag-1:100.32</td>
<td>102</td>
<td>Disabled</td>
<td>Accept</td>
<td>Accept</td>
</tr>
<tr>
<td>lag-1:100.51</td>
<td>201</td>
<td>Disabled</td>
<td>Accept</td>
<td>Accept</td>
</tr>
</tbody>
</table>

No. of Facility SAPs: 4

When the tunnel MEP enters a fault state

- Epipe 101 will start to generate AIS out the mate sap
- Epipe 102 SAP flag will be set
- VPLS 201 SAP will go down

Output from one of the nodes is included below. Since both will react in the same manner output from both nodes is not required.

Aggregation node

# show eth-cfm cfm-stack-table facility all-tunnel-meps

CFM Facility LAG Stack Table

<table>
<thead>
<tr>
<th>Lag</th>
<th>Tunnel</th>
<th>Lvl Dir</th>
<th>Md-index</th>
<th>Ma-index</th>
<th>MepId</th>
<th>Mac-address</th>
<th>Defect</th>
</tr>
</thead>
<tbody>
<tr>
<td>lag-1</td>
<td>100</td>
<td>2 Down</td>
<td>2</td>
<td>1</td>
<td>100</td>
<td>90:f3:ff:00:01:41</td>
<td>--C---</td>
</tr>
</tbody>
</table>

# show service sap-using eth-cfm facility tunnel 100

Service ETH-CFM Facility Information

<table>
<thead>
<tr>
<th>SapId</th>
<th>SvcId</th>
<th>SAP AIS</th>
<th>SAP Tunnel</th>
<th>SVC Tunnel</th>
</tr>
</thead>
<tbody>
<tr>
<td>lag-1:100.0</td>
<td>100</td>
<td>Disabled</td>
<td>Accept</td>
<td>Ignore</td>
</tr>
<tr>
<td>lag-1:100.31</td>
<td>101</td>
<td>Enabled</td>
<td>Accept</td>
<td>Ignore</td>
</tr>
<tr>
<td>lag-1:100.32</td>
<td>102</td>
<td>Disabled</td>
<td>Accept</td>
<td>Accept</td>
</tr>
<tr>
<td>lag-1:100.51</td>
<td>201</td>
<td>Disabled</td>
<td>Accept</td>
<td>Accept</td>
</tr>
</tbody>
</table>
No. of Facility SAPs: 4

# show eth-cfm mep 100 domain 2 association 1

Eth-Cfm MEP Configuration Information

Md-index : 2                    Direction : Down
Ma-index : 1                    Admin     : Enabled
MepId   : 100                   CCM-Enable : Enabled
Port    : lag-1                 VLAN     : 100
Description : Tunnel Facility MEF - Do NOT Delete
FngState : fngDefectReported   ControlMep : False
LowestDefectPri : allDef       HighestDefect : defRemoteCCM
Defect Flags : bDefRemoteCCM    Mac Address : 90:f3:ff:00:01:41
CcmLtmPriority : 7               ControlMep : False
CcmTx      : 4211                 CcmSequenceErr : 0
Fault Propagation : disabled    FacilityFault : Notify
MA-CmInterval : 1               MA-CmHoldTime : 0ms
Eth-1Dm Threshold : 3(sec)      MD-Level : 2
Eth-Ais:      : Enabled          Eth-Ais Rx Ais: No
Eth-Ais Rx Interv*: 7           Eth-Ais Rx Interv*: 1
Eth-Ais Tx Interv*: 1           Eth-Ais Tx Count*: 215
Eth-Ais Tx Levels : 5            Eth-Tst: Disabled
Eth-Tst:     : Disabled

Redundancy:
    MC-LAG State : n/a

CcmLastFailure Frame:
    None

XconCcmFailure Frame:
    None

show service id 101 base

Service Basic Information

Service Id : 101                    Vpn Id : 0
Service Type : Epipe
Name       : (Not Specified)
Description : Customer Service 100.31
Customer Id : 1
Last Status Change: 02/04/2010 15:53:12
Last Mgmt Change : 02/04/2010 16:31:00
Admin State  : Up                  Oper State : Up
MTU         : 1514
Vc Switching : False
SAP Count   : 2                    SDP Bind Count : 0
Per Svc Hashing : false
Force QTag Fwd : Disabled

Identifier              Type     AdmMTU OprMTU Adm Opr

Page 126
# show service id 102 base

## Service Basic Information

<table>
<thead>
<tr>
<th>Service Id</th>
<th>102</th>
<th>Vpn Id</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Type</td>
<td>Epipe</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>(Not Specified)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td>Customer Service 100.32</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Customer Id</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Last Status Change</td>
<td>02/04/2010 15:45:07</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Last Mgmt Change</td>
<td>02/04/2010 16:30:43</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Admin State</td>
<td>Up</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Oper State</td>
<td>Up</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MTU</td>
<td>1514</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vc Switching</td>
<td>False</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SAP Count</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SDP Bind Count</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Per Svc Hashing</td>
<td>Disabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Force QTag Fwd</td>
<td>Disabled</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## Service Access & Destination Points

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Type</th>
<th>AdmMTU</th>
<th>OprMTU</th>
<th>Adm</th>
<th>Opr</th>
</tr>
</thead>
<tbody>
<tr>
<td>sap:1/1/10:100.32</td>
<td>qinq</td>
<td>1522</td>
<td>1522</td>
<td>Up</td>
<td>Up</td>
</tr>
<tr>
<td>sap:lag-1:100.32</td>
<td>qinq</td>
<td>1522</td>
<td>1522</td>
<td>Up</td>
<td>Up</td>
</tr>
</tbody>
</table>

# show service id 102 sap lag-1:100.32

## Service Access Points(SAP)

| Service Id | 102 |
| SAP        | lag-1:100.32 |
| Encap      | qinq |
| QinQ Dot1p | Default |
| Description| (Not Specified) |
| Admin State| Up |
| Oper State | Up |
| Flags      | OamTunnelMEPFault |
| Multi Svc Site | None |
| Last Status Change | 02/04/2010 15:45:07 |
| Last Mgmt Change | 02/04/2010 15:44:26 |

## ETH-CFM SAP specifics

<table>
<thead>
<tr>
<th>Tunnel Faults</th>
<th>accept</th>
</tr>
</thead>
<tbody>
<tr>
<td>AIS</td>
<td>Disabled</td>
</tr>
<tr>
<td>MC Prop-Hold-Timer</td>
<td>n/a</td>
</tr>
</tbody>
</table>

# show service id 201 base

## Service Basic Information

| Service Id | 201 |
| Vpn Id     | 0  |
| Service Type | VPLS |
Name              : (Not Specified)  Description       : Customer Service 100.51
Customer Id       : 1                      Last Status Change: 02/04/2010 15:46:03
Last Mgmt Change  : 02/04/2010 16:30:29
Admin State       : Up                      Oper State : Up  
MTU               : 1514                     Def. Mesh VC Id : 201
SAP Count         : 2                       SDP Bind Count : 0  
Snd Flush on Fail : Disabled                  Host Conn Verify : Disabled
Propagate MacFlush: Disabled                  Per Svc Hashing : Disabled
Allow IP Intf Bind: Disabled                  Def. Gateway IP : None 
Def. Gateway MAC  : None                      Temp Flood Time : Disabled
Temp Flood Chg Cnt: 0                          Temp Flood : Inactive

Service Access & Destination Points

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Type</th>
<th>AdmMTU</th>
<th>OprMTU</th>
<th>Adm</th>
<th>Opr</th>
</tr>
</thead>
<tbody>
<tr>
<td>sap:1/1/10:100.51</td>
<td>qinq</td>
<td>1522</td>
<td>1522</td>
<td>Up</td>
<td>Up</td>
</tr>
<tr>
<td>sap:lag-1:100.51</td>
<td>qinq</td>
<td>1522</td>
<td>1522</td>
<td>Up</td>
<td>Down</td>
</tr>
</tbody>
</table>
Router Interface MEP

MEPs and associated on-demand troubleshooting functions act as router interfaces that are part of the base routing instance. This feature allows the operator to verify Layer 2 transport that connects the Layer 3 interfaces.

Router interfaces MEPs are supported for all router interface instances (null port 1/1/1, dot1q port 1/1/3:vid, null LAG-lag-id and dot1q LAG-lag-id:vid).

Example: Router MEP Configuration

The following illustration, Figure 26, shows how a Router Facility MEP can be configured on a routed interface in the base router instance.

![Router MEP Example](image)

Figure 26: Router MEP Example

ETH-CFM tools for proactive management (ETH-CC), troubleshooting (Loopback, Linktrace, etc.) and profiling (Delay Measurement, etc.) are supported. The configuration and some ETH-CFM test commands are shown for Node1 (left). Following the on-demand test output, the configuration for Node 2 is included for completeness, without repeating the on-demand tests.

NODE1

```plaintext
config>port# info
----------------------------------------------
  ethernet
  exit
  no shutdown
----------------------------------------------
config>eth-cfm# info
----------------------------------------------
  domain 2 format none level 2
  association 2 format icc-based name "FacilityRtr01"
  exit
```

OSSG543
exit

config>router# info

#--------------------------------------------------
echo "IP Configuration"
#--------------------------------------------------
interface "Core1"
  address 192.168.1.1/30
  port 1/2/1
  eth-cfm
    mep 1 domain 2 association 2
    mac-address d0:0d:1e:00:00:01
    no shutdown
  exit
  exit
interface "system"
  exit

# show eth-cfm cfm-stack-table facility all-router-interfaces
CFM Stack Table Defect Legend:
R = Rdi, M = MacStatus, C = RemoteCCM, E = ErrorCCM, X = XconCCM, A = AisRx
CFM Facility Interface Stack Table
Interface  Lvl Dir  Md-index  Ma-index  MepId  Mac-address  Defect
Core1       2 Down  2        2        1 d0:0d:1e:00:00:01 ----

# show eth-cfm cfm-stack-table facility all-router-interfaces
CFM Stack Table Defect Legend:
R = Rdi, M = MacStatus, C = RemoteCCM, E = ErrorCCM, X = XconCCM, A = AisRx
CFM Facility Interface Stack Table
Interface  Lvl Dir  Md-index  Ma-index  MepId  Mac-address  Defect
Core1       2 Down  2        2        1 d0:0d:1e:00:00:01 ----

# oam eth-cfm loopback d0:0d:1e:00:00:02 mep 1 domain 2 association 2
  send-count 5
Eth-Cfm Loopback Test Initiated: Mac-Address: d0:0d:1e:00:00:02, out service: 0
  Sent 5 packets, received 5 packets [0 out-of-order, 0 Bad Msdu]
# oam eth-cfm linktrace d0:0d:1e:00:00:02 mep 1 domain 2 association 2
  Index Ingress Mac  Egress Mac  Relay  Action
  ----- ----------- ----------- ------- -------
  1  D0:0D:1E:00:00:02  00:00:00:00:00:00 n/a  terminate

---------------------------------------------------------------------
No more responses received in the last 6 seconds.

```
# oam eth-cfm two-way-delay-test d0:0d:1e:00:00:02 mep 1 domain 2 association 2
Two-Way-Delay-Test Response:
Delay 1130 microseconds        Variation 63 microseconds

# oam eth-cfm two-way-delay-test d0:0d:1e:00:00:02 mep 1 domain 2 association 2
Two-Way-Delay-Test Response:
Delay 1218 microseconds        Variation 88 microseconds
```

**NODE2**

```
config>port# info
----------------------------------------------
ethernet
exit
no shutdown
----------------------------------------------
config>eth-cfm# info
----------------------------------------------
domain 2 format none level 2
    association 2 format icc-based name "FacilityRtr01"
    exit
exit
----------------------------------------------
config>router# info
----------------------------------------------
#--------------------------------------------------
echo "IP Configuration"
#--------------------------------------------------
interface "Core2"
    address 192.168.1.2/30
    port 1/2/2
    eth-cfm
        mep 2 domain 2 association 2
        mac-address d0:0d:1e:00:00:02
        no shutdown
        exit
        exit
interface "system"
exit
----------------------------------------------
```
**ETH-CFM and MC-LAG**

By default, ETH-CFM Management Points (MEPs and MIPs) and MC-LAG operate independently. Alcatel-Lucent recommends not enabling fault propagation when the default behavior is in use. A global command is available in order to allow ETH-CFM the ability to track the state of the MC-LAG for MPs that are configured on MC-LAG ports. This feature does not allow MEPs to influence MC-LAG state. Since the MP relies heavily on the underlying MC-LAG construct, consideration must be given for the proper MC-LAG design and deployment. It is important to understand that the state of MC-LAG can be reflected in the state of the MPs which are configured on SAPs that are part MC-LAGs. For example, a SAP on a LAG that is part of an MC-LAG configuration can behave in a manner that more appropriately represents the MC-LAG.

---

**ETH-CFM and MC-LAG Default Behavior**

ETH-CFM MPs track the SAPs, bindings and facility independently. Therefore, when an MP is configured on a SAP which is not operationally up because of MC-LAG ETH-CFM defect, conditions are raised for what could be considered normal conditions. Figure 27 shows the default behavior for a point-to-point service without regard for MC-LAG. In the case below, the two up MEPs operating at level 4 on the affected SAPs set the `Interface-Status-TLV` bit in the ETH-CC header to represent the `isDown` condition, assuming ETH-CC is executing between the peer MEPs. This is the correct action based on the ETH-CFM perspective, SAPs are operationally down.

![Figure 27: Independent Processing UP MEP Example](image)

A similar condition exists if down MEPs are configured on the SAPs that are operationally down. Figure 28 shows how the same service configured with down MEPs would generate AIS, if
enabled, toward the remote client at the configured client-meg-level, in the reverse direction of the MEP. This is also the proper behavior from the perspective ETH-CFM.

![Figure 28: Independent Processing Down MEP Example](image)

**Linking ETH-CFM to MC-LAG State**

Allowing ETH-CFM to understand the state of MC-LAG and adjust the behavior of the MP (MEP and MIP) according to that state has benefits.

MC-LAG represents the two upstream nodes as a single system to the node terminating a standard LAG. Linking the ETH-CFM MPs to the state of the MC-LAG allows the operator to configure MPs across the two boxes that appear the same. Under the default configuration, this would introduce various defect conditions to be raised and event conditions. However, when ETH-CFM is tracking the state of the MC-LAG, the MPs performs a role that represents the state of the resiliency mechanism. In order to enable this new behavior, configure the system-wide command `standby-mep-shutdown` under the `config>eth-cfm>redundancy>mc-lag` hierarchy.

When a MP is part of the active MC-LAG system, it performs as a normal MP: terminating, generating, responding to, and processing all appropriate ETH-CFM packets. An MP that is on the standby MC-LAG node enters a pseudo-shutdown state. These MPs terminates all ETH-CFM that are part of the regular interception process, but will not process them. They are silently discarded. Also, an MP that exists on a standby MC-LAG system does not generate any ETH-CFM packets. All proactive and on-demand functions are blocked on the standby MC-LAG node. When scheduled tests are executed through SAA these test will attempt to execute. The tests will record failures as a result of the MEP state. These failures are not representative of the network.

This feature relies on the proper configuration, design, and deployment of the MC-LAG protocol. There are numerous optimizations and configuration parameters that are available as part of the
MC-LAG functions. For example, by default, when a currently active MC-LAG port transitions to standby, by any means including manual operator intervention, the remote node terminating the standard LAG sees the LAG transition because all ports in the LAG are down for an instance in time. This is standard LAG behavior does not change as a result of the linkage of MP state to MC-LAG state. This transition causes the propagation of faults for MEPs configured on that node. Normal architectural LAG design must take these types of events into consideration. MC-LAG provides numerous tuning parameters that need to be considered before deploying in the field. These include a hold-time down option on the node terminating the standard LAG, as well as other parameters for revertive behavior such as the hold-time up option. It is important to ensure that the operator’s specific environment be taken into consideration when tuning the MC-LAG parameters to avoid the propagation of error conditions during normal recover events. In the case that the resumption of data forwarding exceed the timeout value of a MEP (3.5 times the CCM-Interval), the appropriate defect conditions are raised.

ETH-CFM will register a fault propagation delay timer equal to propagate-hold-time under the config>eth-cfm>redundancy>mc-lag hierarchy (default of 1s) to delay notification of an event that may be a result of MC-LAG failover. This allows the system time to coordinate events and triggers that together represent the MC-LAG transition from active to standby.

A fixed timer value of 1s will delay an UP MEP from announcing a SAP down condition through CCM Interface-Status-TLV bits, is Down. ETH-CFM maintains a status of last sent to the UP MEPs peer. When the SAP transitions either to UP or DOWN that fault will be held for the fixed 1s interval and the last Interface-Status-TLV bits will set based on the previous transmission. If the condition, different from the previous sent, still exists at the end of the 1s fixed timer and when the next CCM interval expires, the representative value of the SAP will be sent in the Interface-Status-TLV. These two timers help to smooth out network transitions at the cost of propagation and clearing of faults.

When a node with ETH-CFM linked to MC-LAG is transitioning from standby to active ETH-CFM will assume there are no underlying conditions for any of the SAPs that are now part of the newly activating MC-LAG. The initial notification to an UP MEPs peer will not include any faults. It will assume that the transitioning SAPs are stabilizing as the switchover proceeds. The fixed 1s timer will be starting and a second CCM PDU based on the UP MEPs interval will be sent without any recognition of potential fault on the SAP. However, after the expiration of the fixed timer and on the next CCM-Interval, the Interface-Status-TLV will represent the state of the SAP.

In scaled environments it is important to configure the propagation-hold-time and the CCM intervals to achieve the desired goals. If these timers are set too aggressively, then fault and defect conditions may be generated during times of network stabilization. The use of fault propagation and AIS transmission needs to be carefully considered in environments where MC-LAG protection mechanisms are deployed. Timer values do not guarantee that transitional state will not be propagated to the peer. The propagation of such state may be more taxing and disruptive that allowing the transmission states to complete. For example, if AIS generation is being used in this type of solution the operator should use a 60s AIS interval to avoid transitional state from being advertised.
AIS generation is paced in a first come first serve model not to exceed the system capability, scale is dependent on the type of system. If AIS is configured in an MC-LAG solution the operator must make sure that the same MEPs on each system are configured to generate AIS and this number does not exceed the maximum. This would require the operator to configure both nodes with the same MEPs that can generate AIS and not exceed the system capacity. If the nodes are configured differently or exceed the system scale there is a very high potential where a transition may see a different set of MEPs pacing out the AIS than the original set of MEPs. There is no synchronization of AIS state across nodes.

Administrative functions, like **admin down**, are special cases. When the administrative state changes from **up** to **down**, the timer is bypassed and communication from ETH-CFM is immediate.

When an MP is configured in an MC-LAG environment, Alcatel-Lucent recommends that each aspect of the MP be configured the same, including MAC address. Also, although this may be obvious, both nodes participating in the MC-LAG requiring this functionality should include the global command in the `config>eth-cfm>redundancy>mc-lag>standby-mep>shutdown` context to avoid unpredictable behavior.

In summary, a SAP with ETH-CFM tracking the state of the MC-LAG represents the state of the MC-LAG. MPs configured on the standby MC-LAG ports enters a state similar to shutdown. MPs on the MC-LAG ports on the active MC-LAG ports performs all normal processing.

**Example: ETH-CFM and MC-LAG Configuration**

The following illustration, shows how MEPS can be linked to MC-LAG state. In this example, a service MEP is created on the LAG SAP on NODE1 within service VPLS 100. The MEPs configured on the MC-LAG nodes within service 100 are both configured the same. Both MEPs use the same MEP-ID, the same MAC address.
Figure 29: ETH-CFM and MC-LAG Example

Only one of the MEPs on the MC-LAG nodes is active for VPLS service 100. The other MEP is in a shutdown mode, so that even when the MC-LAG is in standby and the port state is Link Up, the MEP is in a pseudo shutdown state.

The following configuration example is not meant to provide all possible MC-LAG configuration statement to tune each provider’s network. It does provide a base configuration to demonstrate the ETH-CFM feature.

NODE1

```
config>port# info (both ports)
----------------------------------------------
eternet
  mode access
  encap-type qinq
  autonegotiate limited
exit
no shutdown
----------------------------------------------
```  

```
config>lag# info
----------------------------------------------
mode access
  encap-type qinq
  access
    adapt-qos link
exit
port 1/1/5
port 1/1/6
lACP active administrative-key 32768
hold-time down 10
no shutdown
----------------------------------------------
```
config>eth-cfm# info
---------------------------------------------
domain 3 format none level 3
   association 1 format icc-based name "03-0000000100"
      bridge-identifier 100
     exit
    ccm-interval 1
   remote-mepid 101
  exit
  exit
---------------------------------------------

config>service>vpls# info
---------------------------------------------
stp
   shutdown
exit
sap 1/1/3:100.100 create
exit
sap lag-1:100.100 create
   eth-cfm
      mep 100 domain 3 association 1 direction down
         ccm-enable
            mac-address d0:0d:1e:00:01:00
               no shutdown
          exit
          exit
          exit
          no shutdown
---------------------------------------------

TOP (MC-LAG Standby)
config>port# info
---------------------------------------------
ethernet
   mode access
      encap-type qinq
         autonegotiate limited
     exit
    no shutdown
---------------------------------------------

config>lag# info
---------------------------------------------
mode access
encap-type qinq
access
   adapt-qos link
exit
port 1/1/2
   lacp active administrative-key 32768
  no shutdown
---------------------------------------------

config>router# info
#---------------------------------------------
echo "IP Configuration"
#--------------------------------------------------
interface "Core2"
  address 192.168.1.2/30
  port 1/2/2
exit
interface "system"
exit
--------------------------------------------------
config>redundancy# info
--------------------------------------------------
multi-chassis
  peer 192.168.1.1 create
  source-address 192.168.1.2
  mc-lag
    lag 1 lacp-key 1 system-id 00:00:00:00:00:01 system-priority
       100
    no shutdown
    exit
  no shutdown
  exit
synchronize boot-env
--------------------------------------------------
config>eth-cfm# info
--------------------------------------------------
domain 3 format none level 3
  association 1 format icc-based name "03-0000000100"
  bridge-identifier 100
  exit
  ccm-interval 1
  remote-mepid 100
  exit
redundancy
  mc-lag
    standby-mep-shutdown
  exit
exit
--------------------------------------------------
config>service>vpls# info
--------------------------------------------------
stp
  shutdown
exit
sap lag-1:100.100 create
eth-cfm
  mep 101 domain 3 association 1 direction down
  exit
  ccm-enable
  mac-address d0:0d:1e:00:01:01
  no shutdown
  exit
exit
no shutdown
# show lag 1
===============================================================================
Lag Data
===============================================================================
Lag-id  Adm  Opr  Port-Threshold  Up-Link-Count  MC Act/Stdby
-------------------------------------------------------------------------------
1       up  down  0              0               standby
===============================================================================

# show port
===============================================================================
Ports on Slot 1
===============================================================================
Port  Admin Link Port  Cfg  Oper LAG/ Port Port Port  C/QS/S/XFP/
Id    State     State  MTU  MTU  Bndl Mode Encp Type  MDIMDX
-------------------------------------------------------------------------------
... snip ...
1/1/2  Up  Yes  Link Up 1522 1522  1 accs qinq xcme
...snip...
===============================================================================
BOT (MC-LAG Active)
config>port# info
----------------------------------------------
ethernet
    mode access
    encap-type qinq
    autonegotiate limited
    exit
    no shutdown
----------------------------------------------

cfg>lag# info
----------------------------------------------
    mode access
    encap-type qinq
    access
    adapt-qos link
    exit
    port 1/1/2
    lacp active administrative-key 32768
    no shutdown
----------------------------------------------

cfg>router# info
----------------------------------------------
#--------------------------------------------------
echo "IP Configuration"
#--------------------------------------------------
    interface "Core1"
        address 192.168.1.1/30
        port 1/2/1
        exit
    interface "system"
        exit
----------------------------------------------
config>redundancy# info
-------------------------------------------------------------
multi-chassis
  peer 192.168.1.2 create
    source-address 192.168.1.1
  mc-lag
    lag 1 lACP-key 1 system-id 00:00:00:00:00:01 system-priority 100
      no shutdown
      exit
      no shutdown
      exit
      exit
      synchronize boot-env
-------------------------------------------------------------
config>eth-cfm# info
-------------------------------------------------------------
domain 3 format none level 3
  association 1 format icc-based name "03-0000000100"
    bridge-identifier 100
      exit
    ccm-interval 1
      remote-mepid 100
      exit
      exit
      redundancy
      mc-lag
      standby-mep-shutdown
      exit
      exit
-------------------------------------------------------------
config>service>vpls# info
-------------------------------------------------------------
stp
  shutdown
  exit
  sap lag-1:100.100 create
  eth-cfm
    mep 101 domain 3 association 1 direction down
      exit
      ccm-enable
      mac-address d0:0d:1e:00:01:01
        no shutdown
      exit
      exit
      exit
      no shutdown
-------------------------------------------------------------
# show lag 1
===============================================================================
<table>
<thead>
<tr>
<th>Lag Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lag-id</td>
</tr>
<tr>
<td>----------</td>
</tr>
<tr>
<td>1</td>
</tr>
</tbody>
</table>
```
# show port

Ports on Slot 1

<table>
<thead>
<tr>
<th>Port Id</th>
<th>Admin Link State</th>
<th>Link State</th>
<th>MTU</th>
<th>MTU</th>
<th>Bndl Mode</th>
<th>Encp Type</th>
<th>MDIMDX</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1/2</td>
<td>Up</td>
<td>Yes</td>
<td>1522</td>
<td>1522</td>
<td>accs</td>
<td>qinq</td>
<td>xcme</td>
</tr>
</tbody>
</table>
```

...snip...

---

Services
ETH-CFM Features

CCM Hold Timers

In some cases the requirement exists to prevent a MEP from entering the defRemoteCCM defect, remote peer timeout, from more time than the standard 3.5 times the CCM-interval. Both the IEEE 802.1ag standard and ITU-T Y.1731 recommendation provide a non-configurable 3.5 times the CCM interval to determine a peer time out. However, when sub second CCM timers (10ms/100ms) are enabled the carrier may want to provide additional time for different network segments to converge before declaring a peer lost because of a timeout. In order to maintain compliance with the specifications the ccm-hold-timer down <delay-down> option has been introduced to artificially increase the amount of time it takes for a MEP to enter a failed state should the peer time out. This timer is only additive to CCM timeout conditions. All other CCM defect conditions, like defMACStatus, defXconCCM, and so on, will maintain their existing behavior of transitioning the MEP to a failed state and raising the proper defect condition without delay.

When the ccm-hold-timer down delay-down option is configured the following calculation is used to determine the remote peer time out (3.5 times the CCM-Interval + ccm-hold-timer delay-down).

This command is configured under the association. Only sub second CCM enabled MEPs support this hold timer. Ethernet-Tunnel Paths use a similar but slightly different approach and will continue to utilize the existing method. Ethernet-tunnels will be blocked from using this new hold timer.

It is possible to change this command on the fly without deleting it first. Simply entering the command with the new values will change to values without having to delete the command prior to the change.

It is possible to change the ccm-interval of a MEP on the fly without first deleting it. This means it is possible to change a sub second CCM enabled MEP to 1 second or above. The operator will be prevented from changing an association from a sub second CCM interval to a non-sub second CCM interval when ccm-hold-timer is configured in that association. The ccm-hold-timer must be removed using the no option prior to allowing the transition from sub second to non-sub second CCM interval.
## MEP and MIP Support

The following is a general table that indicates the ETH-CFM support for the different services and endpoints. It is not meant to indicate the services that are supported or the requirements for those services on the individual platforms.

<table>
<thead>
<tr>
<th>Service</th>
<th>Ethernet Connection</th>
<th>Down MEP</th>
<th>Up MEP</th>
<th>MIP</th>
<th>Virtual MEP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Epipe</td>
<td>SAP</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>Spoke-SDP</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>-</td>
</tr>
<tr>
<td>VPLS</td>
<td>SAP</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>Spoke-SDP</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>Mesh-SDP</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>-</td>
</tr>
<tr>
<td>B-VPLS</td>
<td>SAP</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>Spoke-SDP</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>Mesh-SDP</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>-</td>
</tr>
<tr>
<td>I-VPLS</td>
<td>SAP</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>Spoke-SDP</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>Mesh-SDP</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>-</td>
</tr>
<tr>
<td>M-VPLS</td>
<td>SAP</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>Spoke-SDP</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>Mesh-SDP</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>-</td>
</tr>
<tr>
<td>PBB Epipe</td>
<td>SAP</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>Spoke-SDP</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>Mesh-SDP</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>-</td>
</tr>
<tr>
<td>IES</td>
<td>SAP</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>Spoke-SDP (Interface)</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>-</td>
</tr>
<tr>
<td>VPRN</td>
<td>SAP</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>Spoke-SDP (Interface)</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>-</td>
</tr>
<tr>
<td>Note¹</td>
<td>Ethernet-Ring (Data)</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>-</td>
</tr>
</tbody>
</table>
Note¹: Ethernet-Tunnels and Ethernet-Rings are not configurable under all service types. Any service restrictions for MEP direction or MIP support will override the generic capability of the Ethernet-Tunnel or Ethernet-Ring MPs. Check the applicable user guide for applicability.
Configuring ETH-CFM Parameters

In general, see the OAM Diagnostics Guide for information about the ETH-CFM building blocks and functional aspects of tools that are available, as well as configuration examples and some sample tool usage. However, even though those configurations are not service-specific, some of the necessary building blocks required for the service configuration are discussed within this section.

Configuring ETH-CFM requires commands at two different hierarchy levels of the CLI.

The configuration under the config>eth-cfm hierarchy defines the domains, associations, and the applicable global parameters for each of those contexts, including the linkage to the service using the bridge-identifier option. Once this configuration is complete, the Management Points (MPs = MEPs and MIPs) may be defined referencing the appropriate global context.

As described in the OAM Diagnostics Guide, MEPs can be implemented at the service or the facility level. The focus of this manual is on how the ETH-CFM MPs are configured within the service hierarchy level. However, because of the wide range of features that the ITU-T has defined in recommendation Y.1731 (Fault Management, Performance Management and Protection Mechanisms) the features may be applied to other features and hierarchies. For example, Ethernet Ring Protection (G.8032) also make use of various ETH-CFM functions. Different section in this manual may contain ETH-CFM specific material as it applies to that specific feature.

Below is an example of how domains and associations could be constructed, illustrating how the different services are linked to the contexts.

```
config>eth-cfm# info
--------------------------------------------
domain 3 format none level 3
  association 1 format icc-based name "03-0000000101"
    bridge-identifier 100
    exit
  exit
  exit
domain 4 format none level 4
  association 1 format icc-based name "04-0000000102"
    bridge-identifier 100
    remote-mepid 200
    ccm-interval 60
    exit
  exit
```

The following configuration examples illustrate how different services make use of the domain and association configuration. It is important to note that the following examples cannot be all configured at the same instance because the service ID 100 cannot be spread across multiple services. An Epipe, VPLS, and IES service are shown in this example. Refer to the previous table that shows the services and the management points that are supported.
# configure service epipe 100 customer 1 create
* config>service>epipe# info
--------------------------------------------
sap 1/1/2:100.31 create
    eth-cfm
        mep 111 domain 3 association 1 direction down
        mac-address d0:0d:1e:00:01:11
        no shutdown
    exit
    exit
exit
exit
exit
no shutdown
--------------------------------------------

# configure service vpls 100 customer 1 create
* config>service>vpls# info
--------------------------------------------
sap 1/1/2:100.31 create
    eth-cfm
        mep 111 domain 3 association 1 direction down
        mac-address d0:0d:1e:00:01:11
        no shutdown
    exit
    exit
exit
exit
sap 1/1/10:100.31 create
    eth-cfm
        mep 101 domain 4 association 1 direction up
        mac-address d0:0d:1e:00:01:01
        ccm-enable
        no shutdown
    exit
    exit
exit
exit
no shutdown
--------------------------------------------

# configure service ies 100 customer 1 create
config>service>ies# info
--------------------------------------------
interface "test" create
    address 10.1.1.1/30
    sap 1/1/9:100 create
    eth-cfm
        mep 111 domain 3 association 1 direction down
        ccm-enable
        no shutdown
    exit
    exit
exit
A Virtual MEP (vMEP) is a MEP that is configured at the service level rather than on a SAP or SDP binding. A vMEP sends ETH-CFM to all the SAPs and SDP bindings in the VPLS, depending on the type of traffic. If it is multicast traffic, the packets forward out all SAPs and SDP bindings. Unicast traffic is forwarded appropriately based on the type of ETH-CFM packet and the forwarding tables. Packets inbound to a context containing a vMEP performs normal processing and forwarding through the data plane with a copying of the ETH-CFM packet delivered to the local MEP for the appropriate levels. The local MEP will determine whether or not it should process a copied inbound ETH-CFM frame acting in accordance with standard rules.

Configuring a vMEP is similar in concept to placing down MEPs on the individual SAPs and SDP bindings in the associated VPLS. This ensures that packets inbound to the service get redirected to the vMEP for processing. Proper domain nesting must be followed in order to avoid ETH-CFM error conditions.

vMEPs have been expanded to include VPLS, m-VPLS, and I-VPLS contexts. The original B-VPLS vMEP remains supported within that context and maintain the original restrictions (no MIPs and only in a B-VPLS context). A vMEP in a B-VPLS context should be migrated to support the enhancements by adding the “vmep-extensions” command, if the hardware requirements are met. The vmep-extensions command is disabled by default for any vMEP configured within a B-VPLS context. This ensures backwards compatibility and does not impose any new hardware requirements for existing vMEPs in B-VPLS contexts. The “vmep-extensions” command is in effect by default and cannot be negated for any other supported VPLS context, meaning these VPLS contexts must meet explicit hardware requirements.

A vMEP in an I-VPLS context can only extract packets inbound on local SAP and SDP bindings. This extraction does not include packets that are mapped to the I-VPLS from associated B-VPLS context. If this type of extraction is required in an I-VPLS context then UP MEPs are required on appropriate SAPs and SDP bindings in the I-VPLS service.

As with the original vMEP functionality introduced for B-VPLS contexts, DOWN MEPs are supported on the individual SAPs or SDP bindings as long as domain nesting rules are not violated. Of course, local UP MEPs are only supported at the same level as the vMEP otherwise various CCM defect conditions will be raised, assuming CCM is enabled, and leaking of ETH-CFM packets will occur (lower level ETH-CFM packets arriving on a lower level MEP). Domain nesting must be properly deployed to avoid unexpected defect conditions and leaking between ETH-CFM domains.

The vMEP enhancements increase scalability, allow for MIPs and include an optional vmep-filter. MIPs may be configured on the SAPs and SDP-Spokes at or above level of the vMEP.
An optional `vmep-filter` provides a coarse means of silently dropping all ETH-CFM packets that would normally be redirected to the CPU following egress processing. These includes any ETH-CFM level equal to or lower than the vMEP and any level equal to and lower than any other Management Points on the same SAP or SDP binding that includes the `vmep-filter`. MIPs will automatically be deleted when they coexist on the same SAP or spoke-sdp as the `vmep-filter`. Since DOWN MEPs are ingress processed they are supported in combination with a vMEP and operate normally regardless of any `vmep-filter`. Domain nesting rules must be adhered to.

If the operator requires an MP on the SAP or SDP binding an UP MEP may be created at the same level as the vMEP on the appropriate SAP or SDP binding to perform the same function as the filter but at the specific level of the MEP. Scalability needs to be clearly understood because this will redirect the ETH-CFM packets to the CPU (consider using CPU protection introduced in release 8.0r5). Consideration must also be given to the impact this approach could have on the total number of MEPs required. There are a number of other approaches that may lend themselves to the specific network architecture.

vMEP filtering is not supported within the a PBB VPLS since it already provides separation between B-components (typically the core) and I-components (typically the customer).

vMEPs do not support any ETH-AIS functionality and do not support fault propagation functions.

Below is a sample configuration that shows how to configure a vMEP in a VPLS context.

```
config>service# vpls 100 customer 1 create
config>service>vpls$ info
----------------------------------------------
stp
shutdown
exit
eth-cfm
  mep 100 domain 3 association 1
  mac-address d0:0d:1e:00:01:11
  ccm-enable
    no shutdown
  exit
exit
no shutdown
----------------------------------------------
```
Service Management Tasks

This section discusses the following service management tasks:

- Modifying Customer Accounts on page 149
- Deleting Customers on page 151
- Modifying SDPs on page 152
- Deleting SDPs on page 153

Modifying Customer Accounts

To access a specific customer account, you must specify the customer ID. To display a list of customer IDs, use the show service customer command. Enter the parameter (description, contact, phone) and then enter the new information.

**CLI Syntax:**
```
cfg>service# customer customer-id create
  [no] contact contact-information
  [no] description description-string
  [no] multi-service-site customer-site-name [create]
    assignment {port port-id | card slot}
    no assignment
  [no] description description-string
  egress
    agg-rate-limit agg-rate [queue-frame-based-accounting]
    no agg-rate-limit
    policer-control-policy name
    no policer-control-policy
    scheduler-policy scheduler-policy-name
    no scheduler-policy
  [no] scheduler-override
    scheduler scheduler-name [create]
    no scheduler scheduler-name
  ingress
    policer-control-policy name
    no policer-control-policy
    scheduler-policy scheduler-policy-name
    no scheduler-policy
  [no] scheduler-override
    scheduler scheduler-name [create]
    no scheduler scheduler-name
  tod-suite tod-suite-name
  [no] phone phone-number
```
Example:

```plaintext
config>service# customer 27 create
config>service>customer$ description “Western Division”
config>service>customer# contact “John Dough”
config>service>customer# no phone “(650) 237-5102”
```
Deleting Customers

The **no** form of the customer command removes a customer ID and all associated information. All service references to the customer must be shut down and deleted before a customer account can be deleted.

**CLI Syntax:**
```
config>service# no customer customer-id
```

**Example:**
```
config>service# epipe 5 customer 27 shutdown
config>service# epipe 9 customer 27 shutdown
config>service# no epipe 5
config>service# no epipe 9
config>service# no customer 27
```
Modifying SDPs

To access a specific SDP, you must specify the SDP ID. To display a list of SDPs, use the `show service sdp` command. Enter the parameter, such as description, far-end, and lsp, and then enter the new information.

**NOTE:** Once created, you cannot modify the SDP encapsulation type.

**CLI Syntax:**
```
config>service# sdp  sd-id
```

**Example:**
```
config>service# sdp 79
config>service>sdp# description "Path-to-107"
config>service>sdp# shutdown
config>service>sdp# far-end "10.10.10.107"
config>service>sdp# path-mtu 1503
config>service>sdp# no shutdown
```
Deleting SDPs

The **no** form of the `sdp` command removes an SDP ID and all associated information. Before an SDP can be deleted, the SDP must be shutdown and removed (unbound) from all customer services where it is applied.

**CLI Syntax:**

```
cfg>service# no sdp 79
```

**Example:**

```
cfg>service# epipe 5 spoke-sdp 79:5
cfg>service>epipe>sdp# shutdown
cfg>service>epipe>sdp# exit
cfg>service>epipe# exit
cfg>service# no sdp 79
```
Global Services Command Reference

Command Hierarchies

- Customer Commands on page 155
- MRP Commands on page 156
- Oper Group Commands on page 157
- Pseudowire (PW) Commands on page 157
- SDP Commands on page 160
- SAP Commands on page 162
- ETH-CFM Configuration Commands on page 163
- Egress Multicast Group Commands on page 736
- Provider Edge Discovery Policy Commands on page 737
- Show Commands on page 164
- Tools Perform Commands on page 165

Customer Commands

```
config
  — service
    — [no] customer customer-id [create]
      — contact contact-information
      — no contact
      — description description-string
      — no description
      — multi-service-site customer-site-name
      — no multi-service-site customer-site-name
      — assignment {port port-id | card slot-number}
      — no assignment
      — description description-string
      — no description
      — egress
    — [no] or channelor channel agg-rate
      — rate {max | rate}
      — no rate
      — [no] limit-unused-bandwidth
      — [no] queue-frame-based-accounting
    — [no] scheduler-override
      — [no] scheduler scheduler-name
      — rate pir-rate [cir cir-rate]
      — no rate
      — scheduler-policy scheduler-policy-name
```
Global Services Command Reference

— no scheduler-policy
— ingress
  — [no] scheduler-override
    — [no] scheduler scheduler-name
    — rate pir-rate \[cir \text{cir-rate}\]
    — no rate
  — scheduler-policy scheduler-policy-name
  — no scheduler-policy
— tod-suite tod-suite-name
— no tod-suite
— [no] phone phone-number

MRP Commands

config
  — service
    — mrp
      — [no] mrp-policy policy-name
        — description description-string
        — no description
        — scope {exclusive | template}
        — no scope
        — default-action {block | allow}
        — [no] entry entry-id
          — description description-string
          — no description
        — [no] match
          — [no] isid value \[from \text{value to higher-value}\]
          — action {block | allow | end-station}
          — no action
      — copy mrp-policy source-name to dest-name
        — renum old-entry-id to new-entry-id
Oper Group Commands

\[
\text{config} \\
\quad \text{service} \\
\quad \quad \text{oper-group group-name} \\
\quad \quad \quad [\text{create}] \\
\quad \quad \text{no oper-group group-name} \\
\quad \quad \quad \text{bfd-enable interface interface-name dst-ip ip-address} [\text{service service-id}] \\
\quad \quad \quad \text{no bfd-enable} \\
\quad \quad \quad \text{hold-time} \\
\quad \quad \quad \quad \text{group up time} | \text{no group up} \\
\quad \quad \quad \quad \text{group down time} | \text{no group down}
\]

\[
\text{config} \\
\quad \text{service} \\
\quad \quad \text{ies service-id} \ (\text{See IES Services Command Reference on page 1091}) \\
\quad \quad \quad [\text{no}] \text{interface ip-int-name} \\
\quad \quad \quad \quad \text{monitor-oper-group name} \\
\quad \quad \quad \text{no monitor-oper-group name}
\]

\[
\text{config} \\
\quad \text{service} \\
\quad \quad \text{vpls service-id} \ (\text{See VPLS Service Commands on page 745}) \\
\quad \quad \quad [\text{no}] \text{interface ip-int-name} \\
\quad \quad \quad \quad \text{monitor-oper-group name} \\
\quad \quad \quad \text{no monitor-oper-group name}
\]

\[
\text{config} \\
\quad \text{service} \\
\quad \quad \text{vprn service-id} \ (\text{See VPRN Service Configuration Commands on page 1274}) \\
\quad \quad \quad \text{site name} \quad [\text{create}] \\
\quad \quad \quad \quad \text{monitor-oper-group name} \\
\quad \quad \quad \text{no monitor-oper-group name}
\]

Pseudowire (PW) Commands

\[
\text{config} \\
\quad \text{service} \\
\quad \quad \text{pw-routing} \\
\quad \quad \quad [\text{no}] \text{block-on-peer-fault} \\
\quad \quad \quad \text{boot-timer secs} \\
\quad \quad \quad \text{no boot-timer} \\
\quad \quad \quad \text{local-prefix local-prefix} \ [\text{create}] \\
\quad \quad \quad \text{no local-prefix local-prefix} \\
\quad \quad \quad \quad \text{advertise-bgp route-distinguisher rd} \ [\text{community community}] \\
\quad \quad \quad \quad \text{no advertise-bgp route-distinguisher rd} \\
\quad \quad \quad \text{path name} \ [\text{create}] \\
\quad \quad \quad \text{no path name} \\
\quad \quad \quad \quad \text{hop hop-index ip-address} \\
\quad \quad \quad \quad \text{no hop hop-index} \\
\quad \quad \quad \quad \quad [\text{no}] \text{shutdown} \\
\quad \quad \quad \quad \text{retry-count} \ [10..10000] \\
\quad \quad \quad \text{no retry-count} \\
\quad \quad \quad \text{retry-timer secs}
\]
--- no retry-timer
--- spe-address global-id:prefix
--- no spe-address
--- [no] static-route route-name

config
--- service
--- [no] pw-template policy-id [use-provisioned-sdp] [create]
--- accounting-policy acct-policy-id
--- no accounting-policy
--- [no] auto-learn-mac-protect
--- [no] block-on-peer-fault
--- [no] collect-stats
--- [no] control-word
--- [no] control-word
--- [no] disable-aging
--- [no] disable-learning
--- [no] discard-unknown-source
--- ingress
--- [no] fast-leave
--- import policy-name
--- no import
--- last-member-query-interval 1/10 seconds
--- no last-member-query-interval
--- max-num-groups max-num-groups
--- no max-num-groups
--- query-interval seconds
--- no query-interval
--- query-response-interval seconds
--- no query-response-interval
--- robust-count robust-count
--- no robust-count
--- [no] send-queries
--- version version
--- no version
--- egress
--- filter ipv6 ipv6-filter-id
--- filter ip ip-filter-id
--- filter mac mac-filter-id
--- [no] filter [ip ip-filter-id] [mac mac-filter-id] [ipv6 ipv6-filter-id]
--- mfib-allowed-mda-destinations
--- [no] mda mda-id
--- qos network-policy-id port-redirect-group queue-group-name [instance instance-id]
--- [no] qos
--- [no] force-vlan-vc-forwarding
--- hash-label [signal-capability]
--- no hash-label
--- igmp-snooping
--- [no] fast-leave
--- import policy-name
--- no import
--- last-member-query-interval 1/10 seconds
--- no last-member-query-interval
--- max-num-groups max-num-groups
--- no max-num-groups
--- query-interval seconds
--- no query-interval
--- query-response-interval seconds
--- no query-response-interval
--- robust-count robust-count
--- no robust-count
--- [no] send-queries
--- version version
--- no version
— limit-mac-move {blockable | non-blockable}
— no limit-mac-move
— [no] mac-pinning
— max-nbr-mac-addr table-size
— no max-nbr-mac-addr
— restrict-protected-src alarm-only
— restrict-protected-src [discard-frame]
— no restrict-protected-src
— [no] sdp-exclude group-name
— [no] sdp-include group-name
— split-horizon-group group-name [residential-group]
— no split-horizon-group
  — [no] auto-learn-mac-protect
  — description description-string
  — no description
  — restrict-protected-src alarm-only
  — restrict-protected-src [discard-frame]
  — no restrict-protected-src
  — [no] restrict-unprotected-dst
— vc-type {ether | vlan}
— vlan-vc-tag 0..4094
— no vlan-vc-tag
SDP Commands

```
cfg  
  service  
    sdp sdp-id [gre | mpls | l2tpv3] [create]  
    no sdp sdp-id  
    accounting-policy acct-policy-id  
    no accounting-policy  
    [no] adv-mtu-override  
    binding  
      port [port-id | lag-id]  
      no port  
      pw-port pw-port-id [vc-id vc-id] [create]  
      no pw-port pw-port-id  
      egress  
        [no] shaper int-dest-id int-dest-id  
        encap-type {dot1q/qinq}  
        no encap-type  
        [no] shutdown  
        vc-type {ether | vlan}  
        no vc-type  
        vlan-vc-tag vlan-id  
        no vlan-vc-tag  
    [no] bgp-tunnel  
    booking-factor percentage  
    no booking-factor  
    class-forwarding [default-lsp lsp-name]  
    no class-forwarding  
      [no] enforce-diffserv-lsp-fc  
      fc {be | l2 | af | l1 | h2 | ef | h1 | nc} lsp lsp-name  
      no fc {be | l2 | af | l1 | h2 | ef | h1 | nc}  
      multicast-lsp lsp-name  
      no multicast-lsp  
      [no] shutdown  
    [no] collect-stats  
    description description-string  
    no description  
    far-end ip-address | {node-id node-id} [global-id global-id]}  
    no far-end  
    keep-alive  
      hello-time seconds  
      no hello-time  
      hold-down-time seconds  
      no hold-down-time  
      max-drop-count count  
      no max-drop-count  
      message-length octets  
      no message-length  
      [no] shutdown  
      timeout timeout  
      no timeout  
    [no] ldp  
    [no] lsp lsp-name  
    metric metric  
    no metric
```
— [no] mixed-lsp-mode
  — [no] sd-p-revert-time seconds | infinite
— network-domain network-domain-name
— no network-domain
— path-mtu octets
— no path-mtu
— pbb-etype [0x0600..0xffff]
— no pbb-etype
— [no] shutdown
— [no] sd-p-group group-name
— signaling [off | tldp|bgp]
— tunnel-far-end ip-address
— no tunnel-far-end [ip-address]
— source-bmac-lsb MAC-lsb control-pw-vc-vc-id vc-id
— vlan-vc-etype 0x0600..0xffff
— sd-p-group
  — group-name group-name value group-value
  — no group-name group-name
SAP Commands

```plaintext
cfg
  - service
    - epipe
      - sap sap-id [create] [no-endpoint]
      - sap sap-id [create] endpoint endpoint-name
      - no sap sap-id
    - ies
      - sap sap-id [create]
      - no sap sap-id
    - vpls
      - sap sap-id [split-horizon-group group-name] [create]
      - no sap sap-id
    - system
      - ethernet
        - [no] new-qinq-untagged-sap
```
ETH-CFM Configuration Commands

```
config
  — eth-cfm
    — domain md-index [format {dns | mac | none | string}] name md-name level level
    — domain md-index
    — no domain md-index
      — association ma-index [format {icc-based | integer | string | vid | vpn-id}] name ma-name
      — association ma-index
      — no association ma-index
        — auto-mep-discovery
        — [no] auto-mep-discovery
        — [no] bridge-identifier bridge-id
          — mhf-creation {default | none | explicit | static}
          — no mhf-creation
          — mip-ltr-priority priority
          — no mip-ltr-priority
          — vlan vlan-id
          — no vlan
          — ccm-interval {10ms | 100ms | 1 | 10 | 60 | 600}
          — no ccm-interval
          — [no] ccm-hold-time
          — ccm-hold-time
          — remote-mep mep-id remote-mac {unicast-da | default}
          — [no] remote-mepid mep-id
        — redundancy
          — mc-lag
            — [no] propagate-hold-time seconds
            — [no] standby-mep-shutdown
        — slm
          — [no] inactivity-timer timeout
        — system
          — grace-tx-enable
```
Show Commands

show
  service
    customer [customer-id] [site customer-site-name]
  —
  [dyn-script] [description] pw-routing [local-prefix] [static-route] [paths] [all]
  pw-routing route-table [all-routes]
  pw-routing route-table summary
  pw-template
  sail-type2-using global-id[.prefix[.ac-id]]
  sdp sdp-id pw-port [pw-port-id]
  sdp [consistent] [inconsistent] [na] egressifs
  sdp sdp-id keep-alive-history
  sdp far-end ip-address keep-alive-history
  sdp [sdp-id] [detail]
  sdp far-end ip-address [detail]
  sdp-group group-name
  sdp-group-using
  sdp-group [sdp-id[.vc-id]] | far-end ip-address]
  service-using [epipe] [ies] [vpls] [vprn] [mirror] [b-vpls] [m-vpls] [iipe] [sdp sdp-
  id] [customer customer-id]
  tail-type2-using global-id[.prefix[.ac-id]]
  —
  eth-cfm
  —
  association [ma-index] [detail]
  cfm-stack-table [port [port-id [vlan vlan-id]]] sdp sdp-id[.vc-id]][level 0..7] [direction up | 
  down]
  cfm-stack-table
  cfm-stack-table port [ [all-ports | all-sdps | all-virtuals]] [level 0..7] [direction up | down]
  cfm-stack-table port-id [vlan qtag [.qtag]] [level 0..7] [direction up | down]
  cfm-stack-table sdp sdp-id[.vc-id] [level 0..7] [direction up | down]
  cfm-stack-table virtual service-id [level 0..7]
  cfm-stack-table facility [ [all-ports|all-lags|all-lag-ports|all-tunnel-meps|all-router-inter-
  faces]] [level 0..7] [direction up|down]
  cfm-stack-table facility lag id [tunnel 1..4094] [level 0..7] [direction up|down]
  cfm-stack-table facility port id [level 0..7] [direction up|down]
  cfm-stack-table facility router-interface ip-int-name [level 0..7] [direction up|down]
  domain [md-index] [association ma-index | all-associations] [detail]
  mep mep-id domain md-index association ma-index [loopback] [linktrace]
  mep mep-id domain md-index association ma-index remote-mepid mep-id | all-remote-
  mepids
  mep mep-id domain md-index association ma-index eth-test-results [remote-peer mac-
  address]
  mep mep-id domain md-index association ma-index one-way-delay-test [remote-peer mac-
  address]
  mep mep-id domain md-index association ma-index two-way-delay-test [remote-peer mac-
  address]
  mep mep-id domain md-index association ma-index two-way-slm-test [remote-peer mac-
  address]
  system-config
Tools Perform Commands

```
tools
  — perform
  — service
    — id service-id
    — loopback
      — sap sap-id start mode [mac-swap [mac ieee-address [all]]]
      — sap sap-id stop
      — sdp sdp-id:vc-id start mode [mac-swap [mac ieee-address [all]]]
      — sdp sdp-id:vc-id stop
```
Global Service Configuration Commands

Generic Commands

shutdown

Syntax  
[no] shutdown

Context  
config>eth-cf>mep  
config>service>sdp  
config>service>sdp>class-forwarding  
config>service>sdp>keep-alive  
config>service>sdp>forwarding-class  
config>service>pw-routing>hop  
config>service>sdp>binding>pw-port

Description  
This command administratively disables an entity. When disabled, an entity does not change, reset, or remove any configuration settings or statistics.

The operational state of the entity is disabled as well as the operational state of any entities contained within. Many objects must be shut down before they may be deleted.

Services are created in the administratively down (shutdown) state. When a no shutdown command is entered, the service becomes administratively up and then tries to enter the operationally up state. Default administrative states for services and service entities is described below in Special Cases.

The no form of this command places the entity into an administratively enabled state.

Special Cases

Service Admin State — Bindings to an SDP within the service will be put into the out-of-service state when the service is shutdown. While the service is shutdown, all customer packets are dropped and counted as discards for billing and debugging purposes.

SDP (global) — When an SDP is shutdown at the global service level, all bindings to that SDP are put into the out-of-service state and the SDP itself is put into the administratively and operationally down states. Packets that would normally be transmitted using this SDP binding will be discarded and counted as dropped packets.

SDP (service level) — Shutting down an SDP within a service only affects traffic on that service from entering or being received from the SDP. The SDP itself may still be operationally up for other services.

SDP Keepalives — Enables SDP connectivity monitoring keepalive messages for the SDP ID. Default state is disabled (shutdown) in which case the operational state of the SDP-ID is not affected by the keepalive message state.
description

Syntax  
```
description description-string
no description
```

Context  
config>service>customer
config>service>customer>multi-service-site
config>service>pw-template
config>service>pw-template>split-horizon-group
config>service>sdp

Description  
This command creates a text description stored in the configuration file for a configuration context.

The **description** command associates a text string with a configuration context to help identify the content in the configuration file.

The **no** form of this command removes the string from the configuration.

Default  
No description associated with the configuration context.

Parameters  
`string` — The description character string. Allowed values are any string up to 80 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

new-qinq-untagged-sap

Syntax  
```
[no] new-qinq-untagged-sap
```

Context  
config>system>ethernet

Description  
This command controls the behavior of QinQ SAP y.0 (for example, 1/1/1:3000.0). If the flag is not enabled (no new-qinq-untagged-sap), the y.0 SAP works the same as the y.* SAP (for example, 1/1/1:3000.*); all frames tagged with outer VLAN y and no inner VLANs or inner VLAN x where inner VLAN x is not specified in a SAP y.x configured on the same port (for example, 1/1/1:3000.10).

If the flag is enabled, then the following new behavior immediately applies to all existing and future y.0 SAPs: the y.0 SAP maps all the ingress frames tagged with outer tag VLAN-id of y (qinq-etype) and no inner tag or with inner tag of VLAN-id of zero (0).

Default  
no new-qinq-untagged-sap. This setting ensures that there will be no disruption for existing usage of this SAP type.
Customer Management Commands

customer

Syntax   customer  customer-id [create]
         no customer  customer-id

Context  config>service

Description This command creates a customer ID and customer context used to associate information with a particular customer. Services can later be associated with this customer at the service level.

Each customer-id must be unique. The create keyword must follow each new customer customer-id entry.

Enter an existing customer customer-id (without the create keyword) to edit the customer’s parameters.

Default customer 1 always exists on the system and cannot be deleted.

The no form of this command removes a customer-id and all associated information. Before removing a customer-id, all references to that customer in all services must be deleted or changed to a different customer ID.

Parameters customer-id — Specifies the ID number to be associated with the customer, expressed as an integer.

Values  1 — 2147483647

create — This keyword is required when first creating the configuration context. Once the context is created, it is possible to navigate into the context without the create keyword.

contact

Syntax   contact  contact-information
         no contact  contact-information

Context  config>service>customer

Description This command allows you to configure contact information for a customer.

Include any customer-related contact information such as a technician’s name or account contract name.

Default No contact information is associated with the customer-id.

The no form of this command removes the contact information from the customer ID.

Parameters contact-information — The customer contact information entered as an ASCII character string up to 80 characters in length. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes. Any printable, seven bit ASCII characters may be used within the string.
multi-service-site

Syntax  multi-service-site customer-site-name [create]
        no multi-service-site customer-site-name

Context  config>service>customer

Description  This command creates a new customer site or edits an existing customer site with the customer-site-name parameter. A customer site is an anchor point to create an ingress and egress virtual scheduler hierarchy. When a site is created, it must be assigned to a chassis slot or port. When scheduler policies are defined for ingress and egress, the scheduler names contained in each policy are created according to the parameters defined in the policy. Multi-service customer sites exist for the sole purpose of creating a virtual scheduler hierarchy and making it available to queues on multiple Service Access Points (SAPs).

The scheduler policy association with the customer site normally prevents the scheduler policy from being deleted until after the scheduler policy is removed from the customer site. The multi-service-site object will generate a log message indicating that the association was deleted due to scheduler policy removal.

When the multi-service customer site is created, an ingress and egress scheduler policy association does not exist. This does not prevent the site from being assigned to a chassis slot or prevent service SAP assignment. After the site has been created, the ingress and egress scheduler policy associations can be assigned or removed at any time.

Default  None — Each customer site must be explicitly created.

Parameters  customer-site-name — Each customer site must have a unique name within the context of the customer. If customer-site-name already exists for the customer ID, the CLI context changes to that site name for the purpose of editing the site scheduler policies or assignment. Any modifications made to an existing site will affect all SAPs associated with the site. Changing a scheduler policy association may cause new schedulers to be created and existing queues on the SAPs to no longer be orphaned. Existing schedulers on the site may cease to exist, causing queues relying on that scheduler to be orphaned.

If the customer-site-name does not exist, it is assumed that an attempt is being made to create a site of that name in the customer ID context. The success of the command execution depends on the following:

- The maximum number of customer sites defined for the chassis has not been met.
- The customer-site-name is valid.
- The create keyword is included in the command line syntax (if the system requires it).

When the maximum number of customer sites has been exceeded a configuration error occurs; the command will not execute and the CLI context will not change.

If the customer-site-name is invalid, a syntax error occurs; the command will not execute and the CLI context will not change.

Values  Valid names consist of any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

phone

Syntax  [no] phone string
This command adds telephone number information for a customer ID.

**Default**

none

The no form of this command removes the phone number value from the customer ID.

**Parameters**

`string` — The customer phone number entered as an ASCII string string up to 80 characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes. Any printable, seven bit ASCII characters may be used within the string.

### Assignment

**Syntax**

```
assignment {port port-id | card slot-number}
no assignment
```

**Context**

config>service>customer>multi-service-site

**Description**

This command assigns a multi-service customer site to a specific chassis slot, port, or channel. This allows the system to allocate the resources necessary to create the virtual schedulers defined in the ingress and egress scheduler policies as they are specified. This also verifies that each SAP assigned to the site exists within the context of the proper customer ID and that the SAP was configured on the proper slot, port, or channel. The assignment must be given prior to any SAP associations with the site.

The no form of the command removes the port, channel, or slot assignment. If the customer site has not yet been assigned, the command has no effect and returns without any warnings or messages.

**Default**

None

**Parameters**

`port port-id` — The port keyword is used to assign the multi-service customer site to the port-id given.

When the multi-service customer site has been assigned to a specific port, all SAPs associated with this customer site must be on a service owned by the customer and created on the defined port. The defined port or channel must already have been pre-provisioned on the system but need not be installed when the customer site assignment is made.

**Syntax:**

```
port-id[:encap-val]
```

**Values**

<table>
<thead>
<tr>
<th>Values</th>
<th>port-id</th>
<th>slot/mda/port</th>
<th>lag-id</th>
<th>lag-id</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>lag</td>
<td>keyword</td>
<td>id</td>
<td>1 — 64</td>
</tr>
</tbody>
</table>

**Values**

`card slot-number` — The card keyword is used to assign the multi-service customer site to the slot-number given. When the multi-service customer site has been assigned to a specific slot in the chassis, all SAPs associated with this customer site must be on a service owned by the customer and created on the defined chassis slot. The defined slot must already have been pre-provisioned on the system but need not be installed when the customer site assignment is made.

**Values**

```
Any pre-provisioned slot number for the chassis type that allows SAP creation
```

```
slot-number 1 — 10
```
Customer Management Commands

**ingress**

**Syntax**
-ingress

**Context**
-config>service>customer>multi-service-site

**Description**
This command enables the context to configure the ingress node associate an existing scheduler policy name with the customer site. The ingress node is an entity to associate commands that complement the association.

**egress**

**Syntax**
-egress

**Context**
-config>service>customer>multi-service-site

**Description**
This command enables the context to configure the egress node associate an existing scheduler policy name with the customer site. The egress node is an entity to associate commands that complement the association.

or channel or channel **agg-rate**

**Syntax**
-[no] agg-rate

**Context**
-config>service>customer>multi-service-site>egress

**Description**
This command is used to control an HQoS aggregate rate limit. It is used in conjunction with the following parameter commands: rate, limit-unused-bandwidth, and queue-frame-based-accounting.

**rate**

**Syntax**
-rate {max | rate}
-no rate

**Context**
-config>service>customer>multi-service-site>egress>agg-rate

**Description**
This command defines the enforced aggregate rate for all queues associated with the agg-rate context. A rate must be specified for the agg-rate context to be considered to be active on the context’s object (SAP, subscriber, VPORT etc.).

**limit-unused-bandwidth**

**Syntax**
-[no] limit-unused-bandwidth

**Context**
-config>service>customer>multi-service-site>egress>agg-rate

**Description**
This command is used to enable (or disable) aggregate rate overrun protection on the agg-rate context.
queue-frame-based-accounting

Syntax  [no] queue-frame-based-accounting
Context config>service>customer>multi-service-site>egress>agg-rate
Description This command is used to enabled (or disable) frame based accounting on all queues associated with the agg-rate context. Only supported on Ethernet ports. Not supported on HSMDA Ethernet ports.

scheduler-override

Syntax  [no] scheduler-override
Context config>service>customer>multi-service-site>ingress
config>service>customer>multi-service-site>egress
Description This command specifies the set of attributes whose values have been overridden by management on this virtual scheduler. Clearing a given flag will return the corresponding overridden attribute to the value defined on the SAP's ingress scheduler policy.

scheduler

Syntax  [no] scheduler scheduler-name
Context config>service>customer>multi-service-site>ingress>sched-override
config>service>customer>multi-service-site>egress>sched-override
Description This command can be used to override specific attributes of the specified scheduler name.

A scheduler defines bandwidth controls that limit each child (other schedulers and queues) associated with the scheduler. Scheduler objects are created within the hierarchical tiers of the policy. It is assumed that each scheduler created will have queues or other schedulers defined as child associations. The scheduler can be a child (take bandwidth from a scheduler in a higher tier, except for schedulers created in tier 1). A total of 32 schedulers can be created within a single scheduler policy with no restriction on the distribution between the tiers.

Each scheduler must have a unique name within the context of the scheduler policy; however the same name can be reused in multiple scheduler policies. If scheduler-name already exists within the policy tier level (regardless of the inclusion of the keyword create), the context changes to that scheduler name for the purpose of editing the scheduler parameters. Modifications made to an existing scheduler are executed on all instantiated schedulers created through association with the policy of the edited scheduler. This can cause queues or schedulers to become orphaned (invalid parent association) and adversely affect the ability of the system to enforce service level agreements (SLAs).

If the scheduler-name exists within the policy on a different tier (regardless of the inclusion of the keyword create), an error occurs and the current CLI context will not change.

If the scheduler-name does not exist in this or another tier within the scheduler policy, it is assumed that an attempt is being made to create a scheduler of that name. The success of the command execution is dependent on the following:

1. The maximum number of schedulers has not been configured.
2. The provided scheduler-name is valid.
3. The create keyword is entered with the command if the system is configured to require it (enabled in the environment create command).

When the maximum number of schedulers has been exceeded on the policy, a configuration error occurs and the command will not execute, nor will the CLI context change.

If the provided scheduler-name is invalid according to the criteria below, a name syntax error will occur, the command will not execute, and the CLI context will not change.

**Parameters**

scheduler-name — The name of the scheduler.

**Values**

Valid names consist of any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

**Default**

None. Each scheduler must be explicitly created.

create — This optional keyword explicitly specifies that it is acceptable to create a scheduler with the given scheduler-name. If the create keyword is omitted, scheduler-name is not created when the system environment variable create is set to true. This safeguard is meant to avoid accidental creation of system objects (such as schedulers) while attempting to edit an object with a mistyped name or ID. The keyword has no effect when the object already exists.

**rate**

**Syntax**

rate pir-rate [cir cir-rate]

no rate

**Context**

config>service>customer>multi-service-site>ingress>sched-override>scheduler

config>service>customer>multi-service-site>egress>sched-override>scheduler

**Description**

This command can be used to override specific attributes of the specified scheduler rate.

The **rate** command defines the maximum bandwidth that the scheduler can offer its child queues or schedulers. The maximum rate is limited to the amount of bandwidth the scheduler can receive from its parent scheduler. If the scheduler has no parent, the maximum rate is assumed to be the amount available to the scheduler. When a parent is associated with the scheduler, the CIR parameter provides the scheduler’s amount of bandwidth to be considered during the parent schedulers ‘within CIR’ distribution phase.

The actual operating rate of the scheduler is limited by bandwidth constraints other than its maximum rate. The scheduler’s parent scheduler may not have the available bandwidth to meet the scheduler’s needs or the bandwidth available to the parent scheduler could be allocated to other child schedulers or child queues on the parent based on higher priority. The children of the scheduler may not need the maximum rate available to the scheduler due to insufficient offered load or limits to their own maximum rates.

When a scheduler is defined without specifying a rate, the default rate is **max**. If the scheduler is a root scheduler (no parent defined), the default maximum rate must be changed to an explicit value. Without this explicit value, the scheduler will assume that an infinite amount of bandwidth is available and allow all child queues and schedulers to operate at their maximum rates.

The **no** form of this command returns all queues created with this queue-id by association with the QoS policy to the default PIR and CIR parameters.
Parameters

pir-rate — The pir parameter accepts a step multiplier value that specifies the multiplier used to determine the PIR rate at which the queue will operate. A value of 0 to 100000000 or the keyword max or sum is accepted. Any other value will result in an error without modifying the current PIR rate.

To calculate the actual PIR rate, the rate described by the queue’s rate is multiplied by the pir-rate.

The SAP ingress context for PIR is independent of the defined forwarding class (fc) for the queue. The default pir and definable range is identical for each class. The PIR in effect for a queue defines the maximum rate at which the queue will be allowed to forward packets in a given second, thus shaping the queue’s output.

The PIR parameter for SAP ingress queues do not have a negate (no) function. To return the queues PIR rate to the default value, that value must be specified as the PIR value.

Values 1 — 100000000, max

Default max

cir cir-rate — The cir parameter accepts a step-multiplier value that specifies the multiplier used to determine the CIR rate at which the queue will operate. A value of 0 to 100000000 or the keyword max or sum are accepted. Any other value will result in an error without modifying the current CIR rate.

To calculate the actual CIR rate, the rate described by the rate pir pir-rate is multiplied by the cir cir-rate. If the cir is set to max, then the CIR rate is set to infinity.

The SAP ingress context for CIR is dependent on the defined forwarding class (fc) for the queue. The default CIR and definable range is different for each class. The CIR in effect for a queue defines both its profile (in or out) marking level as well as the relative importance compared to other queues for scheduling purposes during congestion periods.

Values 0 — 10000000, max, sum

Default sum

scheduler-policy

Syntax scheduler-policy scheduler-policy-name
no scheduler-policy

Context config>service>customer>multi-service-site>ingress
config>service>customer>multi-service-site>egress

Description This command applies an existing scheduler policy to an ingress or egress scheduler used by SAP queues associated with this multi-service customer site. The schedulers defined in the scheduler policy can only be created once the customer site has been appropriately assigned to a chassis port, channel or slot. Scheduler policies are defined in the config>qos>scheduler-policy scheduler-policy-name context.

The no form of this command removes the configured ingress or egress scheduler policy from the multi-service customer site. When the policy is removed, the schedulers created due to the policy are removed also making them unavailable for the ingress SAP queues associated with the customer site. Queues that lose their parent scheduler association are deemed to be orphaned and are no longer subject to a virtual scheduler.

The SAPs that have ingress queues reliant on the removed schedulers enter into an operational state depicting the orphaned status of one or more queues. When the no scheduler-policy command is executed, the customer site ingress or egress node will not contain an applied scheduler policy.
scheduler-policy-name: — The scheduler-policy-name parameter applies an existing scheduler policy that was created in the config>qos>scheduler-policy scheduler-policy-name context to create the hierarchy of ingress or egress virtual schedulers. The scheduler names defined within the policy are created and made available to any ingress or egress queues created on associated SAPs.

Values Any existing valid scheduler policy name.

tod-suite

Syntax tod-suite tod-suite-name
no tod-suite

Context config>service>cust>multi-service-site

Description This command applies a time-based policy (filter or QoS policy) to the multiservice site. The suite name must already exist in the config>cron context.

Default no tod-suite

Parameters tod-suite-name — Specifies collection of policies (ACLs, QoS) including time-ranges. Only the scheduler-policy part of the tod-suite is taken into account. The suite can be applied to more than one multiservice-site.
MRP Commands

mrp

Syntax  mrp
Context  config>service
Description  This command configures a Multi-service Route Processor (MRP).

mrp-policy

Syntax  [no] mrp-policy policy-name
Context  config>service>mrp
Description  This command enables the context for a MRP policy. The mrp-policy specifies either a forward or a drop action for the Group BMAC attributes associated with the ISIDs specified in the match criteria. The mrp-policy can be applied to multiple BVPLS services as long as the scope of the policy is template.

Any changes made to the existing policy, using any of the sub-commands, will be applied immediately to all services where this policy is applied. For this reason, when many changes are required on a mrp-policy, it is recommended that the policy be copied to a work area. That work-in-progress policy can be modified until complete and then written over the original mrp-policy. Use the config mrp-policy copy command to maintain policies in this manner.

The no form of the command deletes the mrp-policy. An MRP policy cannot be deleted until it is removed from all the SAPs or SDPs where it is applied.

Default  no mrp-policy is defined
Parameters  policy-name — Specifies the redirect policy name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

create — This keyword is required when first creating the configuration context. Once the context is created, it is possible to navigate into the context without the create keyword.

scope

Syntax  scope {exclusive | template}
no scope
Context  config>service>mrp>mrp-policy
Description  This command configures the filter policy scope as exclusive or template. If the scope of the policy is template and is applied to one or more services, the scope cannot be changed.

The no form of the command sets the scope of the policy to the default of template.
MRP Commands

**Default**

**Parameters**

- exclusive — When the scope of a policy is defined as exclusive, the policy can only be applied to a single entity (SAP or SDP). Attempting to assign the policy to a second entity will result in an error message. If the policy is removed from the entity, it will become available for assignment to another entity.

- template — When the scope of a policy is defined as template, the policy can be applied to multiple SAPs or network ports.

---

**default-action**

**Syntax**

```
default-action {block | allow}
```

**Context**

`config>service>mrp>mrp-policy`

**Description**

This command specifies the action to be applied to the MMRP attributes (Group BMACs) whose ISIDs do not match the specified criteria in all of the entries of the mrp-policy.

When multiple default-action commands are entered, the last command will overwrite the previous command.

**Default**

default-action-allow

**Parameters**

- block — Specifies that all MMRP attributes will not be declared or registered unless there is a specific mrp-policy entry which causes them to be allowed on this SAP/SDP.

- allow — Specifies that all MMRP attributes will be declared and registered unless there is a specific mrp-policy entry which causes them to be blocked on this SAP/SDP.

---

**entry**

**Syntax**

```
[no] entry entry-id
```

**Context**

`config>service>mrp>mrp-policy`

**Description**

This command creates or edits an mrp-policy entry. Multiple entries can be created using unique entry-id numbers within the policy. The implementation exits the policy on the first match found and executes the actions in accordance with the accompanying action command. For this reason, entries must be sequenced correctly from most to least explicit. An entry may not have any match criteria defined (in which case, everything matches) but must have at least the keyword action for it to be considered complete. Entries without the action keyword will be considered incomplete and hence will be rendered inactive.

The no form of the command removes the specified entry from the mrp-policy. Entries removed from the mrp-policy are immediately removed from all services where the policy is applied.

**Default**

none

**Parameters**

- entry-id — An entry-id uniquely identifies a match criteria and the corresponding action. It is recommended that multiple entries be given entry-ids in staggered increments. This allows users to insert a new entry in an existing policy without requiring renumbering of all the existing entries.

**Values**

1-65535
create — Keyword; required when first creating the configuration context. Once the context is created, one can navigate into the context without the create keyword.

match

Syntax `[no] match`

Context `config>service>mrp>mrp-policy>entry`

Description This command creates the context for entering/editing match criteria for the mrp-policy entry. When the match criteria have been satisfied the action associated with the match criteria is executed. In the current implementation just one match criteria (ISID based) is possible in the entry associated with the mrp-policy. Only one match statement can be entered per entry.

The `no` form of the command removes the match criteria for the entry-id.

isid

Syntax `[no] isid value | from value to higher-value`

Context `config>service>mrp>mrp-policy>entry>match`

Description This command configures an ISID value or a range of ISID values to be matched by the mrp-policy parent when looking at the related MMRP attributes (Group BMACs). The pbb-etype value for the related SAP (inherited from the ethernet port configuration) or for the related SDP binding (inherited from SDP configuration) will be used to identify the ISID tag.

Multiple isid statements are allowed under a match node. The following rules govern the usage of multiple isid statements:

• overlapping values are allowed:
  – isid from 1 to 10
  – isid from 5 to 15
  – isid 16

• the minimum and maximum values from overlapping ranges are considered and displayed. The above entries will be equivalent with “isid from 1 to 16” statement.

• there is no consistency check with the content of isid statements from other entries. The entries will be evaluated in the order of their IDs and the first match will cause the implementation to execute the associated action for that entry and then to exit the mrp-policy.

• If there are no isid statements under a match criteria but the mac-filter type is isid the following behaviors apply for different actions:
  – For end-station – it treats any ISID value as no match and goes to next entry or default action which must be “block” in this case
  – For allow – it treats any ISID value as a match and allows it
  – For block – it treats any ISID value as a match and blocks it

The `no` form of the command can be used in two ways:
no isid - removes all the previous statements under one match node

no isid value | from value to higher-value - removes a specific ISID value or range. Must match a previously used positive statement: for example if the command “isid 16 to 100” was used using “no isid 16 to 50” will not work but “no isid 16 to 100 will be successful.

**Default** no isid

**Parameters**

- value or higher-value — Specifies the ISID value in 24 bits. When just one present identifies a particular ISID to be used for matching.
- from value to higher-value — Identifies a range of ISIDs to be used as matching criteria.

**action**

**Syntax**

```
action {block | allow | end-station}
```

**Context** config>service>mrp>mrp-policy>entry

**Description**

This command specifies the action to be applied to the MMRP attributes (Group BMACs) whose ISIDs match the specified ISID criteria in the related entry.

The action keyword must be entered for the entry to be active. Any filter entry without the action keyword will be considered incomplete and will be inactive. If neither keyword is specified (no action is used), this is considered a No-Op policy entry used to explicitly set an entry inactive without modifying match criteria or removing the entry itself. Multiple action statements entered will overwrite previous actions parameters when defined. To remove a parameter, use the no form of the action command with the specified parameter.

The **no** form of the command removes the specified action statement. The entry is considered incomplete and hence rendered inactive without the action keyword.

**Default** no action

**Parameters**

- block — Specifies that the matching MMRP attributes will not be declared or registered on this SAP/SDP.
- allow — Specifies that the matching MMRP attributes will be declared and registered on this SAP/SDP.
- end-station — Specifies that an end-station emulation is present on this SAP/SDP for the MMRP attributes related with matching ISIDs. Equivalent action with the block keyword on that SAP/SDP—the attributes associated with the matching ISIDs do not get declared or registered on the SAP/SDP. The matching attributes on the other hand are mapped as static MMRP entries on the SAP/SDP which implicitly instantiates in the data plane as a MFIB entry associated with that SAP/SDP for the related Group BMAC. For the other SAPs/SDPs in the BVPLS with MRP enabled (no shutdown) this means permanent declaration of the matching attributes, same as in the case when the IVPLS instances associated with these ISIDs were locally configured.

If an mrp-policy has end-station action in one entry, the only default action allowed in the policy is block. Also no other actions are allowed to be configured in other entry configured under the policy.

This policy will apply even if the MRP is shutdown on the local SAP/SDP or for the whole BVPLS to allow for manual creation of MMRP entries in the data plane. Specifically the following rules apply:
– If service vpls mrp shutdown then MMRP on all SAP/SDPs is shutdown - MRP PDUs pass-through transparently
– If service vpls mrp no shutdown and endstation statement (even with no ISID values in the related match statement) is used in a mrp-policy applied to SAP/SDP - no declaration is sent on SAP/SDP. The provisioned ISIDs in the match statement are registered on that SAP/SDP and are propagated on all the other MRP enabled endpoints.

copy

**Syntax**
```
copy mrp-policy source-name to dest-name
```

**Context**
```
config>service>mrp
```

**Description**
This command copies existing mrp-policy list entries for a specific policy name to another policy name. The copy command is a configuration level maintenance tool used to create new mrp-policy using existing mrp-policy.

An error will occur if the destination policy name exists.

**Parameters**
- `mrp-policy` — Indicates that source-name and dest-name are MRP policy names.
- `source-name` — Identifies the source mrp-policy from which the copy command will attempt to copy. The mrp-policy with this name must exist for the command to be successful.
- `dest-name` — Identifies the destination mrp-policy to which the copy command will attempt to copy. If the mrp-policy with dest-name exist within the system an error message is generated.

renum

**Syntax**
```
renum old-entry-id to new-entry-id
```

**Context**
```
config>service>mrp>mrp-policy
```

**Description**
This command renumbers existing MRP policy entries to properly sequence policy entries. This may be required in some cases since the implementation exits when the first match is found and executes the actions according to the accompanying action command. This requires that entries be sequenced correctly from most to least explicit.

**Parameters**
- `old-entry-id` — Specifies the entry number of an existing entry.
  
  **Values**
  
  1-65535

- `new-entry-id` — Specifies the new entry number to be assigned to the old entry. If the new entry exists, an error message is generated.
Oper Group Commands

Oper Group Commands

oper-group

Syntax  oper-group  group-name  [create]
        no  oper-group  group-name

Context  config>service

Description  This command creates a system-wide group name which can be used to associate a number of service objects (for example, SAPs or pseudowires). The status of the group is derived from the status of its members. The status of the group can then be used to influence the status of non-member objects. For example, when a group status is marked as down, the object(s) that monitor the group change their status accordingly.

The no form of the command removes the group. All the object associations need to be removed before the no command can be executed.

no oper-group

Parameters  group-name — specifies the operational group identifier up to 32 characters in length.

create — This keyword is required when first creating the configuration context. Once the context is created, it is possible to navigate into the context without the create keyword.

bfd-enable

Syntax  bfd-enable  interface  interface-name  dst-ip  ip-address  [service  service-id]
        no  bfd-enable

Context  config>service>oper-group

Description  This command associates a BFD sessions with the named oper-group so that if the BFD session fails then the oper-group is changed to operationally down and all monitoring interfaces should also be brought operationally down.

Default  None

Parameters  interface — Specifies the source interface for the BFD sessions to be monitored for the associated oper-group.

dst-ip — Specifies the destination IP address for the BFD sessions to be monitored for the associated oper-group.

service — Specifies the service context in which the BFD session exists if it is not in the base routing context.
hold-time

Syntax  hold-time
Context  config>service>oper-group
Description  This command enables the context to configure hold time information.

group up

Syntax  group up time | no group up
Context  config>service>oper-group>hold-time
Description  This command configures the number of seconds to wait before notifying clients monitoring this group when its operational status transitions from down to up. A value of zero indicates that transitions are reported immediately to monitoring clients. The up time option is a must to achieve fast convergence: when the group comes up, the monitoring MH site which tracks the group status may wait without impacting the overall convergence; there is usually a pair MH site that is already handling the traffic.

The no form sets the values back to the defaults.

Default  4
Parameters  time — Specifies the group up time value.

Values  0 — 3600

group down

Syntax  group down time | no group down
Context  config>service>oper-group>hold-time
Description  This command configures the number of seconds to wait before notifying clients monitoring this group when its operational status transitions from up to down.

The no form sets the values back to the default.
Pseudowire Commands

**pw-routing**

**Syntax**    
```
pw-routing
```

**Context**  
```
config>service
```

**Description**  
This command enables the context to configure dynamic multi-segment pseudowire (MS-PW) routing. Pseudowire routing must be configured on each node that will be a T-PE or an S-PE.

**Default**  
disabled

**block-on-peer-fault**

**Syntax**    
```
[no] block-on-peer-fault
```

**Context**  
```
config>service>pw-template
```

**Description**  
When enabled, this command blocks the transmit direction of a pseudowire when any of the following pseudowire status codes is received from the far end PE:

- 0x00000001 Pseudowire Not Forwarding
- 0x00000002 Local Attachment Circuit (ingress) Receive Fault
- 0x00000004 Local Attachment Circuit (egress) Transmit Fault
- 0x00000008 Local PSN-facing PW (ingress) Receive Fault
- 0x00000010 Local PSN-facing PW (egress) Transmit Fault

The transmit direction is unblocked when the following PW status code is received:

- 0x00000000 Pseudowire forwarding (clear all failures)

This command is mutually exclusive with `no pw-status-signaling`, and `standby-signaling-slave`. It is not applicable to spoke SDPs forming part of an MC-LAG or spoke SDPs in an endpoint.

**Default**  
no block-on-peer-fault

**boot-timer**

**Syntax**    
```
boot-timer secs
no boot-timer
```

**Context**  
```
config>service>pw-routing
```

**Description**  
This command configures a hold-off timer for MS-PW routing advertisements and signaling and is used at boot time.

The `no` form of this command removes a previously configured timer and restores it to its default.
timer-value — The value of the boot timer in seconds.

Values 0 — 600

local-prefix

Syntax local-prefix local-prefix [create]
no local-prefix/local-prefix

Context config>service>pw-routing

Description This command configures one or more node prefix values to be used for MS-PW routing. At least one prefix must be configured on each node that is an S-PE or a T-PE.

The no form of this command removes a previously configured prefix, and will cause the corresponding route to be withdrawn if it has been advertised in BGP.

Parameters local-prefix — Specifies a 32 bit prefix for the AII. One or more prefix values, up to a maximum of 16 may be assigned to the 7x50 node. The global ID can contain the 2-octet or 4-octet value of the provider's Autonomous System Number (ASN). The presence of a global ID based on the provider's ASN ensures that the AII for spoke-SDPs configured on the node will be globally unique.

Values <global-id>:<ip-addr>|<raw-prefix>
ip-addr a.b.c.d raw-prefix1 — 4294967295 global-id1 — 4294967295

advertise-bgp

Syntax advertise-bgp route-distinguisher rd [community community]
no advertise-bgp route-distinguisher rd

Context config>service>pw-routing

Description This command enables a given prefix to be advertised in MP-BGP for dynamic MS-PW routing.

The no form of this command will explicitly withdraw a route if it has been previously advertised.

Default no advertise-bgp.

Parameters rd — Specifies an 8-octet route distinguisher associated with the prefix. Up to 4 unique route distinguishers can be configured and advertised for a given prefix though multiple instances of the advertise-bgp command. This parameter is mandatory.

Values (6 bytes, other 2 Bytes of type will be automatically generated)
asn:number1 (RD Type 0): 2bytes ASN and 4 bytes locally administered number
ip-address:number2 (RD Type 1): 4bytes IPv4 and 2 bytes locally administered number;
**community community** — An optional BGP communities attribute associated with the advertisement. To delete a previously advertised community, `advertise-bgp route-distinguisher` must be run again with the same value for the RD but excluding the community attribute.

**Values**  
```
community {2-byte-as-number:comm-val}
2-byte-asnumber 0—65535
comm.-val 0 — 65535
```

**path**

**Syntax**  
```
path name [create]
no path name
```

**Context**  
```
config>service>pw-routing
```

**Description**  
This command configures an explicit path between this T-PE and a remote T-PE. For each path, one or more intermediate S-PE hops must be configured. A path can be used by multiple multi-segment pseudowires. Paths are used by a T-PE to populate the list of Explicit Route TLVs included in the signaling of a dynamic MS-PW.

A path may specify all or only some of the hops along the route to reach a T-PE. The **no** form of the command removes a specified explicit path from the configuration.

**Default**  
```
no path
```

**Parameters**  
```
path-name — Specifies a locally-unique case-sensitive alphanumeric name label for the MS-PW path of up to 32 characters in length.
```

**hop**

**Syntax**  
```
hop hop-index ip-address
no hop hop-index
```

**Context**  
```
config>service>pw-routing>hop
```

**Description**  
This command configures each hop on an explicit path that can be used by one or more dynamic MS-PWs. It specifies the IP addresses of the hops that the MS-PE should traverse. These IP addresses can correspond to the system IP address of each S-PE, or the IP address on which the T-LDP session to a given S-PE terminates.

The **no** form of this command deletes hop list entries for the path. All the MS-PWs currently using this path are unaffected. Additionally, all services actively using these MS-PWs are unaffected. The path must be shutdown first in order to delete the hop from the hop list. The ‘no hop hop-index’ command will not result in any action, except for a warning message on the console indicating that the path is administratively up.

**Default**  
```
no hop
```

**Parameters**  
```
hop-index — Specifies a locally significant numeric identifier for the hop. The hop index is used to order the hops specified. The LSP always traverses from the lowest hop index to the highest. The hop index does not need to be sequential.
```

**Values**  
```
1 — 1024
```
ip-address — Specifies the system IP address or terminating IP address for the T-LDP session to the S-PE corresponding to this hop. For a given IP address on a hop, the system will choose the appropriate SDP to use.

retry-count

Syntax  

retry-count [10..10000]
no retry-count

Context  config>service>pw-routing

Description  This optional command specifies the number of attempts software should make to re-establish the spoke-SDP after it has failed. After each successful attempt, the counter is reset to zero. When the specified number is reached, no more attempts are made and the spoke-sdp is put into the shutdown state.

Use the no shutdown command to bring up the path after the retry limit is exceeded.

The no form of this command reverts the parameter to the default value.

Default 30

Parameters  

retry-count — Specifies the maximum number of retries before putting the spoke-sdp into the shutdown state.

Values 10 — 10000

retry-timer

Syntax  

retry-timer secs
no retry-timer

Context  config>service>pw-routing

Description  This command specifies a retry-timer for the spoke-SDP. This is a configurable exponential back-off timer that determines the interval between retries to re-establish a spoke-SDP if it fails and a label withdraw message is received with the status code “AII unreachable”.

The no form of this command reverts the timer to its default value.

Default 30

Parameters  

retry-count — The initial retry-timer value in seconds.

Values 10 – 480
Pseudowire Commands

**spe-address**

**Syntax**  
`spe-address global-id:prefix`  
`no spe-address`

**Context**  
`config>service>pw-routing`

**Description**  
This command configures a single S-PE Address for the node to be used for dynamic MS-PWs. This value is used for the pseudowire switching point TLV used in LDP signaling, and is the value used by pseudowire status signaling to indicate the PE that originates a pseudowire status message. Configuration of this parameter is mandatory to enable dynamic MS-PW support on a node.

If the S-PE Address is not configured, spoke-sdps that use dynamic MS-PWs and pw-routing local-prefixes cannot be configured on a T-PE. Furthermore, and 7x50 node will send a label release for any label mappings received for FEC129 All type 2.

The S-PE Address cannot be changed unless the dynamic ms-pw configuration is removed. Furthermore, changing the S-PE Address will also result in all dynamic MS-PWs for which this node is an S-PE being released. It is recommended that the S-PE Address should be configured for the life of an MS-PW configuration after reboot of the 7x50.

The **no** form of this command removes the configured S-PE Address.

**Default**  
no spe-address

**Parameters**
- `global-id` — Specifies a 4-octet value that is unique to the service provider. For example, the global ID can contain the 2-octet or 4-octet value of the provider's Autonomous System Number (ASN).
- `prefix` — Specifies the prefix length.
- `ipaddress` — Specifies the IP address.

**Syntax**  
`<global-id:prefix>:<global-id>:<prefix>|<ipaddress>`

- `global-id` — 1 — 4294967295
- `prefix` — 1 — 4294967295
- `ipaddress` — a.b.c.d

**static-route**

**Syntax**  
`[no] static-route route-name`

**Context**  
`config>service>pw-routing`

**Description**  
This command configures a static route to a next hop S-PE or T-PE. Static routes may be configured on either S-PEs or T-PEs.

A default static route is entered as follows:

- `static-route 0:0:next_hop_ip_address
  or
  static-route 0:0.0.0.0:next_hop_ip_address`

The **no** form of this command removes a previously configured static route.

**Default**  
no static-route

**Parameters**
- `route-name` — Specifies the static pseudowire route.
<table>
<thead>
<tr>
<th>Values</th>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>route-name</td>
<td>&lt;global-id&gt;::&lt;prefix&gt;::&lt;next-hop-ip_addr&gt;</td>
</tr>
<tr>
<td>global-id</td>
<td>0 — 4294967295</td>
</tr>
<tr>
<td>prefix</td>
<td>a.b.c.d</td>
</tr>
<tr>
<td>ip_addr</td>
<td>a.b.c.d</td>
</tr>
</tbody>
</table>

**pw-template**

**Syntax**

```bash
[no] pw-template sdp-template-id [use-provisioned-sdp] [create]
```

**Context**

config>service

**Description**

This command configures an SDP template.

**Parameters**

- `sdp-template-id` — Specifies a number used to uniquely identify a template for the creation of a Service Distribution Point (SDP). The value 0 is used as the null ID.
- `Values` 0, 1 — 2147483647

- `use-provisioned-sdp` — Specifies whether to use an already provisioned SDP. When specified, the tunnel manager will be consulted for an existing active SDP. Otherwise, the default SDP template will be used to use for instantiation of the SDP.

- `create` — This keyword is required when first creating the configuration context. Once the context is created, it is possible to navigate into the context without the `create` keyword.
SDP Commands

sdp

Syntax

sdp sdp-id [gre | mpls | l2tpv3] [create]
no sdp sdp-id

Context

config>service

Description

This command creates or edits a Service Distribution Point (SDP). SDPs must be explicitly configured.

An SDP is a logical mechanism that ties a far-end router to a particular service without having to specifically define far end SAPs. Each SDP represents a method to reach another router.

One method is IP Generic Router Encapsulation (GRE) which has no state in the core of the network. GRE does not specify a specific path to the far-end router. A GRE-based SDP uses the underlying IGP routing table to find the best next hop to the far-end router.

The second method is Multi-Protocol Label Switching (MPLS) encapsulation. A router supports both signaled and non-signaled Label Switched Paths (LSPs) through the network. Non-signaled paths are defined at each hop through the network. Signaled paths are communicated by protocol from end to end using Resource ReserVation Protocol (RSVP). Paths may be manually defined or a constraint-based routing protocol (such as OSPF-TE or CSPF) can be used to determine the best path with specific constraints. An LDP LSP can also be used for an SDP when the encapsulation is MPLS. The use of an LDP LSP type or an RSVP/Static LSP type are mutually exclusive except when the mixed-lsp option is enabled on the SDP.

L2TPv3-over-IPv6 transport is also an option for Ethernet Pipe (EPIPE) services. Like GRE, L2TPv3 is stateless in the core of the network, as well as on the service nodes as the L2TPv3 control plane functionality is disabled for this SDP type. A unique source and destination IPv6 address combined with TX and RX Cookie values are used to ensure that the SDP is bound to the correct service.

SDPs are created and then bound to services. Many services may be bound to a single SDP. The operational and administrative state of the SDP controls the state of the SDP binding to the service.

If sdp-id does not exist, a new SDP is created. When creating an SDP, either the gre, mpls, or l2tpv3 keyword must be specified. SDPs are created in the admin down state (shutdown) and the no shutdown command must be executed once all relevant parameters are defined and before the SDP can be used.

If sdp-id exists, the current CLI context is changed to that SDP for editing and modification. For editing an existing SDP, neither the gre, mpls, or l2tpv3 keyword is specified. If a keyword is specified for an existing sdp-id, an error is generated and the context of the CLI will not be changed to the specified sdp-id.

The no form of this command deletes the specified SDP. Before an SDP can be deleted, it must be administratively down (shutdown) and not bound to any services. If the specified SDP is bound to a service, the no sdp command will fail generating an error message specifying the first bound service found during the deletion process. If the specified sdp-id does not exist an error will be generated.

Default

none

Parameters

sdp-id — The SDP identifier.

Values

1 — 17407
gre — Specifies the SDP will use GRE to reach the far-end router. Only one GRE SDP can be created to a given destination device. Multiple GRE SDPs to a single destination serve no purpose as the path taken to reach the far end is determined by the IGP which will be the same for all SDPs to a given destination and there is no bandwidth reservation in GRE tunnels.

mpls — Specifies the SDP will use MPLS encapsulation and one or more LSP tunnels to reach the far-end device. Multiple MPLS SDPs may be created to a given destination device. Multiple MPLS SDPs to a single destination device are helpful when they use divergent paths.

l2tpv3 — Specifies the SDP will use L2TPv3-over-IPv6 encapsulation. One SDP is created per service, regardless of whether the far-end node is common or not. Unique local and far-end addresses are configured for every L2TPv3 SDP type. The local address must exist on the local node.

auto-learn-mac-protect

Syntax  
[no] auto-learn-mac-protect

Context  config>service>pw-template
         config>service>pw-template>split-horizon-group

Description  This command specifies whether to enable auto Auto-Learn MAC Protect on page 555 tatic population of the MAC protect list with source MAC addresses learned on the associated with this SHG. For more information about auto-learn MAC protect, refer to Auto-Learn MAC Protect on page 555.

The no form of the command disables the automatic population of the MAC protect list.

Default  auto-learn-mac-protect

accounting-policy

Syntax  accounting-policy acct-policy-id
       no accounting-policy

Context  config>service>pw-template
         config>service>sdp

Description  This command creates the accounting policy context that can be applied to an SDP. An accounting policy must be defined before it can be associated with a SDP. If the policy-id does not exist, an error message is generated.

A maximum of one accounting policy can be associated with a SDP at one time. Accounting policies are configured in the config>log context.

The no form of this command removes the accounting policy association from the SDP, and the accounting policy reverts to the default.

Default  Default accounting policy.

Parameters  acct-policy-id — Enter the accounting policy-id as configured in the config>log>accounting-policy context.

Values  1 — 99
**bgp-tunnel**

**Syntax**
```plaintext
[no] bgp-tunnel
```

**Context**
```
config>service>sdp
```

**Description**
This command allows the use of BGP route tunnels available in the tunnel table to reach SDP far-end nodes. Use of BGP route tunnels are only available with MPLS-SDP. Only one of the transport methods is allowed per SDP - LDP, RSVP-LSP or BGP-Tunnel (BGP-Tunnel is not supported on multi-mode LSP).

The **no** form of the command disables resolving BGP route tunnel LSP for SDP far-end.

**Default**
no bgp-tunnel (BGP tunnel route to SDP far-end is disabled)

**booking-factor**

**Syntax**
```plaintext
booking-factor percentage
no booking-factor
```

**Context**
```
config>service>sdp
```

**Description**
This command specifies the booking factor applied against the maximum SDP available bandwidth by the VLL CAC feature.

The service manager keeps track of the available bandwidth for each SDP. The maximum value is the sum of the bandwidths of all constituent LSPs in the SDP. The SDP available bandwidth is adjusted by the user configured booking factor. A value of 0 means no VLL can be admitted into the SDP.

The **no** form of the command reverts to the default value.

**Parameters**
`percentage` — Specifies the percentage of the SDP maximum available bandwidth for VLL call admission. When the value of this parameter is set to zero (0), no new VLL spoke SDP bindings with non-zero bandwidth are permitted with this SDP. Overbooking, >100% is allowed.

**Values**
- 0 — 1000 %

**Default**
100%

**collect-stats**

**Syntax**
```plaintext
[no] collect-stats
```

**Context**
```
config>service>pw-template
config>service>sdp
```

**Description**
This command enables accounting and statistical data collection for either the SDP. When applying accounting policies the data, by default, is collected in the appropriate records and written to the designated billing file.

When the **no collect-stats** command is issued the statistics are still accumulated by the XCM cards. However, the CPU will not obtain the results and write them to the billing file. If a subsequent **collect-stats** command is issued then the counters written to the billing file include all the traffic while the **no collect-stats** command was in effect.
**control-word**

**Syntax**  
[no] control-word

**Description**  
This command enables the use of the control word on pseudowire packets in VPLS and enables the use of the control word individually on each mesh-sdp or spoke-sdp. By default, the control word is disabled. When the control word is enabled, all VPLS packets, including the BPDU frames, are encapsulated with the control word when sent over the pseudowire. The T-LDP control plane behavior is the same as in the implementation of control word for VLL services. The configuration for the two directions of the Ethernet pseudowire should match. The no form of the command reverts the mesh SDP or spoke-sdp to the default behavior of not using the control word.

**Default**  
no control-word

**disable-aging**

**Syntax**  
[no] disable-aging

**Context**  
config>service>pw-template

**Description**  
This command disables MAC address aging across a service. The no form of this command enables aging.

**Default**  
no disable-aging

**disable-learning**

**Syntax**  
[no] disable-learning

**Context**  
config>service>pw-template

**Description**  
This command enables learning of new MAC addresses. This parameter is mainly used in conjunction with the discard-unknown command. The no form of this command enables learning of MAC addresses.

**Default**  
no disable-learning (Normal MAC learning is enabled)

**discard-unknown-source**

**Syntax**  
[no] discard-unknown-source
SDP Commands

**Context**
config>service>pw-template

**Description**
When this command is enabled, packets received with an unknown source MAC address will be dropped only if the maximum number of MAC addresses have been reached.

When disabled, the packets are forwarded based on the destination MAC addresses.

The no form of this command causes packets with an unknown source MAC addresses to be forwarded by destination MAC addresses.

**Default**
no discard-unknown

**egress**

**Syntax**
egress

**Context**
config>service>pw-template

**Description**
This command enables the context to configure spoke SDP binding egress filter parameters.

**ingress**

**Syntax**
ingress

**Context**
config>service>pw-template

**Description**
This command enables the context to configure spoke SDP binding ingress filter parameters.

**filter**

**Syntax**
filter ip ip-filter-id
filter ipv6 ipv6-filter-id
filter mac mac-filter-id
no filter [ip ip-filter-id] [mac mac-filter-id] [ipv6 ipv6-filter-id]

**Context**
config>service>pw-template>egress
config>service>pw-template>ingress

**Description**
This command associates an IP filter policy or MAC filter policy on egress or ingress. Filter policies control the forwarding and dropping of packets based on IP or MAC matching criteria. There are two types of filter policies: IP and MAC. Only one type may be applied to a SAP at a time.

The filter command is used to associate a filter policy with a specified filter ID with an ingress or egress SAP. The filter ID must already be defined before the filter command is executed. If the filter policy does not exist, the operation will fail and an error message returned.

The no form of this command removes any configured filter ID association with the SAP or IP interface. The filter ID itself is not removed from the system unless the scope of the created filter is set to local. To avoid deletion of the filter ID and only break the association with the service object, use scope command within the filter definition to change the scope to local or global. The default scope of a filter is local.
Parameters

**ip ip-filter-id** — Specifies IP filter policy. The filter ID must already exist within the created IP filters.

**Values**

1 — 65535

**ipv6 ipv6-filter-id** — Specifies the IPv6 filter policy. The filter ID must already exist within the created IPv6 filters.

**Values**

1 — 65535

**mac mac-filter-id** — Specifies the MAC filter policy. The specified filter ID must already exist within the created MAC filters. The filter policy must already exist within the created MAC filters.

**Values**

1 — 65535

QoS

**Syntax**

```
qos network-policy-id port-redirect-group queue-group-name [instance instance-id]
no qos [network-policy-id]
```

**Context**

```
configure>service>apipe>spoke-sdp>egress
cfgure>service>cpipe>spoke-sdp>egress
cfgure>service>epipe>spoke-sdp>egress
cfgure>service>fpipe>spoke-sdp>egress
cfgure>service>ipipe>spoke-sdp>egress
cfgure>service>vpl>spoke-sdp>egress
cfgue>service>vpls>mesh-sdp>egress
cfgure>service>pw-template>egress
cfgue>service>vprn>interface>spoke-sdp>egress
cfgue>service>ies>interface>spoke-sdp>egress
```

**Description**

This command is used to redirect pseudowire packets to an egress port queue-group for the purpose of shaping.

The egress pseudowire shaping provisioning model allows the mapping of one or more pseudowires to the same instance of queues, or policers and queues, which are defined in the queue-group template.

Operationally, the provisioning model consists of the following steps:

1. Create an egress queue-group template and configure queues only or policers and queues for each FC that needs to be redirected.
2. Apply the queue-group template to the network egress context of all ports where there exists a network IP interface on which the pseudowire packets can be forwarded. This creates one instance of the template on the egress of the port. One or more instances of the same template can be created.
3. Configure FC-to-policer or FC-to-queue mappings together with the redirect to a queue-group in the egress context of a network QoS policy. No queue-group name is specified in this step, which means the same network QoS policy can redirect different pseudowires to different queue-group templates.
4. Apply this network QoS policy to the egress context of a spoke-SPD inside a service or to the egress context of a pseudowire template and specify the redirect queue-group name.

One or more spoke-SPDs can have their FCs redirected to use queues only or queues and policers in the same queue-group instance.

The following are the constraints and rules of this provisioning model:
1. When a pseudowire FC is redirected to use a queue or a policer and a queue in a queue-group and the queue-group name does not exist, the association is failed at the time the user associates the egress context of a spoke-SPD to the named queue-group. In such a case, the pseudowire packet will be fed directly to the corresponding egress queue for that FC used by the IP network interface on which the pseudowire packet is forwarded. This queue can be a queue-group queue, or the egress shared queue for that FC defined in the network-queue policy applied to the egress of this port. This is the existing implementation and default behavior for a pseudowire packet.

2. When a pseudowire FC is redirected to use a queue or a policer, and a queue in a queue-group and the queue-group name exists, but the policer-id and/or the queue-id is not defined in the queue-group template, the association is failed at the time the user associates the egress context of a spoke-SPD to the named queue-group. In such a case, the pseudowire packet will be fed directly to the corresponding egress queue for that FC used by the IP network interface the pseudowire packet is forwarded on.

3. When a pseudowire FC is redirected to use a queue, or a policer and a queue in a queue-group, and the queue-group name exists and the policer-id or policer-id plus queue-id exist, it is not required to check that an instance of that queue-group exists in all egress network ports which have network IP interfaces. The handling of this is dealt with in the data path as follows:
   a. When a pseudowire packet for that FC is forwarded and an instance of the referenced queue-group name exists on that egress port, the packet is processed by the queue-group policer and will then be fed to the queue-group queue.
   b. When a pseudowire packet for that FC is forwarded and an instance of the referenced queue-group name does not exist on that egress port, the pseudowire packet will be fed directly to the corresponding egress shared queue for that FC defined in the network-queue policy applied to the egress of this port.

4. If a network QoS policy is applied to the egress context of a pseudowire, any pseudowire FC, which is not explicitly redirected in the network QoS policy, will have the corresponding packets feed directly the corresponding the egress shared queue for that FC defined in the network-queue policy applied to the egress of this port.

When the queue-group name the pseudowire is redirected to exists and the redirection succeeds, the marking of the packet DEI/dot1.p/DSCP and the tunnel DEI/dot1.p/DSCP/EXP is performed; according to the relevant mappings of the (FC, profile) in the egress context of the network QoS policy applied to the pseudowire. This is true regardless, wether an instance of the queue-group exists or not on the egress port to which the pseudowire packet is forwarded. If the packet profile value changed due to egress child policer CIR profiling, the new profile value is used to mark the packet DEI/dot1.p and the tunnel DEI/dot1.p/EXP, but the DSCP is not modified by the policer operation.

When the queue-group name the pseudowire is redirected does not exist, the redirection command is failed. In this case, the marking of the packet DEI/dot1.p/DSCP and the tunnel DEI/dot1.p/DSCP/EXP fields is performed according to the relevant commands in the egress context of the network QoS policy applied to the network IP interface to which the pseudowire packet is forwarded.

The no version of this command removes the redirection of the pseudowire to the queue-group.

**Parameters**

- **network-policy-id** — Specifies the network policy identification. The value uniquely identifies the policy on the system.

  - **Values**
    - 1 — 65535

- **queue-redirect-group queue-group-name** — This optional parameter specifies that the queue-group-name will be used for all egress forwarding class redirections within the network QoS policy ID. The
specified queue-group-name must exist as a port egress queue group on the port associated with the IP interface.

egress-instance instance-id — Specifies the identification of a specific instance of the queue-group.

Values 1 — 16384

hash-label

Syntax hash-label [signal-capability]
no hash-label

Context config>service>pw-template

Description This command enables the use of the hash label on a VLL, VPRN or VPLS service bound to LDP or RSVP SDP as well as to a VPRN service using the autobind mode with the ldp, rsvp-te, or mpls options. This feature is not supported on a service bound to a GRE SDP or for a VPRN service using the autobind mode with the gre option. This feature is also not supported on multicast packets forwarded using RSVP P2MP LPS or mLDP LSP in both the base router instance and in the multicast VPN (mVPN) instance. It is, however, supported when forwarding multicast packets using an IES/VPRN spoke-interface.

When this feature is enabled, the ingress data path is modified such that the result of the hash on the packet header is communicated to the egress data path for use as the value of the label field of the hash label. The egress data path appends the hash label at the bottom of the stack (BoS) and sets the S-bit to one (1).

In order to allow applications where the egress LER infers the presence of the hash label implicitly from the value of the label, the Most Significant Bit (MSB) of the result of the hash is set before copying into the Hash Label. This means that the value of the hash label will always be in the range [524,288 - 1,048,575] and will not overlap with the signaled/static LSP and signaled/static service label ranges. This also guarantees that the hash label will not match a value in the reserved label range.

The (unmodified) result of the hash continues to be used for the purpose of ECMP and LAG spraying of packets locally on the ingress LER. Note, however, that for VLL services, the result of the hash is overwritten and the ECMP and LAG spraying will be based on service-id when ingress SAP shared queuing is not enabled. However, the hash label will still reflect the result of the hash such that an LSR can use it to perform fine grained load balancing of VLL pseudowire packets.

Packets generated in CPM and that are forwarded labeled within the context of a service (for example, OAM packets) must also include a Hash Label at the BoS and set the S-bit accordingly.

The TTL of the hash label is set to a value of 0.

The user enables the signaling of the hash-label capability under a VLL spoke-sdp, a VPLS spoke-sdp or mesh-sdp, or an IES/VPRN spoke interface by adding the signal-capability option. In this case, the decision whether to insert the hash label on the user and control plane packets by the local PE is solely determined by the outcome of the signaling process and can override the local PE configuration. The following are the procedures:

- The local PE will insert the flow label interface parameters sub-TLV with F=1 in the PW ID FEC element in the label mapping message for that spoke-sdp or mesh-sdp.
- If the remote PE includes this sub-TLV with F=1 or F=0, then local PE must insert the hash label in the user and control plane packets.
- If remote PE does not include this sub-TLV (for example, it does not support it, or it is supported but the user did not enable the hash-label option or the signal-capability option), then the local PE establishes
the pseudowire but must not insert the hash label in the user and control packets over that spoke-sdp or mesh-sdp. If the remote PE does not support the **signal-capability** option, then there are a couple of possible outcomes:

- If the **hash-label** option was enabled on the local configuration of the spoke-sdp or mesh-sdp at the remote PE, the pseudowire packets received by the local PE will have the hash label included. These packets must be dropped. The only way to solve this is to disable the signaling capability option on the local node which will result in the insertion of the hash label by both PE nodes.

- If the **hash-label** option is not supported or was not enabled on the local configuration of the spoke-sdp or mesh-sdp at the remote PE, the pseudowire received by the local PE will not have the hash label included.

  • The user can enable or disable the signal-capability option in CLI as needed. When doing so, the router must withdraw the label it sent to its peer and send a new label mapping message with the new value of the F bit in the flow label interface parameters sub-TLV of the PW ID FEC element.

The **no** form of this command disables the use of the hash label.

**Default**

```
no hash-label
```

**Parameters**

**signal-capability** — Enables the signaling and negotiation of the use of the hash label between the local and remote PE nodes. The **signal-capability** option is not supported on a VPRN spoke-sdp.

### force-vlan-vc-forwarding

**Syntax**

```
[no] force-vlan-vc-forwarding
```

**Context**

```
config>service>pw-template
```

**Description**

This command forces vc-vlan-type forwarding in the data path for spoke and mesh SDPs that have either vc-type. This comand is not allowed on vlan-vc-type SDPs.

The **no** version of this command sets default behavior.

**Default**

```
per default this feature is disabled
```

### QOS

**Syntax**

```
sos network-policy-id fp-redirect-group queue-group-name instance instance-id
```

**Context**

```
config>service>apipe>spoke-sdp>ingress
config>service>cpipe>spoke-sdp>ingress
config>service>epipe>spoke-sdp>ingress
config>service>fpipe>spoke-sdp>ingress
config>service>ipipe>spoke-sdp>ingress
config>service>vpl>spoke-sdp>ingress
config>service>vpls>spoke-sdp>ingress
config>service>vpl>mesh-sdp>ingress
config>service>pw-template>ingress
config>service>vprn>interface>spoke-sdp>ingress
```
Description

This command is used to redirect pseudowire packets to an ingress forwarding plane queue-group for the purpose of rate-limiting.

The ingress pseudowire rate-limiting feature uses a policer in queue-group provisioning model. This model allows the mapping of one or more pseudowires to the same instance of policers which are defined in a queue-group template.

Operationally, the provisioning model in the case of the ingress pseudowire shaping feature consists of the following steps:

1. Create an ingress queue-group template and configure policers for each FC which needs to be redirected and optionally for each traffic type (unicast or multicast).
2. Apply the queue-group template to the network ingress forwarding plane where there exists a network IP interface which the pseudowire packets can be received on. This creates one instance of the template on the ingress of the FP. One or more instances of the same template can be created.
3. Configure FC-to-policer mappings together with the policer redirect to a queue-group in the ingress context of a network QoS policy. No queue-group name is specified in this step which means the same network QoS policy can redirect different pseudowires to different queue-group templates.
4. Apply this network QoS policy to the ingress context of a spoke-sdp inside a service or to the ingress context of a pseudowire template and specify the redirect queue-group name.

One or more spoke-sdps can have their FCs redirected to use policers in the same policer queue-group instance.

The following are the constraints and rules of this provisioning model when used in the ingress pseudowire rate-limiting feature:

1. When a pseudowire FC is redirected to use a policer in a named policer queue-group and the queue-group name does not exist, the association is failed at the time the user associates the ingress context of a spoke-sdp to the named queue-group. In such a case, the pseudowire packet will feed directly the ingress network shared queue for that FC defined in the network-queue policy applied to the ingress of the XMA/FP.
2. When a pseudowire FC is redirected to use a policer in a named policer queue-group and the queue-group name exists but the policer-id is not defined in the queue-group template, the association is failed at the time the user associates the ingress context of a spoke-sdp to the named queue-group. In such a case, the pseudowire packet will feed directly the ingress network shared queue for that FC defined in the network-queue policy applied to the ingress of the XMA/MDA/FP.
3. When a pseudowire FC is redirected to use a policer in a named policer queue-group and the queue-group name exists and the policer-id is defined in the queue-group template, it is not required to check that an instance of that queue-group exists in all ingress FPs which have network IP interfaces. The handling of this is dealt with in the data path as follows:
   - When a pseudowire packet for that FC is received and an instance of the referenced queue-group name exists on that FP, the packet is processed by the policer and will then feed the per FP ingress shared queues referred to as “policer-output-queues”.
   - When a pseudowire packet for that FC is received and an instance of the referenced queue-group name does not exist on that FP, the pseudowire packets will be fed directly into the corresponding ingress network shared queue for that FC defined in the network-queue policy applied to the ingress of the XMA/MDA/FP.
4. If a network QoS policy is applied to the ingress context of a pseudowire, any pseudowire FC which is not explicitly redirected in the network QoS policy will have the corresponding packets feed directly the ingress network shared queue for that FC defined in the network-queue policy applied to the ingress of the XMA/MDA/FP.

5. If no network QoS policy is applied to the ingress context of the pseudowire, then all packets of the pseudowire will feed:
   - the ingress network shared queue for the packet’s FC defined in the network-queue policy applied to the ingress of the XMA/MDA/FP. This is the default behavior.
   - a queue-group policer followed by the per-FP ingress shared queues referred to as “policer-output-queues” if the ingress context of the network IP interface from which the packet is received is redirected to a queue-group [csc-policing]. The only exceptions to this behavior are for packets received from a IES/VPRN spoke interface and from a R-VPLS spoke-sdp which is forwarded to the R-VPLS IP interface. In these two cases, the ingress network shared queue for the packet’s FC defined in the network-queue policy applied to the ingress of the XMA/MDA/FP is used.

When a pseudowire is redirected to use a policer queue-group, the classification of the packet for the purpose of FC and profile determination is performed according to default classification rule or the QoS filters defined in the ingress context of the network QoS policy applied to the pseudowire. This is true regardless if an instance of the named policer queue-group exists on the ingress FP the pseudowire packet is received on. The user can apply a QoS filter matching the dot1p in the VLAN tag corresponding to the Ethernet port encapsulation, the EXP in the outer label when the tunnel is an LSP, the DSCP in the IP header if the tunnel encapsulation is GRE, and the DSCP in the payload’s IP header if the user enabled the ler-use-dscp option and the pseudowire terminates in IES or VPRN service (spoke-interface).

When the policer queue-group name the pseudowire is redirected does not exist, the redirection command is failed. In this case, the packet classification is performed according to default classification rule or the QoS filters defined in the ingress context of the network QoS policy applied to the network IP interface the pseudowire packet is received on.

The no version of this command removes the redirection of the pseudowire to the queue-group.

**Parameters**

**network-policy-id** — Specifies the network policy identification. The value uniquely identifies the policy on the system.

**Values**

1 — 65535

**fp-redirect-group** **queue-group-name** — Specifies the network policy identification. The value uniquely identifies the policy on the system.

**Values**

1 — 16384

**vc-label**

**Syntax**

```
[no] vc-label vc-label
```

**Context**

config>service>pw-template>ingress

**Description**

This command configures the ingress VC label.

**Parameters**

**vc-label** — A VC ingress value that indicates a specific connection.

**Values**

2048 — 18431
limit-mac-move

**Syntax**

```plaintext
limit-mac-move [blockable | non-blockable]
no limit-mac-move
```

**Context**

config>service>pw-template

**Description**

This command indicates whether or not the mac-move agent will limit the MAC re-learn (move) rate.

**Default**

blockable

**Parameters**

- **blockable** — The agent will monitor the MAC re-learn rate, and it will block it when the re-learn rate is exceeded.
- **non-blockable** — When specified, a SAP will not be blocked, and another blockable SAP will be blocked instead.

mac-pinning

**Syntax**

```plaintext
[no] mac-pinning
```

**Context**

config>service>pw-template

**Description**

Enabling this command will disable re-learning of MAC addresses on other SAPs within the service. The MAC address will remain attached to a given SAP for duration of its age-timer.

The age of the MAC address entry in the FIB is set by the age timer. If **mac-aging** is disabled on a given VPLS service, any MAC address learned on a SAP/SDP with **mac-pinning** enabled will remain in the FIB on this SAP/SDP forever. Every event that would otherwise result in re-learning will be logged (MAC address; original-SAP; new-SAP).

**Default**

When a SAP or spoke SDP is part of a Residential Split Horizon Group (RSHG), MAC pinning is activated at creation of the SAP. Otherwise MAC pinning is not enabled by default.

max-nbr-mac-addr

**Syntax**

```plaintext
max-nbr-mac-addr table-size
no max-nbr-mac-addr
```

**Context**

config>service>pw-template

**Description**

This command specifies the maximum number of FDB entries for both learned and static MAC addresses for this SAP or spoke SDP.

When the configured limit has been reached, and discard-unknown-source has been enabled for this SAP or spoke SDP (see **discard-unknown-source on page 193**), packets with unknown source MAC addresses will be discarded.

The **no** form of the command restores the global MAC learning limitations for the SAP or spoke SDP.

**Default**

no max-nbr-mac-addr

**Parameters**

- **table-size** — Specifies the maximum number of learned and static entries allowed in the FDB of this service.
Values

<table>
<thead>
<tr>
<th>Values</th>
<th>1 — 196607</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The chassis-mode C limit: 511999</td>
</tr>
</tbody>
</table>

restrict-protected-src

**Syntax**

```
restrict-protected-src alarm-only
restrict-protected-src [discard-frame]
no restrict-protected-src
```

**Context**

```
config>service>pw-template
config>service>pw-template>split-horizon-group
```

**Description**

This command indicates the action to take whenever a relearn request for a protected MAC is received on a restricted SAP belonging to this SHG.

When enabled, the agent will protect the MAC from being learned or re-learned on a SAP that has restricted learning enabled.

**Default**

`restrict-protected-src`

**Parameters**

- **alarm-only** — Specifies that the SAP will be left up and only a notification, `sapReceivedProtSrcMac`, will be generated.
- **discard-frame** — Specifies that the SAP will start discarding the frame in addition to generating `sapReceivedProtSrcMac` notification.

mfib-allowed-mda-destinations

**Syntax**

```
mfib-allowed-mda-destinations
```

**Context**

```
config>service>pw-template>egress
```

**Description**

This command enables the context to configure MFIB-allowed XMA/MDA destinations.

The `allowed-mda-destinations` node and the corresponding `mda` command are used on spoke and mesh SDP bindings to provide a list of XMA/MDA destinations in the chassis that are allowed as destinations for multicast streams represented by `[*,g]` and `[s,g]` multicast flooding records on the VPLS service. The XMA/MDA list only applies to IP multicast forwarding when IGMP snooping is enabled on the VPLS service. The XMA/MDA list has no effect on normal VPLS flooding such as broadcast, Layer 2 multicast, unknown destinations or non-snooped IP multicast.

At the IGMP snooping level, a spoke or mesh SDP binding is included in the flooding domain for an IP multicast stream when it has either been defined as a multicast router port, received a IGMP query through the binding or has been associated with the multicast stream through an IGMP request by a host over the binding. Due to the dynamic nature of the way that a spoke or mesh SDP binding is associated with one or more egress network IP interfaces, the system treats the binding as appearing on all network ports. This causes all possible network destinations in the switch fabric to be included in the multicast streams flooding domain. The XMA/MDA destination list provides a simple mechanism that narrows the IP multicast switch fabric destinations for the spoke or mesh SDP binding.

If no XMAs/MDAs are defined within the allowed-mda-destinations node, the system operates normally and will forward IP multicast flooded packets associated with the spoke or mesh SDP binding to all switch...
fabric taps containing network IP interfaces.

The XMA/MDA inclusion list should include all XMA/MDAs that the SDP binding may attempt to forward through. A simple way to ensure that an XMA/MDA that is not included in the list is not being used by the binding is to define the SDP the binding is associated with as MPLS and use an RSVP-TE LSP with a strict egress hop. The XMA/MDA associated with the IP interface defined as the strict egress hop should be present in the inclusion list.

If the inclusion list does not currently contain the XMA/MDA that the binding is forwarding through, the multicast packets will not reach the destination represented by the binding. By default, the XMA/MDA inclusion list is empty.

If an XMA/MDA is removed from the list, the XMA/MDA is automatically removed from the flooding domain of any snooped IP multicast streams associated with a destination on the XMA/MDA unless the XMA/MDA was the last XMA/MDA on the inclusion list. Once the inclusion list is empty, all XMA/MDAs are eligible for snooped IP multicast flooding for streams associated with the SDP binding.

### mda

**Syntax**

```
[no] mda mda-id
```

**Context**

```
config>service>pw-template>egress>mfib-mda
```

**Description**

This command specifies an MFIB-allowed XMA/MDA destination for an SDP binding configured in the system.

**Parameters**

- `mda-id` — Specifies an MFIB-allowed XMA/MDA destination.

### igmp-snooping

**Syntax**

```
igmp-snooping
```

**Context**

```
config>service>pw-template
```

**Description**

This command enables the Internet Group Management Protocol (IGMP) snooping context.

**Default**

none

### fast-leave

**Syntax**

```
[no] fast-leave
```

**Context**

```
config>service>pw-template>igmp-snooping
```

**Description**

This command enables fast leave.

When IGMP fast leave processing is enabled, the SR-Series will immediately remove a SAP or SDP from the IP multicast group when it detects an IGMP 'leave' on that SAP or SDP. Fast leave processing allows the switch to remove a SAP or SDP that sends a 'leave' from the forwarding table without first sending out group-specific queries to the SAP or SDP, and thus speeds up the process of changing channels ('zapping').
SDP Commands

Fast leave should only be enabled when there is a single receiver present on the SAP or SDP. When fast leave is enabled, the configured last-member-query-interval value is ignored.

Default no fast-leave

import

**Syntax** import *policy-name*  
no import  

**Context** config>service>pw-template>igmp-snooping  

**Description** This command specifies the import routing policy to be used for IGMP packets. Only a single policy can be imported at a time. The no form of the command removes the policy association.

**Default** no import — No import policy is specified.

**Parameters**  
*policy-name* — The import policy name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes. Routing policies are configured in the config>router>policy-options context. The router policy must be defined before it can be imported.

last-member-query-interval

**Syntax** last-member-query-interval *tenths-of-seconds*  
no last-member-query-interval  

**Context** config>service>pw-template>igmp-snooping  

**Description** This command configures the maximum response time used in group-specific queries sent in response to ‘leave’ messages, and is also the amount of time between 2 consecutive group-specific queries. This value may be tuned to modify the leave latency of the network. A reduced value results in reduced time to detect the loss of the last member of a group. The configured last-member-query-interval is ignored when fast-leave is enabled on the SAP or SDP.

**Default** 10  

**Parameters**  
tenths of seconds — Specifies the frequency, in tenths of seconds, at which query messages are sent.  

**Values** 1 — 50

max-num-groups

**Syntax** max-num-groups *count*  
no max-num-groups  

**Context** config>service>pw-template>igmp-snooping
Description: This command defines the maximum number of multicast groups that can be joined. If the SR-Series receives an IGMP join message that would exceed the configured number of groups, the request is ignored.

Default: no max-num-groups

Parameters: count — Specifies the maximum number of groups that can be joined.

Values: 1 — 1000

query-interval

Syntax: query-interval seconds

no query-interval

Context: config>service>pw-template>igmp-snooping

Description: This command configures the IGMP query interval. If the send-queries command is enabled, this parameter specifies the interval between two consecutive general queries sent by the system on this SAP or SDP.

The configured query-interval must be greater than the configured query-response-interval.

If send-queries is not enabled on this SAP or SDP, the configured query-interval value is ignored.

Default: 125

Parameters: seconds — The time interval, in seconds, that the router transmits general host-query messages.

Values: 2 — 1024

query-response-interval

Syntax: query-response-interval seconds

Context: config>service>pw-template>igmp-snooping

Description: This command configures the IGMP query response interval. If the send-queries command is enabled, this parameter specifies the maximum response time advertised in IGMPv2/v3 queries.

The configured query-response-interval must be smaller than the configured query-interval.

If send-queries is not enabled on this SAP or SDP, the configured query-response-interval value is ignored.

Default: 10

Parameters: seconds — Specifies the length of time to wait to receive a response to the host-query message from the host.

Values: 1 — 1023
robust-count

Syntax

\texttt{robust-count \RobustCount \textit{robust-count}}

\texttt{no \ RobustCount}

Context

\texttt{config>service>pw-template>igmp-snooping}

Description

If the \texttt{send-queries} command is enabled, this parameter allows tuning for the expected packet loss. The robust-count variable allows tuning for the expected packet loss on a subnet and is comparable to a retry count.

If send-queries is not enabled, this parameter will be ignored.

Default

\texttt{2}

Parameters

\texttt{robust-count} — Specifies the robust count for the SAP or SDP.

Values

\texttt{2} — \texttt{7}

send-queries

Syntax

\texttt{[no] send-queries}

Context

\texttt{config>service>pw-template>igmp-snooping}

Description

This command specifies whether to send IGMP general query messages.

When send-queries is configured, all type of queries generate ourselves are of the configured version. If a report of a version higher than the configured version is received, the report will get dropped and a new wrong version counter will get incremented.

If send-queries is not configured, the version command has no effect. The version used on that SAP/SDP will be the version of the querier. This implies that, for example, when we have a v2 querier, we will never send out a v3 group or group-source specific query when a host wants to leave a certain group.

Default

\texttt{no send-queries}

version

Syntax

\texttt{version \textit{version}}

\texttt{no \textit{version}}

Context

\texttt{config>service>pw-template>igmp-snooping}

Description

This command specifies the version of IGMP. This object can be used to configure a router capable of running either value. For IGMP to function correctly, all routers on a LAN must be configured to run the same version of IGMP on that LAN.

When the \texttt{send-query} command is configured, all type of queries generate ourselves are of the configured version. If a report of a version higher than the configured version is received, the report gets dropped and a new “wrong version” counter is incremented.

If the \texttt{send-query} command is not configured, the \texttt{version} command has no effect. The version used on that
SAP or SDP will be the version of the querier. This implies that, for example, when there is a v2 querier, a v3 group or group-source specific query when a host wants to leave a certain group will never be sent.

**Parameters**

`version` — Specify the IGMP version.

**Values**

1, 2, 3

---

**sdp-include**

**Syntax**

```bash
[no] sdp-include group-name
```

**Context**

config>service>pw-template

**Description**

This command configures SDP admin group constraints for a PW template.

The admin group name must have been configured or the command is failed. The user can execute the command multiple times to include or exclude more than one admin group. The sdp-include and sdp-exclude commands can only be used with the `use-provisioned-sdp` option. If the same group name is included and excluded within the same PW template, only the exclude option will be enforced.

Any changes made to the admin group sdp-include and sdp-exclude constraints will only be reflected in existing spoke-sdps after the following command has been executed:

```
tools>perform>service>eval-pw-template>allow-service-impact
```

When the service is bound to the PW template, the SDP selection rules will enforce the admin group constraints specified in the sdp-include and sdp-exclude commands.

In the SDP selection process, all provisioned SDPs with the correct far-end IP address, the correct tunnel-far-end IP address, and the correct service label signaling are considered. The SDP with the lowest admin metric is selected. If more then one SDP with the same lowest metric are found then the SDP with the highest sdp-id is selected. The type of SDP, GRE or MPLS (BGP/RSVP/LDP) is not a criterion in this selection.

The selection rule with SDP admin groups is modified such that the following admin-group constraints are applied upfront to prune SDPs that do not comply:

- if one or more `sdp-include` statement is part of the pw-template, then an SDP that is a member of one or more of the included groups will be considered. With the `sdp-include` statement, there is no preference for an SDP that belongs to all included groups versus one that belongs to one or fewer of the included groups. All SDPs satisfying the admin-group constraint will be considered and the selection above based on the lowest metric and highest sdp-id is applied.

- if one or more `sdp-exclude` statement is part of the pw-template, then an sd that is a member of any of the excluded groups will not be considered.

SDP admin group constraints can be configured on all 7x50 services that makes use of the PW template (i.e., BGP-AD VPLS service, BGP-VPLS service, and FEC129 VLL service). In the latter case, only support at a T-PE node is provided.

The `no` form of this command removes the SDP admin group constraints from the PW template.

**Default**

none

**Parameters**

`group-name` — Specifies the name of the SDP admin group. A maximum of 32 characters can be entered.
sdp-exclude

Syntax  
[no] sdp-exclude group-name

Context  
config>service>pw-template

Description  
This command configures SDP admin group constraints for a PW template.

The admin group name must have been configured or the command is failed. The user can execute the command multiple times to include or exclude more than one admin group. The sdp-include and sdp-exclude commands can only be used with the use-provisioned-sdp option. If the same group name is included and excluded within the same PW template, only the exclude option will be enforced.

Any changes made to the admin group sdp-include and sdp-exclude constraints will only be reflected in existing spoke-sdps after the following command has been executed:

tools>perform>service>eval-pw-template>allow-service-impact

When the service is bound to the PW template, the SDP selection rules will enforce the admin group constraints specified in the sdp-include and sdp-exclude commands.

In the SDP selection process, all provisioned SDPs with the correct far-end IP address, the correct tunnel-far-end IP address, and the correct service label signaling are considered. The SDP with the lowest admin metric is selected. If more then one SDP with the same lowest metric are found then the SDP with the highest sdp-id is selected. The type of SDP, GRE or MPLS (BGP/RSVP/LDP) is not a criterion in this selection.

The selection rule with SDP admin groups is modified such that the following admin-group constraints are applied upfront to prune SDPs that do not comply:

- if one or more sdp-include statement is part of the pw-template, then an SDP that is a member of one or more of the included groups will be considered. With the sdp-include statement, there is no preference for an SDP that belongs to all included groups versus one that belongs to one or fewer of the included groups. All SDPs satisfying the admin-group constraint will be considered and the selection above based on the lowest metric and highest sdp-id is applied.

- if one or more sdp-exclude statement is part of the pw-template, then an sd that is a member of any of the excluded groups will not be considered.

SDP admin group constraints can be configured on all 7x50 services that makes use of the PW template (i.e., BGP-AD VPLS service, BGP-VPLS service, and FEC129 VLL service). In the latter case, only support at a T-PE node is provided.

The no form of this command removes the SDP admin group constraints from the PW template.

Default  
none

Parameters  
group-name — Specifies the name of the SDP admin group. A maximum of 32 characters can be entered.

split-horizon-group

Syntax  
[no] split-horizon-group [group-name] [residential-group]

Context  
config>service>pw-template

Description  
This command creates a new split horizon group (SGH).
Comparing a “residential” SGH and a “regular” SHG is that a residential SHG:

- Has different defaults for the SAP/SDP that belong to this group (ARP reply agent enabled (SAP only), MAC pinning enabled). These can be disabled in the configuration.
- Does not allow enabling spanning tree (STP) on a SAP. It is allowed on an SDP.
- Does not allow for downstream broadcast (broadcast / unknown unicast) on a SAP. It is allowed on an SDP.
- On a SAP, downstream multicast is only allowed when IGMP is enabled (for which an MFIB state exists; only IP multicast); on a SDP, downstream mcast is allowed.

When the feature was initially introduced, residential SHGs were also using ingress shared queing by default to increase SAP scaling.

A residential SAP (SAP that belongs to a RSHG) is used to scale the number of SAPs in a single VPLS instance. The limit depends on the hardware used and is higher for residential SAPs (where there is no need for egress multicast replication on residential SAPs) than for regular SAPs. Therefore, residential SAPs are useful in residential aggregation environments (for example, triple play networks) with a VLAN/subscriber model.

The no form of the command removes the group name from the configuration.

**Parameters**

- **group-name** — Specifies the name of the split horizon group to which the SDP belongs.
- **residential-group** — Defines a split horizon group as a residential split horizon group (RSHG). Doing so entails that:

  - SAPs which are members of this Residential Split Horizon Group will have:
    - Double-pass queuing at ingress as default setting (can be disabled)
    - STP disabled (cannot be enabled)
    - ARP reply agent enabled per default (can be disabled)
    - MAC pinning enabled per default (can be disabled)
    - Downstream Broadcast packets are discarded thus also blocking the unknown, flooded traffic
    - Downstream Multicast packets are allowed when IGMP snooping is enabled
  
  - Spoke SDPs which are members of this Residential Split Horizon Group will have:
    - Downstream multicast traffic supported
    - Double-pass queuing is not applicable
    - STP is disabled (can be enabled)
    - MAC pinning enabled per default (can be disabled)

**Default**

A split horizon group is by default not created as a residential-group.

### auto-learn-mac-protect

**Syntax**

[no] auto-learn-mac-protect

**Context**

config>service>vpls>sap
config>service>vpls>spoke-sdp
config>service>vpls>mesh-sdp
config>service>vpls>split-horizon-group
config>service>vpls>endpoint
config>service>pw-template
**SDP Commands**

config>service>pw-template>split-horizon-group

**Description**
This command enables the automatic protection of source MAC addresses learned on the associated object. MAC protection is used in conjunction with restrict-protected-src, restrict-unprotected-dst and mac-protect. When this command is applied or removed, the MAC addresses are cleared from the related object.

When the auto-learn-mac-protect is enabled on an SHG the action only applies to the associated SAPs (no action is taken by default for spoke SDPs in the SHG). In order to enable this function for spoke SDPs within a SHG, the auto-learn-mac-protect must be enabled explicitly under the spoke-SDP. If required, auto-learn-mac-protect can also be enabled explicitly under specific SAPs within the SHG. For more information about auto-learn MAC protect, refer to Auto-Learn MAC Protect on page 555.

**Default**
no auto-learn-mac-protect

**restrict-protected-src**

**Syntax**
restrict-protected-src [alarm-only | discard-frame]

no restrict-protected-src

**Context**
config>service>vpls>sap
config>service>vpls>spoke-sdp
config>service>vpls>mesh-sdp
config>service>vpls>split-horizon-group
config>service>vpls>endpoint
config>service>pw-template>
config>service>pw-template>split-horizon-group

**Description**
This command indicates how the agent will handle relearn requests for protected MAC addresses, either manually added using the mac-protect command or automatically added using the auto-learn-mac-protect command. While enabled all packets entering the configured SAP, spoke-SDP, mesh-SDP, or any SAP that is part of the configured split horizon group (SHG) will be verified not to contain a protected source MAC address. If the packet is found to contain such an address, the action taken depends on the parameter specified on the restrict-protected-src command, namely:

- **No parameter**
  The packet will be discarded, an alarm will be generated and the SAP, spoke-SDP or mesh-SDP will be set operationally down. The SAP, spoke-SDP or mesh-SDP must be shutdown and enabled (no shutdown) for this state to be cleared.

- **alarm-only**
  The packet will be forwarded, an alarm will be generated but the source MAC is not learned on the SAP/spoke-SDP/mesh-SDP.

- **discard-frame**
  The packet will be discarded and an alarm generated. The frequency of alarm generation is fixed to be at most one alarm per MAC address per FP2 per 10 minutes in a given VPLS service. This parameter is only applicable to automatically protected MAC addresses.

When the restrict-protected-src is enabled on an SHG the action only applies to the associated SAPs (no action is taken by default for spoke SDPs in the SHG). In order to enable this function for spoke SDPs within a SHG, the restrict-protected-src must be enabled explicitly under the spoke-SDP. If required, restrict-protected-src can also be enabled explicitly under specific SAPs within the SHG.
When this command is applied or removed, with either the alarm-only or discard-frame parameters, the MAC addresses are cleared from the related object.

The use of “restrict-protected-src discard-frame” is mutually exclusive with both the “restrict-protected-src [alarm-only]” command and with the configuration of manually protected MAC addresses within a given VPLS. “restrict-protected-src discard-frame” can only be enabled on SAPs on FP2 or later hardware or on SDPs where all network interfaces are on FP2 or later hardware.

**Parameters**

- **alarm-only** — Specifies that the packet will be forwarded, an alarm will be generated but the source MAC is not learned on the SAP/spoke-SDP/mesh-SDP.
  
  **Default** no alarm-only

- **discard-frame** — Specifies that the packet will be discarded and an alarm generated. The frequency of alarm generation is fixed to be at most one alarm per FP2 per MAC address per 10 minutes within a given VPLS service.
  
  **Default** no discard-frame

**Default** no restrict-protected-src

---

**restrict-unprotected-dst**

**Syntax**

```
restrict-unprotected-dst alarm-only
no restrict-unprotected-dst
```

**Context**

- `config>service>pw-template>split-horizon-group`
- `config>service>vpls>split-horizon-group`
- `config>service>vpls>sap`

**Description**

This command indicates how the system will forward packets destined to an unprotected MAC address, either manually added using the mac-protect command or automatically added using the auto-learn-mac-protect command. While enabled all packets entering the configured SAP or SAPs within a split-horizon-group (but not spoke or mesh-SDPs) will be verified to contain a protected destination MAC address. If the packet is found to contain a non-protected destination MAC, it will be discarded. Detecting a non-protected destination MAC on the SAP will not cause the SAP to be placed in the operationally down state. No alarms are generated.

If the destination MAC address is unknown, even if the packet is entering a restricted SAP, with restrict-unprotected-dst enabled, it will be flooded.

**Default** no restrict-unprotected-dst

---

**vc-type**

**Syntax**

```
vc-type {ether | vlan}
```

**Context**

`config>service>pw-template`

**Description**

This command overrides the default VC type signaled for the binding to the far end SDP. The VC type is a 15 bit-quantity containing a value which represents the type of VC. The actual signaling of the VC type depends on the signaling parameter defined for the SDP. If signaling is disabled, the `vc-type` command can...
still be used to define the dot1q value expected by the far-end provider equipment. A change of the bindings VC type causes the binding to signal the new VC type to the far end when signaling is enabled. VC types are derived according to IETF draft-martini-l2circuit-trans-mpls.

- The VC type value for Ethernet is 0x0005.
- The VC type value for an Ethernet VLAN is 0x0004.

**Parameters**

ether — Defines the VC type as Ethernet. The ethernet and vlan keywords are mutually exclusive. When the VC type is not defined then the default is Ethernet for spoke SDP bindings. Defining Ethernet is the same as executing no vc-type and restores the default VC type for the spoke SDP binding. (hex 5)

vlan — Defines the VC type as VLAN. The ethernet and vlan keywords are mutually exclusive. When the VC type is not defined then the default is Ethernet for spoke SDP bindings.

dot1q

**Syntax**

```
vlan-vc-tag 0..4094
no vlan-vc-tag [0..4094]
```

**Context**

config>service>pw-template

**Description**

This command specifies an explicit dot1q value used when encapsulating to the SDP far end. When signaling is enabled between the near and far end, the configured dot1q tag can be overridden by a received TLV specifying the dot1q value expected by the far end. This signaled value must be stored as the remote signaled dot1q value for the binding. The provisioned local dot1q tag must be stored as the administrative dot1q value for the binding.

When the dot1q tag is not defined, the default value of zero is stored as the administrative dot1q value. Setting the value to zero is equivalent to not specifying the value.

The no form of this command disables the command.

**Default**

no vlan-vc-tag

**Parameters**

- 0..4094 — Specifies a valid VLAN identifier to bind an 802.1Q VLAN tag ID.

adv-mtu-override

**Syntax**

```
[no] adv-mtu-override
```

**Context**

config>service>sdp

**Description**

This command overrides the advertised VC-type MTU of all spoke-sdp's of L2 services using this SDP-ID. When enabled, the router signals a VC MTU equal to the service MTU, which includes the Layer 2 header. It also allows this router to accept an MTU advertised by the far end PE which value matches either its advertised MTU or its advertised MTU minus the L2 headers.

By default, the router advertizes a VC-MTU equal to the L2 service MTU minus the Layer 2 header and always matches its advertized MTU to that signaled by the far-end PE router, otherwise the spoke-sdp goes operationally down.

When this command is enabled on the SDP, it has no effect on a spoke-sdp of an IES/VPRN spoke interface using this SDP-ID. The router continues to signal a VC MTU equal to the net IP interface MTU, which is
min\{ip-mtu, sdp operational path mtu - L2 headers\}. The router also continues to make sure that the advertised MTU values of both PE routers match or the spoke-sdp goes operationally down.

The no form of the command disables the VC-type MTU override and returns to the default behavior.

Default: no adv-mtu-override

**binding**

**Syntax:** binding

**Context:** config>service>sdp

**Description:** The command enables the context to configure SDP bindings.

**port**

**Syntax:**

```
port [port-id | lag-id]
no port
```

**Context:** config>service>sdp>binding

**Description:** This command specifies the port or lag identifier, to which the pseudowire ports associated with the underlying SDP are bound. If the underlying SDP is re-routed to a port or lag other than the specified one, the pseudowire ports on the SDP are operationally brought down.

The no form of the command removes the value from the configuration.

Default: none

**Parameters**

- `port-id` — The identifier of the port in the slot/mda/port format.
- `lag-id` — Specifies the LAG identifier.

**pw-port**

**Syntax:**

```
pw-port pw-port-id [vc-id vc-id] [create]
no pw-port
```

**Context:** config>service>sdp>binding

**Description:** This command creates a pseudowire port.

The no form of the command removes the pseudowire port ID from the configuration.

Default: none

**Parameters**

- `pw-port-id` — Specifies a unique identifier of the pseudowire port.
  - **Values:** 1 — 10239
vc-id

Specifies a virtual circuit identifier signaled to the peer.

Values

   1 — 4294967295

encap-type

Syntax

encap-type {dot1q|qinq}

no encap-type

Context

config>service>sdp>binding>pw-port

Description

This command sets the encapsulation type for the pseudowire port as dot1q or qinq.

Default

dot1q

Parameters

dot1q — Specifies dot1q encapsulation type.

qinq — Specifies qinq encapsulation type.

vc-type

Syntax

vc-type {ether|vlan}

no vc-type

Context

config>service>sdp>binding>pw-port

Description

This command sets the forwarding mode for the pseudowire port. The vc-type is signaled to the peer, and must be configured consistently on both ends of the pseudowire. vc-type VLAN is only configurable with dot1q encapsulation on the pseudowire port. The tag with vc-type vlan only has significance for transport, and is not used for service delineation or ESM. The top (provider tag) is stripped while forwarding out of the pseudowire, and a configured vlan-tag (for vc-type vlan) is inserted when forwarding into the pseudowire. With vc-type ether, the tags if present (max 2), are transparently preserved when forwarding in our out of the pseudowire.

The no form of the command reverts to the default value.

Default

ether

Parameters

ether — Specifies ether as the virtual circuit (VC) associated with the SDP binding.

vlan — Specifies vlan as the virtual circuit (VC) associated with the SDP binding.

vlan-vc-tag

Syntax

vlan-vc-tag vlan-id

no vc-type

Context

config>service>sdp>binding>pw-port

Description

This command sets tag relevant for vc-type vlan mode. This tag is inserted in traffic forwarded into the pseudowire.
The **no** form of the command reverts to the default value.

**Default**  
0

**Parameters**  
`vlan-id` — Specifies the VLAN ID value.

**Values**  
0 — 4094

### egress

**Syntax**  
egress

**Context**  
`config>service>sdp>binding>pw-port`

**Description**  
This command enters egress configuration context for the vport.

**Default**  
none

### shaper

**Syntax**  
[**no**] shaper

**Context**  
`config>service>sdp>binding>pw-port>egress`

**Description**  
This command configures an egress shaping option for use by a pseudowire port.

**Default**  
no shaper.

### class-forwarding

**Syntax**  
`class-forwarding [default-lsp lsp-name]`

**Context**  
`config>service>sdp`

**Description**  
This command enables the forwarding of a service packet over the SDP based on the class of service of the packet. Specifically, the packet is forwarded on the RSVP LSP or static LSP whose forwarding class matches that of the packet. The user maps the system forwarding classes to LSPs using the `config>service>sdp>class-forwarding>fc` command. If there is no LSP that matches the packet’s forwarding class, the default LSP is used. If the packet is a VPLS multicast/broadcast packet and the user did not explicitly specify the LSP to use under the `config>service>sdp>class-forwarding>multicast-lsp` context, then the default LSP is used.

VLL service packets are forwarded based on their forwarding class only if shared queuing is enabled on the ingress SAP. Shared queuing must be enabled on the VLL ingress SAP if class-forwarding is enabled on the SDP the service is bound to. Otherwise, the VLL packets will be forwarded to the LSP which is the result of hashing the VLL service ID. Since there are eight entries in the ECMP table for an SDP, one LSP ID for each forwarding class, the resulting load balancing of VLL service ID is weighted by the number of times an LSP appears on that table. For instance, if there are eight LSPs, the result of the hashing will be similar to when class based forwarding is disabled on the SDP. If there are fewer LSPs, then the LSPs which were
mapped to more than one forwarding class, including the default LSP, will have proportionally more VLL services forwarding to them.

Class-based forwarding is not supported on a spoke SDP used for termination on an IES or VPRN service. All packets are forwarded over the default LSP.

The no form of the command deletes the configuration and the SDP reverts back to forwarding service packets based on the hash algorithm used for LAG and ECMP.

**Default**

`no class-forwarding` — Packets of a service bound to this SDP will be forwarded based on the hash algorithm used for LAG and ECMP.

**Parameters**

`default-lsp lsp-name` — Specifies the default LSP for the SDP. This LSP name must exist and must have been associated with this SDP using the `lsp-name` configured in the `config>service>sdp>lsp` context. The default LSP is used to forward packets when there is no available LSP which matches the packet’s forwarding class. This could be because the LSP associated with the packet’s forwarding class is down, or that the user did not configure a mapping of the packet’s forwarding class to an LSP using the `config>service>sdp<class-forwarding>fc` command. The default LSP is also used to forward VPLS service multicast/broadcast packets in the absence of a user configuration indicating an explicit association to one of the SDP LSPs.

Note that when the default LSP is down, the SDP is also brought down. The user will not be able to enter the class-forwarding node if the default LSP was not previously specified. In other words the class-forwarding for this SDP will remain shutdown.

**enforce-diffserv-lsp-fc**

**Syntax**

```plaintext
[no] enforce-diffserv-lsp-fc
```

**Context**

`config>service>sdp<class-forwarding`

**Description**

This command enables checking by RSVP that a Forwarding Class (FC) mapping to an LSP under the SDP configuration is compatible with the Diff-Serv Class Type (CT) configuration for this LSP.

When the user enables this option, the service manager enquires with RSVP if the FC is supported by the LSP. RSVP checks if the FC maps to the CT of the LSP, for example, the default class-type value or the class-type value entered at the LSP configuration level.

If RSVP did not validate the FC, then the service manager will return an error and the check has failed. In this case, packets matching this FC will be forwarded over the default LSP. Any addition of an LSP to an SDP that will not satisfy the FC check will also be rejected.

The service manager does no validate the default-lsp FC-to-CT mapping. Whether or not the FC is validated, the default-lsp will always end up being used in this case.

RSVP will not allow the user to change the CT of the LSP until no SDP with class-based forwarding enabled and the `enforce-diffserv-lsp-fc` option enabled is using this LSP. All other SDPs using this LSP are not concerned by this rule.

The SDP will continue to enforce the mapping of a single LSP per FC. However, when `enforce-diffserv-lsp-fc` enabled, RSVP will also enforce the use of a single CT per FC as per the user configured mapping in RSVP.

If class-forwarding is enabled but `enforce-diffserv-lsp-fc` is disabled, forwarding of the service packets will continue to be based on the user entered mapping of FC to LSP name without further validation as per the existing implementation. The CT of the LSP does not matter in this case.
If class-forwarding is not enabled on the SDP, forwarding of the service packets will continue to be based on the ECMP/LAG hash routine. The CT of the LSP does not matter in this case.

The no form of this command reverts to the default value which is to use the user entered mapping of FC to LSP name.

Default no enforce-diffserv-lsp-fc

**far-end**

**Syntax**

```
far-end ip-address | {node-id node-id [global-id global-id]}
no far-end
```

**Context**

config>service>sdp

**Description**

This command configures the system IP address of the far-end destination router for the Service Distribution Point (SDP) that is the termination point for a service.

The far-end IP address must be explicitly configured. The destination IP address must be a 7950 SR system IP address.

If the SDP uses GRE for the destination encapsulation, the ip-address is checked against other GRE SDPs to verify uniqueness. If the ip-address is not unique within the configured GRE SDPs, an error is generated and the ip-address is not associated with the SDP. The local device may not know whether the ip-address is actually a system IP interface address on the far end device.

If the SDP uses MPLS encapsulation, the far-end ip-address is used to check LSP names when added to the SDP. If the “to IP address” defined within the LSP configuration does not exactly match the SDP far-end ip-address, the LSP will not be added to the SDP and an error will be generated. Alternatively, and SDP that uses MPLS can have an MPLS-TP node with an MPLS-TP node-id and (optionally) global-id. In this case, the SDP must use an MPLS-TP LSP and the SDP signaling parameter must be set to off.

An SDP cannot be administratively enabled until a far-end ip-address or MPLS-TP node-id is defined. The SDP is operational when it is administratively enabled (no shutdown) and the far-end ip-address is contained in the IGP routing table as a host route. OSPF ABRs should not summarize host routes between areas. This can cause SDPs to become operationally down. Static host routes (direct and indirect) can be defined in the local device to alleviate this issue.

The no form of this command removes the currently configured destination IP address for the SDP. The ip-address parameter is not specified and will generate an error if used in the no far-end command. The SDP must be administratively disabled using the config service sdp shutdown command before the no far-end command can be executed. Removing the far end IP address will cause all lsp-name associations with the SDP to be removed.

Default none

**Parameters**

- **ip-address** — The system address of the far-end 7950 SR for the SDP in dotted decimal notation.

- **node-id** — The MPLS-TP Node ID of the far-end system for the SDP, either in dotted decimal notation (a.b.c.d) or an unsigned 32-bit integer (1 – 4294967295). This parameter is mandatory for an SDP using an MPLS-TP LSP.

- **global-id** — The MPLS-TP Global ID of the far-end system for the SDP, in an unsigned 32-bit integer (0 – 4294967295). This parameter is optional for an SDP using an MPLS-TP LSP. If not entered, a default value for the Global ID of ‘0’ is used. A global ID of ‘0’ indicates that the far end
node is in the same domain as the local node. The user must explicitly configure a Global ID if its value is non-zero.

fc

Syntax: fc {be | I2 | af | I1 | h2 | ef | h1 | nc} lsp lsp-name
no fc {be | I2 | af | I1 | h2 | ef | h1 | nc}

Context: config>service>sdp>forwarding-class

Description: This command makes an explicit association between a forwarding class and an LSP. The LSP name must exist and must have been associated with this SDP using the command config>service>sdp>lsp. Multiple forwarding classes can be associated with the same LSP. However, a forwarding class can only be associated with a single LSP in a given SDP. All subclasses will be assigned to the same LSP as the parent forwarding class.

Default: none

Parameters:
- lsp lsp-name — Specifies the RSVP or static LSP to use to forward service packets which are classified into the specified forwarding class.

multicast-lsp

Syntax: multicast-lsp lsp-name
no multicast-lsp

Context: config>service>sdp>forwarding-class

Description: This command specifies the RSVP or static LSP in this SDP to use to forward VPLS multicast and broadcast packets. The LSP name must exist and must have been associated with this SDP using the command config>service>sdp>lsp. In the absence of an explicit configuration by the user, the default LSP is used.

Default: default-lsp-name

ldp

Syntax: [no] ldp

Context: config>service>sdp

Description: This command enables LDP-signaled LSP’s on MPLS-encapsulated SDPs.

In MPLS SDP configurations either one LSP can be specified or LDP can be enabled. The SDP ldp and lsp commands are mutually exclusive. If an LSP is specified on an MPLS SDP, then LDP cannot be enabled on the SDP. To enable LDP on the SDP when an LSP is already specified, the LSP must be removed from the configuration using the no lsp lsp-name command.

Alternatively, if LDP is already enabled on an MPLS SDP, then an LSP cannot be specified on the SDP. To specify an LSP on the SDP, the LDP must be disabled. The LSP must have already been created in the config>router>mpls context with a valid far-end IP address. The above rules are relaxed when the mixed-
Services

lsp option is enabled on the SDP.

**Default** no ldp (disabled)

### lsp

**Syntax**

```
lsp lsp-name
no lsp lsp-name
```

**Context**

config>service>sdp

**Description**

This command creates associations between one or more label switched paths (LSPs) and an Multi-Protocol Label Switching (MPLS) Service Distribution Point (SDP). This command is implemented only on MPLS-type encapsulated SDPs.

In MPLS SDP configurations either one LSP can be specified or LDP can be enabled. The SDP ldp and lsp commands are mutually exclusive. If an LSP is specified on an MPLS SDP, then LDP cannot be enabled on the SDP. To enable LDP on the SDP when an LSP is already specified, the LSP must be removed from the configuration using the **no lsp lsp-name** command.

Alternatively, if LDP is already enabled on an MPLS SDP, then an LSP cannot be specified on the SDP. To specify an LSP on the SDP, the LDP must be disabled. The LSP must have already been created in the **config>router>mpls** context. with a valid far-end IP address. RSVP must be enabled.

If no LSP is associated with an MPLS SDP, the SDP cannot enter the operationally up state. The SDP can be administratively enabled (**no shutdown**) with no LSP associations. The **lsp-name** may be shutdown, causing the association with the SDP to be operationally down (the LSP will not be used by the SDP).

Up to 16 LSP names can be entered on a single command line.

The **no** form of this command deletes one or more LSP associations from an SDP. If the **lsp-name** does not exist as an association or as a configured LSP, no error is returned. An **lsp-name** must be removed from all SDP associations before the **lsp-name** can be deleted from the system. The SDP must be administratively disabled (**shutdown**) before the last **lsp-name** association with the SDP is deleted.

**Default** none

**Parameters**

```
lsp-name — The name of the LSP to associate with the SDP. An LSP name is case sensitive and is limited to 32 ASCII 7-bit printable characters with no spaces. If an exact match of **lsp-name** does not already exist as a defined LSP, an error message is generated. If the **lsp-name** does exist and the LSP to IP address matches the SDP far-end IP address, the association is created.
```

### metric

**Syntax**

```
metric metric
no metric
```

**Context**

config>service>sdp

**Description**

This command specifies the metric to be used within the tunnel table manager for decision making purposes. When multiple SDPs going to the same destination exist, this value is used as a tie-breaker by tunnel table manager users such as MP-BGP to select the route with the lower value.
mixed-lsp-mode

Parameters

metric — Specifies the SDP metric.

Values

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 — 65535</td>
<td></td>
</tr>
</tbody>
</table>

Syntax

[no] mixed-lsp-mode

Context

config>service>sdp

Description

This command enables the use by an SDP of the mixed-LSP mode of operation. This command indicates to the service manager that it must allow a primary LSP type and a backup LSP type in the same SDP configuration. For example, the lsp and ldp commands are allowed concurrently in the SDP configuration. The user can configure one or two types of LSPs under the same SDP. Without this command, these commands are mutually exclusive.

The user can configure an RSVP LSP as a primary LSP type with an LDP LSP as a backup type. The user can also configure a BGP RFC 3107 BGP LSP as a backup LSP type.

If the user configures an LDP LSP as a primary LSP type, then the backup LSP type must be an RFC 3107 BGP labeled route.

At any given time, the service manager programs only one type of LSP in the linecard that will activate it to forward service packets according to the following priority order:

1. RSVP LSP type. Up to 16 RSVP LSPs can be entered by the user and programmed by the service manager in ingress linecard to load balance service packets. This is the highest priority LSP type.
2. LDP LSP type. One LDP FEC programmed by service manager but ingress linecard can use up to 16 LDP ECMP paths for the FEC to load balance service packets when ECMP is enabled on the node.
3. BGP LSP type. One RFC 3107-labeled BGP prefix programmed by the service manager. The ingress linecard can use more than one next-hop for the prefix.

In the case of the RSVP/LDP SDP, the service manager will program the NHLFE(s) for the active LSP type preferring the RSVP LSP type over the LDP LSP type. If no RSVP LSP is configured or all configured RSVP LSPs go down, the service manager will re-program the linecard with the LDP LSP if available. If not, the SDP goes operationally down.

When a higher priority type LSP becomes available, the service manager reverts back to this LSP at the expiry of the sdp-revert-time timer or the failure of the currently active LSP, whichever comes first. The service manager then re-programs the linecard accordingly. If the infinite value is configured, then the SDP reverts to the highest priority type LSP only if the currently active LSP failed.

Note however, that LDP uses a tunnel down damp timer which is set to three seconds by default. When the LDP LSP fails, the SDP will revert to the RSVP LSP type after the expiry of this timer. For an immediate switchover this timer must be set to zero. Use the configure>router>ldp>tunnel-down-damp-time command.

If the user changes the value of the sdp-revert-time timer, it will take effect only at the next use of the timer. Any timer which is outstanding at the time of the change will be restarted with the new value.

If class based forwarding is enabled for this SDP, the forwarding of the packets over the RSVP LSPs will be based on the FC of the packet as in current implementation. When the SDP activates the LDP LSP type, then packets are forwarded over the LDP ECMP paths using the regular hash routine.
In the case of the LDP/BGP SDP, the service manager will prefer the LDP LSP type over the BGP LSP type. The service manager will re-program the linecard with the BGP LSP if available otherwise it brings down the SDP operationally.

Also Note the following difference in behavior of the LDP/BGP SDP compared to that of an RSVP/LDP SDP. For a given /32 prefix, only a single route will exist in the routing table: the IGP route or the BGP route. Thus, either the LDP FEC or the BGP label route is active at any given time. The impact of this is that the tunnel table needs to be re-programmed each time a route is deactivated and the other is activated. Furthermore, the SDP revert-time cannot be used since there is no situation where both LSP types are active for the same /32 prefix.

The no form of this command disables the mixed-LSP mode of operation. The user first has to remove one of the LSP types from the SDP configuration or the command will fail.

**Default**

```
no mixed-lsp-mode
```

### sdp-revert-time

**Syntax**

```
sdp-revert-time seconds | infinite
no sdp-revert-time
```

**Context**

```
config>service>sdp>mixed-lsp-mode
```

**Description**

This command configures the delay period the SDP must wait before it reverts to a higher priority LSP type when one becomes available.

The no form of the command resets the timer to the default value of 0. This means the SDP reverts immediately to a higher priority LSP type when one becomes available.

**Default**

0

**Parameters**

- `seconds` — Specifies the delay period, in seconds, that the SDP must wait before it reverts to a higher priority LSP type when one becomes available. A value of zero means the SDP reverts immediately to a higher priority LSP type when one becomes available.

  **Values**

  - 0 — 600

  - `infinite` — This keyword forces the SDP to never revert to another higher priority LSP type unless the currently active LSP type is down.

### sdp-group

**Syntax**

```
[no] sdp-group group-name
```

**Context**

```
config>service>sdp
```

**Description**

This command configures the SDP membership in admin groups.

The user can enter a maximum of one (1) admin group name at once. The user can execute the command multiple times to add membership to more than one admin group. The admin group name must have been configured or the command is failed. Admin groups are supported on an SDP of type GRE and of type MPLS (BGP/RSVP/LDP). They are also supported on an SDP with the mixed-lsp-mode option enabled.

The no form of this command removes this SDP membership to the specified admin group.
SDP Commands

**Default**

none

**Parameters**

group-name — Specifies the name of the SDP admin group. A maximum of 32 characters can be entered.

**group-name**

**Syntax**

```
group-name group-name value group-value
no group-name group-value
```

**Context**

config>service>sdp-group

**Description**

This command defines SDP administrative groups, referred to as SDP admin groups. SDP admin groups provide a way for services using a PW template to automatically include or exclude specific provisioned SDPs. SDPs sharing a specific characteristic or attribute can be made members of the same admin group. When users configure a PW template, they can include and/or exclude one or more admin groups. When the service is bound to the PW template, the SDP selection rules will enforce the admin group constraints specified in the `sdp-include` and `sdp-exclude` commands.

A maximum of 32 admin groups can be created. The group value ranges from zero (0) to 31. It is uniquely associated with the group name at creation time. If the user attempts to configure another group name for a group value that is already assigned to an existing group name, the SDP admin group creation is failed. The same happens if the user attempts to configure an SDP admin group with a new name but associates it to a group value already assigned to an existing group name.

The `no` option of this command deletes the SDP admin group but is only allowed if the group-name is not referenced in a pw-template or SDP.

**Default**

none

**Parameters**

group-name — Specifies the name of the SDP admin group. A maximum of 32 characters can be entered.

value group-value — Specifies the group value associated with this SDP admin group. This value is unique within the system.

**Values**

0—31

**signaling**

**Syntax**

```
signaling {off | tldp | bgp}
```

**Context**

config>service>sdp

**Description**

This command specifies the signaling protocol used to obtain the ingress and egress pseudowire labels in frames transmitted and received on the SDP. When signaling is `off` then labels are manually configured when the SDP is bound to a service. The signalling value can only be changed while the administrative status of the SDP is down. Additionally, the signaling can only be changed on an SDP if that SDP is not in use by BGP-AD or BGP-VPLS. BGP signaling can only be enabled if that SDP does not already have pseudowires signaled over it. Also, BGP signaling is not supported with mixed mode LSP SDPs.

The `no` form of this command is not applicable. To modify the signaling configuration, the SDP must be administratively shut down and then the signaling parameter can be modified and re-enabled.
Default  tldp

Parameters  off — Ingress and egress signal auto-labeling is not enabled. If this parameter is selected, then each service using the specified SDP must manually configure VPN labels. This configuration is independent of the SDP’s transport type, GRE, MPLS (RSVP or LDP).

tldp — Ingress and egress pseudowire signaling using T-LDP is enabled. Default value used when BGP AD automatically instantiates the SDP.

bgp — Ingress and egress pseudowire signaling using BGP is enabled. Default value used when BGP VPLS automatically instantiates the SDP.

tunnel-far-end

Syntax  tunnel-far-end ip-address
do tunnel-far-end [ip-address]

Context  config>service>sdp

Description  This command enables the user to specify an SDP tunnel destination address that is different from the configuration in the SDP far-end option.

The SDP must be shutdown first to add or change the configuration of the tunnel-far-end option.

When this option is enabled, service packets are encapsulated using an LDP LSP with a FEC prefix matching the value entered in ip-address. By default, service packets are encapsulated using an LDP LSP with a FEC prefix matching the address entered in the SDP far-end option.

The T-LDP session to the remote PE is still targeted to the address configured under the far-end option. This means that targeted “hello” messages are sent to the far-end address, which is also the LSR-ID of the remote node. TCP based LDP messages, such as initialization and label mapping messages, are sent to the address specified in the transport-address field of the “hello” message received from the remote PE. This address can be the same as the remote PE LSR-ID, or a different address. This feature works, however, if the signaling option in the SDP is set to off instead of tldp, in which case, the service labels are statically configured.

This feature operates on an SDP of type LDP only. It can be used with VLL, VPLS, and VPRN services when an explicit binding to an SDP with the tunnel-far-end option is specified. It also operates with a spoke interface on an IES or VPRN service. Finally, this feature operates with a BGP AD based VPLS service when the use-provisioned-sdp option is enabled in the pseudowire template.

This feature is not supported in an SDP of type MPLS when an RSVP LSP name is configured under the SDP. It also does not work with a mixed-lsp SDP.

The no form of this command disables the use of the tunnel-far-end option and returns to using the address specified in the far-end.

Default  no tunnel-far-end

Parameters  ip-address — The system address of the far-end router for the SDP in dotted decimal notation.

path-mtu

Syntax  path-mtu bytes
no path-mtu

**Context** config>service>sdp

**Description** This command configures the Maximum Transmission Unit (MTU) in bytes that the Service Distribution Point (SDP) can transmit to the far-end device router without packet dropping or IP fragmentation overriding the SDP-type default path-mtu.

The default SDP-type path-mtu can be overridden on a per SDP basis. Dynamic maintenance protocols on the SDP like RSVP may override this setting.

If the physical mtu on an egress interface or PoS channel indicates the next hop on an SDP path cannot support the current path-mtu, the operational path-mtu on that SDP will be modified to a value that can be transmitted without fragmentation.

The no form of this command removes any path-mtu defined on the SDP and the SDP will use the system default for the SDP type.

**Default** The default path-mtu defined on the system for the type of SDP is used.

network-domain

**Syntax** network-domain network-domain-name

no network-domain

**Context** config>service>sdp

**Description** This command assigns a given SDP to a given network-domain. The network-domain is then taken into account during sap-ingress queue allocation for VPLS SAP.

The network-domain association can only be done in a base-routing context. Associating a network domain with an loop-back or system interface will be rejected. Associating a network-domain with an interface that has no physical port specified will be accepted, but will have no effect as long as a corresponding port, or LAG, is undefined.

A single SDP can only be associated with a single network-domain.

**Default** per default “default” network domain is assigned

pbb-etype

**Syntax** pbb-etype [0x0600..0xffff]

no pbb-etype

**Context** configure>service>sdp

**Default** 0x88E7

**Description** This command configures the Ethertype used for PBB.

**Values** 0x0600..0xffff: 1536 — 65535 (accepted in decimal or hex)
source-bmac-lsb

Syntax

source-bmac-lsb MAC-lsb control-pw-vc-id vc-id
no source-bmac-lsb

Context config>service>sdp

Description This command defines the 16 least significant bits (lsb) which, when combined with the 32 most significant bits of the PBB source-bmac, are used as the virtual backbone MAC associated with this SDP. The virtual backbone MAC is used as the source backbone MAC for traffic received on a PBB EPIPE spoke-SDP with use-sdp-bmac configured (that is, a redundant pseudowire) and forwarded into the B-VPLS domain.

The control-pw-vc-id defines VC identifier of the spoke-SDP relating to the control pseudowire whose status is to be used to determine whether SPBM advertises this virtual backbone MAC. This is a mandatory parameter when the source-bmac-lsb is added or changed. The spoke SDP must have the parameter use-sdp-bmac for the control pseudowire to be active.

Default no source-bmac-lsb

MAC-lsb — Specifies the 16 least significant bits of the virtual backbone MAC associated with this SDP.
Values [1..65535] or xx-xx or xx:xx

control-pw-vc-id vc-id — Specifies the VC identifier of the control pseudowire.
Values 1 — 4294967295

vlan-vc-etype

Syntax

vlan-vc-etype 0x0600..0xffff
no vlan-vc-etype [0x0600..0xffff]

Context config>service>sdp

Description This command configures the VLAN VC EtherType.
The no form of this command returns the value to the default.

Default no vlan-vc-etype

Parameters 0x0600..0xffff — Specifies a valid VLAN etype identifier.
SDP Keepalive Commands

keep-alive

Syntax
keepalive

Context
config>service>sdp

Description
Context for configuring SDP connectivity monitoring keepalive messages for the SDP ID.

SDP-ID keepalive messages use SDP Echo Request and Reply messages to monitor SDP connectivity. The operating state of the SDP is affected by the keepalive state on the SDP-ID. SDP Echo Request messages are only sent when the SDP-ID is completely configured and administratively up. If the SDP-ID is administratively down, keepalives for that SDP-ID are disabled. SDP Echo Requests (when sent for keepalive messages) are always sent with the `originator-sdp-id`. All SDP-ID keepalive SDP Echo Replies are sent using generic IP/GRE OAM encapsulation.

When a keepalive response is received that indicates an error condition, the SDP ID will immediately be brought operationally down. Once a response is received that indicates the error has cleared and the `hold-down-time` interval has expired, the SDP ID will be eligible to be put into the operationally up state. If no other condition prevents the operational change, the SDP ID will enter the operational state.

A set of event counters track the number of keepalive requests sent, the size of the message sent, non-error replies received and error replies received. A keepalive state value is kept indicating the last response event. A keepalive state timestamp value is kept indicating the time of the last event. With each keepalive event change, a log message is generated indicating the event type and the timestamp value.

The table below describes keepalive interpretation of SDP echo reply response conditions and the effect on the SDP ID operational status.

<table>
<thead>
<tr>
<th>Result of Request</th>
<th>Stored Response State</th>
<th>Operational State</th>
</tr>
</thead>
<tbody>
<tr>
<td>keepalive request timeout without reply</td>
<td>Request Timeout</td>
<td>Down</td>
</tr>
<tr>
<td>keepalive request not sent due to non-existent <code>orig-sdp-id</code></td>
<td>Orig-SDP Non-Existent</td>
<td>Down</td>
</tr>
<tr>
<td>keepalive request not sent due to administratively down <code>orig-sdp-id</code></td>
<td>Orig-SDP Admin-Down</td>
<td>Down</td>
</tr>
<tr>
<td>keepalive reply received, invalid origination-id</td>
<td>Far End: Originator-ID Invalid</td>
<td>Down</td>
</tr>
<tr>
<td>keepalive reply received, invalid responder-id</td>
<td>Far End: Responder-ID Error</td>
<td>Down</td>
</tr>
<tr>
<td>keepalive reply received, No Error</td>
<td>Success</td>
<td>Up (If no other condition prevents)</td>
</tr>
</tbody>
</table>

a. This condition should not occur.

Page 226
hello-time

Syntax  hello-time seconds
       no hello-time

Context  config>service>sdp>keep-alive

Description  Configures the time period between SDP keepalive messages on the SDP-ID for the SDP connectivity monitoring messages.

The no form of this command reverts the hello-time seconds value to the default setting.

Default  hello-time 10 — 10 seconds between keepalive messages

seconds — The time period in seconds between SDP keepalive messages, expressed as a decimal integer.

Values  1 — 3600

hold-down-time

Syntax  hold-down-time seconds
       no hold-down-time

Context  config>service>sdp>keep-alive

Description  Configures the minimum time period the SDP will remain in the operationally down state in response to SDP keepalive monitoring.

This parameter can be used to prevent the SDP operational state from “flapping” by rapidly transitioning between the operationally up and operationally down states based on keepalive messages.

When an SDP keepalive response is received that indicates an error condition or the max-drop-count keepalive messages receive no reply, the sdp-id will immediately be brought operationally down. If a keepalive response is received that indicates the error has cleared, the sdp-id will be eligible to be put into the operationally up state only after the hold-down-time interval has expired.

The no form of this command reverts the hold-down-time seconds value to the default setting.

Default  hold-down-time 10 — The SDP is operationally down for 10 seconds after an SDP keepalive error.

Parameters  seconds — The time in seconds, expressed as a decimal integer, the sdp-id will remain in the operationally down state before it is eligible to enter the operationally up state. A value of 0 indicates that no hold-down-time will be enforced for sdp-id.

Values  0 — 3600

max-drop-count

Syntax  max-drop-count count
       no max-drop-count

Context  config>service>sdp>keep-alive

Description  This command configures the number of consecutive SDP keepalive failed request attempts or remote
replies that can be missed after which the SDP is operationally downed. If the `max-drop-count` consecutive keepalive request messages cannot be sent or no replies are received, the SDP-ID will be brought operationally down by the keepalive SDP monitoring. The `no` form of this command reverts the `max-drop-count count` value to the default settings.

**Default**  
`max-drop-count 3`

**Parameters**  
`count` — The number of consecutive SDP keepalive requests that are failed to be sent or replies missed, expressed as a decimal integer.

**Values**  
1 — 5

### message-length

**Syntax**  
`message-length octets`

**no** `message-length`

**Context**  
`config>service>sdp>keep-alive`

**Description**  
This command configures the SDP monitoring keepalive request message length transmitted. The `no` form of this command reverts the `message-length octets` value to the default setting.

**Default**  
0 — The message length should be equal to the SDP’s operating path MTU as configured in the `path-mtu` command. If the default size is overridden, the actual size used will be the smaller of the operational SDP-ID Path MTU and the size specified.

`octets` — The size of the keepalive request messages in octets, expressed as a decimal integer. The `size` keyword overrides the default keepalive message size.

**Values**  
40 — 9198

### timeout

**Syntax**  
`timeout timeout`

**no timeout**

**Context**  
`config>service>sdp>keep-alive`

**Description**  
This command configures the time interval that the SDP waits before tearing down the session.

**Default**  
5

**Parameters**  
`timeout` — The timeout time, in seconds.

**Values**  
1 — 10


**ETH-CFM Configuration Commands**

**eth-cfm**

- **Syntax**: `eth-cfm`
- **Context**: `config`
- **Description**: This command enables the context to configure 802.1ag CFM parameters.

**mep**

- **Syntax**: `mep mep-id domain md-index association ma-index [vlan vlan-id]`
- **Context**: `config>port>ethernet>eth-cfm`
  - `config>lag>eth-cfm`
  - `config>router>if>eth-cfm`
- **Description**: This command provisions the maintenance endpoint (MEP).
  - The no form of the command reverts to the default values.
- **Parameters**:
  - `mep-id` — Specifies the maintenance association end point identifier.
    - **Values**: 1 — 81921
  - `md-index` — Specifies the maintenance domain (MD) index value.
    - **Values**: 1 — 4294967295
  - `ma-index` — Specifies the MA index value.
    - **Values**: 1 — 4294967295
  - `vlan-id` — Specific to tunnel facility MEPs which means this option is only applicable to the `lag>eth-cfm>context`. Used to specify the outer vlan id of the tunnel.
    - **Values**: 1 — 4094

**ais-enable**

- **Syntax**: `[no] ais-enable`
- **Context**: `config>port>ethernet>eth-cfm>mep`
  - `config>lag>eth-cfm>mep`
- **Description**: This command enables the reception of AIS messages.
  - The no form of the command reverts to the default values.
client-meg-level

Syntax  client-meg-level [[level [level ...]]]
       no client-meg-level

Context  config>port>ethernet>eth-cfm>mep>ais-enable
       config>lag>eth-cfm> mep>ais-enable

Description  This command configures the client maintenance entity group (MEG) level(s) to use for AIS message generation. Up to 7 levels can be provisioned with the restriction that the client MEG level must be higher than the local MEG level. Only the lowest client MEG level will be used for facility MEPs.

The no form of the command reverts to the default values.

Parameters  level — Specifies the client MEG level.

Values  1 — 7
Default  1

interval

Syntax  interval {1 | 60}
       no interval

Context  config>port>ethernet>eth-cfm>mep>ais-enable
       config>lag>eth-cfm> mep>ais-enable

Description  This command specifies the transmission interval of AIS messages in seconds.

The no form of the command reverts to the default values.

Parameters  1 | 60 — The transmission interval of AIS messages in seconds.

Default  1

priority

Syntax  priority priority-value
       no priority

Context  config>port>ethernet>eth-cfm>mep>ais-enable
       config>lag>eth-cfm> mep>ais-enable

Description  This command specifies the priority of the AIS messages generated by the node.

The no form of the command reverts to the default values.

Parameters  priority-value — Specify the priority value of the AIS messages originated by the node.

Values  0 — 7
Default  7
ccm-enable

Syntax  [no] ccm-enable
Context  config>port>ethernet>eth-cfm>mep
        config>lag>eth-cfm>mep
Description  This command enables the generation of CCM messages.
The no form of the command disables the generation of CCM messages.

ccm-ltm-priority

Syntax  ccm-ltm-priority priority
        no ccm-ltm-priority
Context  config>port>ethernet>eth-cfm>mep
        config>lag>eth-cfm>mep
        config>router>interface>eth-cfm>mep
Description  This command specifies the priority of the CCM and LTM messages transmitted by the MEP. Since CCM
does not apply to the Router Facility MEP only the LTM priority is of value under that context.
The no form of the command reverts to the default values.
Default  priority — Specifies the priority value
        Values  0 — 7
        Default  7

ccm-tlv-ignore

Syntax  ccm-tlv-ignore [interface-status][port-status]
        [no] ccm-tlv-ignore
Context  config>port>ethernet>eth-cfm>mep
        config>lag>eth-cfm>mep
        config>router>interface>eth-cfm>mep
Description  This command allows the receiving MEP to ignore the specified TLVs in CCM PDU. Ignored TLVs will be
reported as absent and will have no impact on the MEP state machine.
The no form of the command means the receiving MEP will process all recognized TLVs in the CCM PDU.
Default  [no] ccm-tlv-ignore
Parameters  interface-status — ignores the interface status TLV on reception.
        port-status — ignores the port status TVL on reception.
eth-test-enable

Syntax

[no] eth-test-enable

Context

config>port>ethernet>eth-cfm>mep
config>lag>eth-cfm>mep
config>router>if>eth-cfm>mep

Description

For this test to work, operators need to configure ETH-test parameters on both sender and receiver nodes. The ETH-test then can be done using the following OAM commands:

oam eth-cfm eth-test mac-address mep mep-id domain md-index association ma-index [priority priority] [data-length data-length]

The no form of the command disables eth-test capabilities.

test-pattern

Syntax

test-pattern {all-zeros | all-ones} [crc-enable]
no test-pattern

Context

config>port>ethernet>eth-cfm>mep>eth-test
config>lag>eth-cfm>mep>eth-test
config>router>if>eth-cfm>mep>eth-test

Description

This command specifies the test pattern of the ETH-TEST frames. This does not have to be configured the same on the sender and the receiver.

The no form of the command reverts to the default values.

Parameters

all-zeros — Specifies to use all zeros in the test pattern.
all-ones — Specifies to use all ones in the test pattern.
crc-enable — Generates a CRC checksum.

Default

all-zeros

low-priority-defect

Syntax

low-priority-defect {allDef | macRemErrXcon | remErrXcon | errXcon | xcon | noXcon}

Context

config>port>ethernet>eth-cfm>mep>eth-test
config>lag>eth-cfm>mep>eth-test

Description

This command specifies the lowest priority defect that is allowed to generate a fault alarm. This setting is also used to determine the fault state of the MEP which, well enabled to do so, causes a network reaction.

Default

macRemErrXcon

Values

allDef DefRDICCM, DefMACstatus, DefRemoteCCM, DefErrorCCM, and DefXconCCM
macRemErrXcon
mac-address

Syntax  

mac-address  mac-address
no mac-address

Context  
config>port>ethernet>eth-cfm>mep
config>lag>eth-cfm>mep
config>router>if>eth-cfm>mep

Description  This command specifies the MAC address of the MEP.

The no form of the command reverts to the MAC address of the MEP back to the default, that of the port, since this is SAP based.

Default  no mac-address

Parameters  
mac-address — Specifies the MAC address of the MEP.

Values  6-byte unicast mac-address (xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx) of the MEP. Using the all zeros address is equivalent to the no form of this command.

facility-fault

Syntax  

[no] facility-fault

Context  
config>lag>eth-cfm>mep
config>port>ethernet>eth-cfm>mep

Description  Allows the facility MEP to move from alarming only to network actionable function. This means a facility MEP will not merely report the defect conditions but will be able to action based on the transition of the MEP state. Without this command the facility MEP will only monitor and report and conditions of the MEP do not affect related services.

Default  no facility-fault

tunnel-fault

Syntax  

tunnel-fault  {accept | ignore}

Context  
config>service>vpls>eth-cfm
config>service>vpls>sap>eth-cfm
config>service>epipe>eth-cfm
config>service>epipe>sap>eth-cfm
config>service>ies>eth-cfm
config>service>ies>if>sap>eth-cfm
config>service>ies>sub-if>grp-if>sap>eth-cfm
config>service>vprn>eth-cfm
config>service>vprn>if>sap>eth-cfm

**Description**

Allows the individual service SAPs to react to changes in the tunnel MEP state. When tunnel-fault accept is configured at the service level, the SAP will react according to the service type. Epipe will set the operational flag and VPLS, IES and VPRN SAP operational state will become down on failure or up on clear. This command triggers the OAM mapping functions to mate SAPs and bindings in an Epipe service as well as setting the operational flag. If AIS generation is the requirement for the Epipe services this command is not required. See the ais-enable command under the config>service>epipe>sap>eth-cfm>ais-enable context for more details. This works in conjunction with the tunnel-fault accept on the individual SAPs. Both must be set to accept to react to the tunnel MEP state. By default the service level command is “ignore” and the SAP level command is “accept”. This means simply changing the service level command to “accept” will enable the feature for all SAPs. This is not required for Epipe services that only wish to generate AIS on failure.

**Parameters**

*accept* — Share fate with the facility tunnel MEP  
*ignore* — Do not share fate with the facility tunnel MEP  

**Default**

ignore (Service Level)  
accept (SAP Level for Epipe and VPLS)

domain

**Syntax**

domain md-index [format {dns | mac | none | string}] name md-name level level
domain md-index

**Context**

config>eth-cfm

**Description**

This command configures Connectivity Fault Management domain parameters. The no form of the command removes the MD index parameters from the configuration.

**Parameters**

*md-index* — Specifies the Maintenance Domain (MD) index value.  

<table>
<thead>
<tr>
<th>Values</th>
<th>1 — 4294967295</th>
</tr>
</thead>
</table>

*format {dns | mac | none | string}* — Specifies a value that represents the type (format).

| Values | dns: Specifies the DNS name format.  
|-------| X:XX:XX:XX:XX-u  
|       | X: [0..FF]h  
|       | u: [0..65535]d  
| mac:  | Specifies a Y.1731 domain format and the only format allowed to execute Y.1731 specific functions.  
| none: | Specifies an ASCII string.  
| string: | Specifies an ASCII string.  

| Default | string |
**name md-name** — Specifies a generic Maintenance Domain (MD) name.

**Values**

1 — 43 characters

**level level** — Specifies the integer identifying the maintenance domain level (MD Level). Higher numbers correspond to higher maintenance domains, those with the greatest physical reach, with the highest values for customers' CFM packets. Lower numbers correspond to lower maintenance domains, those with more limited physical reach, with the lowest values for single bridges or physical links.

**Values**

0 — 7

**association**

**Syntax**

association ma-index [format {icc-based | integer | string | vid | vpn-id}] name ma-name

no association ma-index

**Context**

config>eth-cfg>domain

**Description**

This command configures the Maintenance Association (MA) for the domain.

**ma-index** — Specifies the MA index value.

**Values**

1 — 4294967295

**format**

{icc-based | integer | string | vid | vpn-id} — Specifies a value that represents the type (format).

**Values**

<table>
<thead>
<tr>
<th>Values</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>icc-based</td>
<td>Only applicable to a Y.1731 context where the domain format is configured as none. Allows for exactly a 13 character name.</td>
</tr>
<tr>
<td>integer</td>
<td>0 — 65535 (integer value 0 means the MA is not attached to a VID.)</td>
</tr>
<tr>
<td>string</td>
<td>raw ascii</td>
</tr>
<tr>
<td>vid</td>
<td>0 — 4095</td>
</tr>
<tr>
<td>vpn-id</td>
<td>RFC-2685, Virtual Private Networks Identifier</td>
</tr>
<tr>
<td></td>
<td>xxx:xxxx, where x is a value between 00 and FF. For example 00164D:AABBCCDD</td>
</tr>
</tbody>
</table>

**Default**

integer

**name ma-name** — Specifies the part of the maintenance association identifier which is unique within the maintenance domain name.

**Values**

1 — 45 characters

**auto-mep-discovery**

**Syntax**

auto-mep-discovery

[no] auto-mep-discovery

**Context**

config>eth-cfm>domain>association

**Description**

Enable/disable the ability to auto-discover remote MEPs from a peer MEP sending ETH-CC.

**Default**

[no] auto-mep-discovery
bridge-identifier

Syntax  [no] bridge-identifier bridge-id

Context  config>eth-cfm>domain>association

Description  This command configures the service ID for the domain association. The value must be configured to match the service-id of the service where MEPs for this association will be created. Note that there is no verification that the service with a matching service-id exists. This is not used for facility MEPs as they are not tied to services.

Parameters  

bridge-id — Specifies the bridge ID for the domain association.

Values  

1 — 2147483647

mhf-creation

Syntax  mhf-creation {default | none | explicit | static}

no mhf-creation

Context  config>eth-cfm>domain>association>bridge-identifier

Description  This command determines whether to allow MIP creation for the MA. Use of the none, default and explicit parameters are only allowed for MHFs (MIPs) that are not associated with a configured Primary VLAN. The static parameter is only applicable to MHFs (MIPs) that are associated with a Primary VLAN.

Default  none

Parameters  

default — Specifies MHFs (MIPs) can be created for this SAP or Spoke-Sdp without the requirement for a MEP at some lower MA level.

none — Specifies that no MHFs (MIPs) can be created for this SAP or Spoke-SDP.

explicit — Specifies that MHFs (MIPs) can be created for this SAP or Spoke-Sdp only if a MEP is created at some lower MD Level. There must be at least one lower MD Level MEP provisioned on the same SAP or Spoke-SDP.

static — Specifies the exact level of the MHF (MIP) that will be created for this SAP. Multiple MHFs (MIPs) are allowed as long as the MD Level hierarchy is properly configured for the particular Primary VLAN. Ingress MHFs (MIPs) with primary VLAN are not supported on SDP Bindings.

mip-ltr-priority

Syntax  mip-ltr-priority priority

no mip-ltr-priority

Context  config>eth-cfm>domain>association>bridge-identifier

Description  This command allows the operator to set the priority of the Linktrace Response Message (ETH-LTR) from a MIP for this association. If this command is not specified a LTR priority of 7 will be used.

Default  no mip-ltr-priority
Parameters  

*priority* — Specifies the priority of the Linktrace Response Message (ETH-LTR) from a MIP for this association.

**Values**  
0 — 7

### vlan

**Syntax**  
```
vlan vlan-id
no vlan```

**Context**  
```
config>eth-cfm>domain>association>bridge-identifier```

**Description**  
This command configures the bridge-identifier primary VLAN ID. Note that it is informational only, and no verification is done to ensure MEPs on this association are on the configured VLAN.

**Parameters**  

*vlan-id* — Specifies a VLAN ID monitored by MA.

**Values**  
0 — 4094

### ccm-interval

**Syntax**  
```
ccm-interval interval
no ccm-interval```

**Context**  
```
config>eth-cfm>domain>association```

**Description**  
This command configures the CCM transmission interval for all MEPs in the association. The no form of the command reverts the value to the default.

**Default**  
10 seconds

**Parameters**  

*interval* — Specifies the interval between CCM transmissions to be used by all MEPs in the MA.

**Values**  
10 milliseconds, 100 milliseconds, 1 second, 10 seconds, 60 seconds, 600 seconds, 100 milliseconds

### remote-mep

**Syntax**  
```
[no] remote-mepid mep-id remote-mac {unicast-da | default}```

**Context**  
```
config>eth-cfm>domain>association```

**Description**  
This command identifies remote maintenance association endpoint (MEP) the systems is expecting to receive packets form. Optionally, the operator may configure a unciast MAC address associated with the remote-mep. This unicast value will replace the default layer two class 1 multicast address that is typically associated with ETH-CC packets.

**Note:** This command is not supported with sub second CCM intervals. *unicast-da* may only be configured when a single remote MEP exists in the association.

**Default**  
multicast class 1 address
Parameters  remote-mep  
   mep-id — Specifies the remote MEP identifier.
   
   Values  
   mep-id 1 — 8191

remote-mac  
   {unicast-da | default}
   
   Values  
   
   default — Removes the unicast address and reverts back to class 1 multicast.

remote-mepid

   Syntax  [no] remote-mepid mep-id
   
   Context  config>eth-cfm>domain>association
   
   Description  This command configures the remote maintenance association end point (MEP) identifier.
   
   Parameters  mep-id — Maintenance association end point identifier of a remote MEP whose information from the MEP database is to be returned.
   
   Values  
   1 — 8191

ccm-hold-time

   Syntax  ccm-hold-time down delay-down
   no ccm-hold-time
   
   Context  config>eth-cfm>domain>association
   
   Description  This command allows a sub second CCM enabled MEP to delay a transition to a failed state if a configured remote CCM peer has timed out. The MEP will remain in the UP state for 3.5 times CCM interval + down-delay.
   
   The no form of this command removes the additional delay
   
   Default  0 second
   
   Parameters  down — Specifies the amount of time to delay in 100ths of a second
   
   Values  
   0-1000

slm

   Syntax  slm
   
   Context  config>eth-cfm
   
   Description  This is the container that provides the global configuration parameters for ITU-T Synthetic Loss Measurement (ETH-SL).
inactivity-timer

Syntax  

inactivity-timer  timeout  

[no]  inactivity-timer

Context  

config>eth-cfm>slm

Description  

The time the responder keeps a test active. Should the time between packets exceed this values within a test the responder will mark the previous test as complete. It will treat any new packets from a peer with the same test-id, source-mac and MEP-ID as a new test responding with the sequence number one.

Default  

100 seconds

Parameters

timeout  —  Specifies the amount of time in seconds

Values  

10 100

ccm-hold-time

Syntax  

ccm-hold-time  down  delay-down  

no  ccm-hold-time

Context  

config>eth-cfm>domain>association

Description  

This command allows a sub second CCM enabled MEP to delay a transition to a failed state if a configured remote CCM peer has timed out. The MEP will remain in the UP state for 3.5 times CCM interval + down-delay.

The no form of this command removes the additional delay

Default  

0 second

Parameters

down  —  Specifies the amount of time to delay in 100ths of a second

Values  

0-1000

system

Syntax  

system

Context  

config>eth-cfm

Description  

This command configures Connectivity Fault Management General System parameters.

grace-tx-enable

Syntax  

grace-tx-enable  

[no]  grace-tx-enable

Context  

config>eth-cfm>system
ETH-CFM Configuration Commands

Description  This command enables and disables the transmission of ETH-VSM messages to delay CCM timeout and AIS churn during ISSU and soft reset functions.

Default  grace-tx-enable

redundancy

Syntax  redundancy

Context  config>eth-cfm

Description  This command provides the context under which the ETH-CFM redundancy parameters are to be configured

Default  none

mc-lag

Syntax  mc-lag

Context  config>eth-cfm>redundancy

Description  This command provides the context under which the MC-LAG specific ETH-CFM redundancy parameters are to be configured

Default  none

propagate-hold-time

Syntax  propagate-hold-time second>
       no propagate-hold-time

Context  config>eth-cfm>redundancy>mc-lag

Description  Configure the delay, in seconds, that fault propagation is delayed because of port or MC-LAG state changes. This provides the amount of time for system stabilization during a port state changes that may be protected by MC-LAG. This command requires the standby-mep-shutdown command in order to take effect.

Default  1 second

Parameters  seconds — The amount of time in seconds, zero means no delay.

Values  0-60

standby-mep-shutdown

Syntax  standby-mep-shutdown
       no standby-mep-shutdown

Context  config>eth-cfm>redundancy>mc-lag
<table>
<thead>
<tr>
<th><strong>Description</strong></th>
<th>System wide command that enables MEPs to track the state of MC-LAG. This allows MEPs on the standby MC-LAG to act administratively down.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Default</strong></td>
<td>no standby-mep-shutdown</td>
</tr>
<tr>
<td><strong>Values</strong></td>
<td>, or BCP-enabled port or sub-port0 — 11840</td>
</tr>
</tbody>
</table>
Tools Perform Commands

tools

Syntax  tools
Context  root
Description  This command enables the context to enable useful tools for debugging purposes.
Default  none
Parameters  
  - dump  — Enables dump tools for the various protocols.
  - perform  — Enables tools to perform specific tasks.

perform

Syntax  perform
Context  tools
Description  This command enables the context to enable tools to perform specific tasks.
Default  none

service

Syntax  services
Context  tools>perform
Description  This command enables the context to configure tools for services.

id

Syntax  id service-id
Context  tools>perform>service
Description  This command enables the context to configure tools for a specific service.
Parameters  
  - service-id  — Specify an existing service ID.
  Values  1 — 2147483647
## loopback

**Syntax**
loopback

**Context**
tools>perform>service>id

**Description**
Tools for placing and removing saps and SDP bindings in data loopback. Overwrite will occur for any SAP or SDP Binding when issuing a subsequent loopback command on the same SAP or SDP Binding.

**Interactions:** Loopback functions are only applicable to epipe, PBB ePipe, VPLS, I-VPLS and PBB core service contexts.

## sap

**Syntax**
sap sap-id start mode [mac-swap [mac ieee-address [all]]]
sap sap-id stop

**Context**
tools>perform>service>loopback

**Description**
This command places and removes the specific SAP in loopback mode for reflecting traffic back in the direction of the received stream. This is only applicable to Ethernet based SAPs.

**Parameters**

- **sap-id** — 
  - NULL
  - dot1q
  - QinQ
  - port-id
  - lag-id

- **start** — keyword that places the sap in loopback mode.
  - **mode ingress | egress:** keywords that specifies the location on the loopback in relation to the SAP.
  - **ingress** — Traffic arriving at the sap-ingress will be reflected back out the same sap.
  - **egress** — Traffic arriving at the sap-egress will be reflected back into the service in the direction of the original source.

- **stop** — removes the SAP from loopback mode.
mac-swap — enable source address and destination address swapping for the reflected packets when the arriving packet is unicast. Any broadcast and multicast packets arriving on a looped point will be dropped.

mac — ieee-address optionally configure the source MAC address used in the reflected packet when the arriving packet is a broadcast or multicast. This does not apply to arriving unicast packets.

Value: 6-byte unicast mac-address in the form

all — configured ieee-address is used as the source address for all reflected packets regardless of the arriving destination.

Default [no] mac-swap — no swapping of mac addresses are performed without specifying this option and any non-unicast destined packets will not be reflected back to the source.

sdp

Syntax sdp sdp-id:vc-id start mode [mac-swap [mac ieee-address [all]]]
sdp sdp-id:vc-id stop

Context tools>perform>service>loopback

Description This command places the specific MPLS SDP binding in loopback mode for reflecting traffic back in the direction of the received stream. This is only applicable to MPLS SDP Bindings.

Parameters sdp-id:vc-id — sdp-id [1..17407]
vc-id [1..4294967295]

start — keyword that places the sap in loopback mode.

mode ingress | egress: keywords that specifies the location on the loopback in relation to the MPLS SDP Binding.

ingress — Traffic arriving at the sap-ingress will be reflected back out the same sap.

egress — Traffic arriving at the sap-egress will be reflected back into the service in the direction of the original source.

stop — rkeyword that removes the MPLS SD- binding from loopback mode.

mac-swap — enable source address and destination address swapping for the reflected packets when the arriving packet is unicast. Any broadcast and multicast packets arriving on a looped point will be dropped.

mac — ieee-address optionally configure the source MAC address used in the reflected packet when the arriving packet is a broadcast or multicast. This does not apply to arriving unicast packets.

Value: 6-byte unicast mac-address in the form

all — configured ieee-address is used as the source address for all reflected packets regardless of the arriving destination.

Default [no] mac-swap — no swapping of mac addresses are performed without specifying this option and any non-unicast destined packets will not be reflected back to the source.
In This Chapter

This section provides information about Virtual Leased Line (VLL) services and implementation notes.

Topics in this section include:

- Ethernet Pipe (Epipe) Services on page 246
- Pseudowire Switching on page 259
- Pseudowire Redundancy on page 267
- Dynamic Multi-Segment Pseudowire Routing on page 268
- Epipe Using BGP-MH Site Support for Ethernet Tunnels on page 296
- BGP Virtual Private Wire Service (VPWS) on page 323
Ethernet Pipe (Epipe) Services

This section provides information about the Epipe service and implementation notes.

Topics in this section include:

- **Epipe Service Overview** on page 247
  - SAP Encapsulations and Pseudowire Types on page 336
  - QoS Policies on page 337
  - Filter Policies on page 337
  - MAC Resources on page 337
- **Basic Configurations** on page 340
- **Common Configuration Tasks** on page 340
  - Configuring VLL Components on page 341
    - Creating an Epipe Service on page 342
- **Service Management Tasks** on page 369
Epipe Service Overview

An Epipe service is Alcatel-Lucent’s implementations of an Ethernet VLL based on the IETF “Martini Drafts” (draft-martini-l2circuit-trans-mpls-08.txt and draft-martini-l2circuit-encapmpls-04.txt) and the IETF Ethernet Pseudo-wire Draft (draft-so-pwe3-ethernet-00.txt).

An Epipe service is a Layer 2 point-to-point service where the customer data is encapsulated and transported across a service provider’s IP, MPLS or PBB VPLS network. An Epipe service is completely transparent to the customer’s data and protocols. The SR-OS Epipe service does not perform any MAC learning. A local Epipe service consists of two SAPs on the same node, whereas a distributed Epipe service consists of two SAPs on different nodes. SDPs are not used in local Epipe services.

Each SAP configuration includes a specific port/channel on which service traffic enters the SR-OS from the customer side (also called the access side). Each port is configured with an encapsulation type. If a port is configured with an IEEE 802.1Q (referred to as Dot1q) encapsulation, then a unique encapsulation value (ID) must be specified.

![Figure 30: Epipe/VLL Service](image)
Epipe Up Operational State Configuration Option

By default, the operational state of the Epipe is tied to the state of the two connections that comprise the Epipe. If either of the connections in the Epipe are operationally down, the Epipe service that contains that connection will also be operationally down. The operator does have the ability to configure a single SAP within an Epipe not to affect the operational state of that Epipe using the optional command `ignore-oper-state`. Within an Epipe, if a SAP that includes this optional command becomes operationally down state, the operational state of the Epipe will not transition to down. The operational state of the Epipe will remain up. This does not change the fact that the SAP is down and no traffic will transit an operationally down SAP. Removing and adding this command on the fly will evaluate the service's operational state based on the SAPs and the addition or deletion of this command.

Service OAM (SOAM) designers may consider using this command if an UP MEP configured on the operationally down SAP within an Epipe is required to receive and process SOAM PDUs. When a service is operationally down, this is not possible. For SOAM PDUs to continue to arrive on an UP, MEP configured on the failed SAP the service must be operationally up. Consider the case where an UP MEP is placed on a UNI-N or E-NNI and the UNI-C on E-NNI peer is shutdown in such a way that it causes the SAP to enter an operational state Down.

Two connections must be configured within the Epipe, otherwise, the service will be operationally down regardless of this command. The `ignore-oper-state` functionality will only operate as intended when the Epipe has one ingress and one egress. This command is not to be used for Epipe services with redundant connections that provide alternate forwarding in case of failure, even though the CLI does not prevent this configuration.

Support is available on Ethernet SAPs configured on ports or Ethernet SAPs configured on LAG. However, it is not allowed on SAPs using LAG profiles or if the SAP is configured on a LAG which has no ports.
Epipe with PBB

A pbb-tunnel may be linked to an Epipe to a B-VPLS. MAC switching and learning is not required for the point-to-point service (all packets ingressing the SAP are PBB encapsulated and forwarded to the PBB tunnel to the backbone destination MAC address and all the packets ingressing the B-VPLS destined for the ISID are PBB de-encapsulated and forwarded to the Epipe SAP. A fully specified backbone destination address must be provisioned for each PBB Epipe instance to be used for each incoming frame on the related I-SAP. If the backbone destination address is not found in the B-VPLS FDB then packets may be flooded through the B-VPLSs.

All B-VPLS constructs may be used including B-VPLS resiliency and OAM. Not all generic Epipe commands are applicable when using a PBB tunnel.
Epipe over L2TPv3

L2TPv3 feature provides a framework to support transporting Ethernet pseudowire services over an IPv6-only network without MPLS. This architecture relies on the abundance of address space in the IPv6 protocol to provide unique far-end and local-end addressing that uniquely identify each tunnel and service binding.

This feature allows for multiple EPIPES to be transported (up to 16K per system) by binding multiple IPv6 addresses to each node and configuring one SDP per Epipe.

As the IPv6 addressing uniqueness identifies the customer and service binding, the L2TPv3 control plane is disabled in this mode.

ETH-CFM is supported for OAM services.

Figure 31: L2TPv3 SDP Illustration
A PE does not flush the ARP cache unless the SAP goes administratively or operationally down. The PE with the Ethernet SAP sends unsolicited ARP requests to refresh the ARP cache every $T$ seconds. ARP requests are staggered at an increasing rate if no reply is received to the first unsolicited ARP request. The value of $T$ is configurable by user through the `mac-refresh` CLI command.
Extension to IP VLL for Discovery of Ethernet CE IP Address

VLL services provide IP connectivity between a host attached to a point to point access circuit (FR, ATM, PPP) with routed PDU encapsulation and a host attached to an Ethernet interface. Both hosts appear to be on the same IP interface. This feature is supported only for IPv4 payload.

In deployments where it is not practical for operators to obtain and configure their customer CE address, the following behaviors apply:

- A service comes up without prior configuration of the CE address parameter under both the SAP and the spoke SDP.
- Rely solely on received ARP messages from the Ethernet SAP attached CE device to update the ARP cache with no further check of the validity of the source IP address of the ARP request message and the IP address ARPed for.
- The LDP address list TLV to signal the learned CE IP address to the remote PE is supported. This is to allow the PE with the FR SAP to respond to an invFR ARP request message received from the FR attached CE device. Only Ethernet SAP and FR SAP can learn the CE address through ARP and invFR ARP respectively.

VLL Ethernet SAP Procedures

The operator can enable the following CE address discovery procedures by configuring the `ce-address-discovery` in the `config>service>ipipe` context.

- The service is brought up without the CE address parameter configured at either the SAP or the spoke SDP.
- The operator cannot configure the `ce-address` parameter under the `config>service>ipipe>sap` or `config>service>ipipe>spoke-sdp` context when the `ce-address-discovery` in the `config>service>ipipe` context is enabled. Conversely, the operator is not allowed to enable the `ce-address-discovery` option under the Ipipe service if it has a SAP and/or spoke SDP with a user-entered `ce-address` parameter.
- While an ARP cache is empty, the PE does not forward unicast IP packets over the Ethernet SAP but forwards multicast/broadcast packets.
- The PE waits for an ARP request from the CE to learn both IP and MAC addresses of the CE. Both entries are added into the ARP cache. The PE accepts any ARP request message received over Ethernet SAP and updates the ARP cache IP and MAC entries with no further check of the source IP address of the ARP request message or of the IP address being ARPed.
- The 7950 SR will always reply to a received ARP request message from the Ethernet SAP with the SAP MAC address and a source IP address of the IP address being ARPed without any further check of the latter.
• If the router received an address list TLV from the remote PE node with a valid IP address of the CE attached to the remote PE, it not checks it against the IP address being ARPed for when replying to an ARP request over the Ethernet SAP.

• The ARP cache is flushed when the SAP bounces or when the operator manually clears the ARP cache. This results in the clearing of the CE address discovered on this SAP. However, when the SAP comes up initially or comes back up from a failure, an unsolicited ARP request is not sent over the Ethernet SAP.

• If the Ipipe service makes use of a spoke SDP, the router includes the address list TLV in the interface parameters field of the pseudowire FEC TLV in the label mapping message. The address list TLV contains the current value of the CE address in the ARP cache. If no address was learned, then an address value of 0.0.0.0 must be used.

• If the remote PE included the address list TLV in the received label mapping message, the local updates the remote PE node with the most current IP address of the Ethernet CE using a T-LDP notification message with status TLV status code is set to 0x0000002C and containing an LDP address list. The notification message is sent each time an IP address different from the current value in the ARP cache is learned. This includes when the ARP is flushed and the CE address is reset to the value of 0.0.0.0.

• If the remote PE did not include the address list TLV in the received label mapping message, the local router will not send any notification messages containing the address list TLV during the lifetime of the IP pseudowire.

• If the operator disables the ce-address-discovery option under the VLL service, service manager instructs LDP to withdraw the service label and the service is shutdown. The pseudowire labels will only be signaled and the service will come up if the operator re-enters the option again or enters manually the ce-address parameter under SAP and spoke SDP.
IPv6 Support on IP Interworking VLL

The 7950 SR supports both the transport of IPv6 packets and the interworking of IPv6 Neighbor discovery/solicitation messages on an IP Interworking VLL. IPv6 capability is enabled on an Ipipe using the `ce-address-discovery ipv6` command in the CLI.

IPv6 Datapath Operation

The IPv6 uses ICMPv6 extensions to automatically resolve IP address and link address associations. These are IP packets, as compared to ARP and invARP in IPv4, which are separate protocols and not based on IP packets. Manual configuration of IPv6 addresses is not supported on the IP Interworking VLL.

Each 7x50 PE device intercepts ICMPv6 Neighbor Discovery (RFC 2461) packets, whether received over the SAP or over the pseudowire, inspects them to learn IPv6 interface addresses and CE link-layer addresses, and modifies these packets as required according to the SAP type, and then forwards them towards the original destination. The 7x50 PE is also capable of generating packets to interwork between CEs by using IPv6 Neighbor Discovery, and CEs that use other neighbor discovery protocols to bring up the link, for example, IPv6CP for PPP.

The 7x50 PE device learns the IPv6 interface addresses for its directly-attached CE and another IPv6 interface addresses for the far-end CE. The 7x50 PE device also learns the link-layer address of the local CE and uses it when forwarding traffic between the local and far-end CEs. As with IPv4, the SAP accepts both unicast and multicast packets. For unicast packets, the 7x50 PE checks that the MAC address/IP addresses are consistent with that in the ARP cache before forwarding; otherwise the packet is silently discarded. Multicast packets are validated and forwarded. If more than one IP address is received per MAC address in a neighbor discovery packet, or if multiple neighbor discovery packets are received for a given MAC address, the currently cached address is overwritten with the most recent value.

**Figure 33** illustrates the data path operation for IPv6 on an IP Interworking VLL between the Ethernet and PPP (IPv6CP) SAPs.
With reference to neighbor discovery between Ethernet and PPP CEs in Figure 33, the steps are as follows:

1. Ethernet attached CE2 sends a Neighbor Solicitation message towards PE2 in order to begin the neighbor discovery process.
2. PE2 snoops this message, and the MAC address and IP address of CE2 is stored in the ARP cache of PE2 before forwarding the Neighbor Solicitation on the IP pseudowire to PE1.
3. PE1 snoops this message that arrives on the IP pseudowire and stores the IP address of the remote CE2. Since CE3 is attached to a PPP SAP, which uses IPv6CP to bring up the link, PE1 generates a neighbor advertisement message and sends it on the ipipe towards PE2.
4. PE2 receives the neighbor advertisement on the ipipe from PE1. It must replace the layer 2 address in the neighbor advertisement message with the MAC address of the SAP before forwarding to CE2.
IPv6 Stack Capability Signaling

The 7x50 supports IPv6 capability negotiation between PEs at the ends of an IP interworking VLL. Stack capability negotiation is performed if stack-capability-signaling is enabled in the CLI. Stack capability negotiation is disabled by default. In which case, it must be assumed that the remote PE supports both IPv4 and IPv6 transport over an ipipe.

A 'stack capability' sub-TLV is signaled by the two 7x50 PEs using T-LDP so that they can agree on which stacks they should be using.

By default, the IP pseudowire will always be capable of carrying IPv4 packets. Thus this capability sub-TLV is used to indicate if other stacks need to be supported concurrently with IPv4.

The stack capability sub-TLV is a part of the interface parameters of the pseudowire FEC. This means any change to the stack support requires that the pseudowire be torn down and re-signaled.

A PE that supports IPv6 on an IP pseudowire must signal the stack capability sub-TLV in the initial label mapping message for the pseudowire. For the 7x50, this means that the stack capability sub-TLV must be included if both the stack-capability-signaling and ce-address-discovery ipv6 options are enabled under the VLL service.

In this release, if one PE of an IP interworking VLL supports IPv6, while the far end-PE does not support IPv6 (or ce-address-discovery ipv6 is disabled), the pseudowire does not come up.

If a 7x50 PE that supports IPv6 (that is, stack-capability-signaling ipv6 is enabled) has already sent an initial label mapping message for the pseudowire, but does not receive a ‘stack capability’ sub-TLV from the far-end PE in the initial label mapping message, or one is received but it is set to a reserved value, then the PE assumes that a configuration error has occurred. That is, if the remote PE did not include the capability sub-TLV in the received Label Mapping message, or it does include the sub-TLV but with the IPv6 bit cleared, and if stack-capability-signaling is enabled, the local 7x50 with ce-address-discovery ipv6 enabled withdraws its pseudowire label with the LDP status code “IP Address type mismatch”.

If a 7x50 PE that supports IPv6 (that is, stack-capability-signaling ipv6 is enabled) has not yet sent a label mapping message for the pseudowire and does not receive a ‘stack capability’ sub-TLV from the far-end PE in the initial label mapping message, or one is received but it is set to a reserved value, the PE assumes that a configuration error has occurred and does not send a label mapping message of its own.

If the IPv6 stack is not supported by both PEs, or at least one of the PEs does support IPv6 but does not have the ce-address-discovery ipv6 option selected in the CLI, IPv6 packets received from the AC are discarded by the PE. IPv4 packets are always supported.

If IPv6 stack support is implemented by both PEs, but the ce-address-discovery ipv6 command was not enabled on both so that the IP pseudowire came up with only IPv4 support, and one PE is later toggled to ce-address-discovery ipv6, then that PE sends a label withdraw with the LDP status code meaning “Wrong IP Address Type” (Status Code 0x0000004B9).
If the IPv6 stack is supported by both PEs, and therefore the pseudowire is established with IPv6 capability at both PEs, but the `ce-address-discovery ipv6` command on one PE is later toggled to `no ce-address-discovery ipv6` so that a PE ceases to support the IPv6 stack, then that PE sends a label withdraw with the LDP status code meaning “Wrong IP Address Type”.
for spoke-sdps configured for spoke-sdps with statically assigned labels (and the SDP has signaling off) and MPLS-TP identifiers:
Pseudowire Switching

The pseudowire switching feature provides the user with the ability to create a VLL service by cross-connecting two spoke SDPs. This feature allows the scaling of VLL and VPLS services in a large network in which the otherwise full mesh of PE devices would require thousands of Targeted LDP (T-LDP) sessions per PE node.

Services with one SAP and one spoke SDP are created normally on the PE; however, the target destination of the SDP is the pseudowire switching node instead of what is normally the remote PE. In addition, the user configures a VLL service on the pseudowire switching node using the two SDPs.

The pseudowire switching node acts in a passive role with respect to signalling of the pseudowires. It waits until one or both of the PEs sends the label mapping message before relaying it to the other PE. This is because it needs to pass the Interface Parameters of each PE to the other.

A pseudowire switching point TLV is inserted by the switching pseudowire to record its system address when relaying the label mapping message. This TLV is useful in a few situations:

- It allows for troubleshooting of the path of the pseudowire especially if multiple pseudowire switching points exist between the two PEs.
- It helps in loop detection of the T-LDP signalling messages where a switching point would receive back a label mapping message it had already relayed.
- The switching point TLV is inserted in pseudowire status notification messages when they are sent end-to-end or from a pseudowire switching node towards a destination PE.

Pseudowire OAM is supported for the manual switching pseudowires and allows the pseudowire switching node to relay end-to-end pseudowire status notification messages between the two PEs. The pseudowire switching node can generate a pseudowire status and to send it to one or both of the PEs by including its system address in the pseudowire switching point TLV. This allows a PE to identify the origin of the pseudowire status notification message.

In the Figure 34, the user configures a regular Epipe VLL service PE1 and PE2. These services consist each of a SAP and a spoke SPD. However, the target destination of the SDP is actually not the remote PE but the pseudowire switching node. In addition, the user configures an Epipe VLL service on the pseudowire switching node using the two SDPs.

| 7950 SR PE1 (Epipe) | ---sdp 2:10--- | 7950 SR PW SW (Epipe) | ---sdp 7:15--- | 7950 SR PE2 (Epipe) |

Figure 34: Pseudowire Service Switching Node

Configuration examples can be found in Configuring Two VLL Paths Terminating on T-PE2 on page 355.
Pseudowire Switching with Protection

Pseudowire switching scales VLL and VPLS services over a multi-area network by removing the need for a full mesh of targeted LDP sessions between PE nodes. Figure 35 illustrates the use of pseudowire redundancy to provide a scalable and resilient VLL service across multiple IGP areas in a provider network.

In the network in Figure 35, PE nodes act as masters and pseudowire switching nodes act as slaves for the purpose of pseudowire signaling. A switching node will need to pass the SAP Interface Parameters of each PE to the other. T-PE1 sends a label mapping message for the Layer 2 FEC to the peer pseudowire switching node” for example, S-PE1. It will include the SAP interface parameters, such as MTU, in the label mapping message. S-PE1 checks the FEC against the local information and if a match exists, it appends the optional pseudowire switching point TLV to the FEC TLV in which it records its system address. T-PE1 then relays the label mapping message to S-PE2. S-PE2 performs similar operations and forwards a label mapping message to T-PE2. The same procedures are followed for the label mapping message in the reverse direction, for example, from T-PE2 to T-PE1. S-PE1 and S-PE2 will effect the spoke SDP cross-connect only when both directions of the pseudowire have been signaled and matched.
The pseudowire switching TLV is useful in a few situations. First, it allows for troubleshooting of the path of the pseudowire especially if multiple pseudowire switching points exist between the two T-PE nodes. Secondly, it helps in loop detection of the T-LDP signaling messages where a switching point receives back a label mapping message it already relayed. Finally, it can be inserted in pseudowire status messages when they are sent from a pseudowire switching node towards a destination PE.

Pseudowire status messages can be generated by the T-PE nodes and/or the S-PE nodes. Pseudowire status messages received by a switching node are processed and then passed on to the next hop. An S-PE node appends the optional pseudowire switching TLV, with its system address added to it, to the FEC in the pseudowire status notification message only if it originated the message or the message was received with the TLV in it. Otherwise, it means the message was originated by a T-PE node and the S-PE should process and pass the message without changes except for the VCID value in the FEC TLV.
Pseudowire Switching Behavior

In the network in Figure 35, PE nodes act as masters and pseudowire switching nodes act as slaves for the purpose of pseudowire signaling. This is because a switching node will need to pass the SAP interface parameters of each PE to the other. T-PE1 sends a label mapping message for the Layer 2 FEC to the peer pseudowire switching node, for example, S-PE1. It will include the SAP interface parameters, such as MTU, in the label mapping message. S-PE1 checks the FEC against the local information and if a match exists, it appends the optional pseudowire switching point TLV to the FEC TLV in which it records its system address. T-PE1 then relays the label mapping message to S-PE2. S-PE2 performs similar operation and forwards a label mapping message to T-PE2. The same procedures are followed for the label mapping message in the reverse direction, for example, from T-PE2 to T-PE1. S-PE1 and S-PE2 will effect the spoke SDP cross-connect only when both directions of the pseudowire have been signaled and matched.

Pseudowire status notification messages can be generated by the T-PE nodes and/or the S-PE nodes. Pseudowire status notification messages received by a switching node are processed and then passed on to the next hop. An S-PE node appends the optional pseudowire switching TLV, with its system address added to it, to the FEC in the pseudowire status notification message only if it originated the message or the message was received with the TLV in it. Otherwise, it means the message was originated by a T-PE node and the S-PE should process and pass the message without changes except for the VC ID value in the FEC TLV.

The merging of the received T-LDP status notification message and the local status for the spoke SDPs from the service manager at a PE complies with the following rules:

- When the local status for both spokes is up, the S-PE passes any received SAP or SDP-binding generated status notification message unchanged, for example, the status notification TLV is unchanged but the VC-ID in the FEC TLV is set to value of the pseudowire segment to the next hop.
- When the local operational status for any of the spokes is down, the S-PE always sends SDP-binding down status bits regardless if the received status bits from the remote node indicated SAP up/down or SDP-binding up/down.
Pseudowire Switching TLV

The format of the pseudowire switching TLV is as follows:

```
+-------+-------+-------+-------+
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-------+-------+-------+-------+
|1|0|     pw sw TLV (0x096D) |     pseudowire sw TLV Length |
+-------+-------+-------+-------+
|     Type      |    Length     |    Variable Length Value      |
+-------+-------+-------+-------+
|                         Variable Length Value                 |
|                             "                                 |
+-------+-------+-------+-------+
PW sw TLV Length — Specifies the total length of all the following pseudowire switching point TLV fields in octets

Type — Encodes how the Value field is to be interpreted.

Length — Specifies the length of the Value field in octets.

Value — Octet string of Length octets that encodes information to be interpreted as specified by the Type field.

Pseudowire Switching Point Sub-TLVs

Below are details specific to pseudowire switching point sub-TLVs:

pseudowire ID of last pseudowire segment traversed — This sub-TLV type contains a pseudowire ID in the format of the pseudowire ID

Pseudowire switching point description string — An optional description string of text up to 80 characters long.

IP address of pseudowire switching point.

The IP V4 or V6 address of the pseudowire switching point. This is an optional sub-TLV.

MH VCCV capability indication.
Static-to-Dynamic Pseudowire Switching

When one segment of the pseudowire cross-connect at the S-PE is static while the other is signaled using T-LDP, the S-PE operates much like a T-PE from a signaling perspective and as an S-PE from a data plane perspective.

The S-PE signals a label mapping message as soon as the local configuration is complete. The control word C-bit field in the pseudowire FEC is set to the value configured on the static spok-sdp.

When the label mapping for the egress direction is also received from the T-LDP peer, and the information in the FEC matches that of the local configuration, the static-to-dynamic cross-connect is effected.

Note that it is possible that end nodes of a static pseudowire segment be misconfigured. In this case, an S-PE or T-PE node may be receiving packets with the wrong encapsulation. In this case, it is possible that an invalid payload will be forwarded over the pseudowire or the SAP respectively. Furthermore, if the S-PE or T-PE node is expecting the control word in the packet encapsulation and the received packet comes with no control word but the first nibble below the label stack is 0x0001, the packet may be mistaken for a VCCV OAM packet and may be forwarded to the CPM. In that case, the CPM will perform a check of the IP header fields such as version, IP header length, and checksum. If any of this fails the VCCV packet will be discarded.
Ingress VLAN Swapping

This feature is supported on VPLS and VLL services where the end to end solution is built using two node solutions (requiring SDP connections between the nodes).

In VLAN swapping, only the VLAN-id value is copied to the inner VLAN position. The Ethertype of the inner tag will be preserved and all consecutive nodes will work with that value. Similarly, the dot1p bits value of outer-tag will not be preserved.

![Figure 36: Ingress VLAN Swapping](image)

The network diagram in Figure 36 describes the network where at user access side (DSLAM facing SAPs) every subscriber is represented by several QinQ SAPs with inner-tag encoding service and outer-tag encoding subscriber (DSL line). The aggregation side (BRAS or PE facing SAPs) the is represented by DSL line number (inner VLAN tag) and DSLAM (outer VLAN tag). The effective operation on VLAN tag is to “drop inner tag at access side and push another tag at the aggregation side”.

Ingress VLAN Translation

The drawing in Figure 37 indicates an application where different circuits are aggregated in the VPLS-based network. The access side is represented by an explicit dot1q encapsulated SAP. As the VLAN-id is port specific, those connected to different ports might have the same VLAN. The aggregation side (the right side Figure 37) is aggregated on the same port, and hence, unique a VLAN-id is required.
Pseudowire Redundancy

Pseudowire redundancy provides the ability to protect a pseudowire with a pre-provisioned pseudowire and to switch traffic over to the secondary standby pseudowire in case of a SAP and/or network failure condition. Normally, pseudowires are redundant by the virtue of the SDP redundancy mechanism. For instance, if the SDP is an RSVP LSP and is protected by a secondary standby path and/or by Fast-Reroute paths, the pseudowire is also protected. However, there are a couple of applications in which SDP redundancy does not protect the end-to-end pseudowire path:

- There are two different destination PE nodes for the same VLL service. The main use case is the provision of dual-homing of a CPE or access node to two PE nodes located in different POPs. The other use case is the provision of a pair of active and standby BRAS nodes, or active and standby links to the same BRAS node, to provide service resiliency to broadband service subscribers.
- The pseudowire path is switched in the middle of the network and the SR-Series pseudowire switching node fails.

Pseudowire and VPLS link redundancy extends link-level resiliency for pseudowires and VPLS to protect critical network paths against physical link or node failures. These innovations enable the virtualization of redundant paths across the metro or core IP network to provide seamless and transparent fail-over for point-to-point and multi-point connections and services. When deployed with multi-chassis LAG, the path for return traffic is maintained through the pseudowire or VPLS switchover, which enables carriers to deliver “always on” services across their IP/MPLS networks.
Dynamic Multi-Segment Pseudowire Routing

Overview

Dynamic Multi-Segment Pseudowire Routing (Dynamic MS-PWs) enable a complete multi-segment pseudowire to be established, while only requiring per-pseudowire configuration on the T-PEs. No per-pseudowire configuration is required on the S-PEs. End-to-end signaling of the MS-PW is achieved using T-LDP, while multi-protocol BGP is used to advertise the T-PEs, so allowing dynamic routing of the MS-PW through the intervening network of S-PEs. Dynamic multi-segment pseudowires are described in the IETF in draft-ietf-pwe3-dynamic-ms-pw-13.txt.

Figure 38 illustrates the operation of dynamic MS-PWs.

![Figure 38: Dynamic MS-PW Overview](image-url)
The FEC 129 AII Type 2 structure depicted in Figure 39 is used to identify each individual pseudowire endpoint:

![Figure 39: Figure 2 MS-PW Addressing using FEC129 All Type 2](image)

A 4-byte global ID followed by a 4 byte prefix and a 4 byte attachment circuit ID are used to provide for hierarchical, independent allocation of addresses on a per service provider network basis. The first 8 bytes (Global ID + Prefix) may be used to identify each individual T-PE or S-PE as a loopback Layer 2 Address.

This new AII type is mapped into the MS-PW BGP NLRI (a new BGP AFI of L2VPN, and SAFI for network layer reachability information for dynamic MS-PWs. As soon as a new T-PE is configured with a local prefix address of global id:prefix, pseudowire routing will proceed to advertise this new address to all the other T-PEs and S-PEs in the network, as depicted in Figure 40:
In step 1 a new T-PE (T-PE2) is configured with a local prefix.

Next, in steps 2-5, MP-BGP will use the NLRI for the MS-PW routing SAFI to advertise the location of the new T-PE to all the other PEs in the network. Alternatively, static routes may be configured on a per T-PE/S-PE basis to accommodate non-BGP PEs in the solution.

As a result, pseudowire routing tables for all the S-PEs and remote T-PEs are populated with the next hop to be used to reach T-PE2.

VLL services can then be established, as illustrated in Figure 41.

Figure 40: Advertisement of PE Addresses by PW Routing
In step 1 and 1' the T-PEs are configured with the local and remote endpoint information, Source All (SAll), Target All (TAll). On the 7x50, the Alls are locally configured for each spoke SDP, according to the model shown in Figure 42. The 7x50 therefore provides for a flexible mapping of All to SAP. That is, the values used for the All are through local configuration, and it is the context of the spoke SDP that binds it to a specific SAP.

**Figure 41: Signaling of Dynamic MS-PWs using T-LDP**

**Figure 42: Mapping of All to SAP**
Before T-LDP signaling starts, the two T-PEs decide on an active and passive relationship using the highest AII (comparing the configured SAII and TAII) or the configured precedence. Next, the active T-PE (in the IETF draft this is referred to as the source T-PE or ST-PE) checks the PW Routing Table to determine the next signaling hop for the configured TAII using the longest match between the TAII and the entries in the PW routing table.

This signaling hop is then used to choose the T-LDP session to the chosen next-hop S-PE. Signaling proceeds through each subsequent S-PE using similar matching procedures to determine the next signaling hop. Otherwise, if a subsequent S-PE does not support dynamic MS-PW routing and thus uses a statically configured PW segment, the signaling of individual segments follows the procedures already implemented in the PW Switching feature. Note that BGP can install a PW AII route in the PW routing table with ECMP next-hops. However when LDP needs to signal a PW with matching TAII, it will choose only one next-hop from the available ECMP next-hops. PW routing supports up to 4 ECMP paths for each destination.

The signaling of the forward path ends once the PE matches the TAII in the label mapping message with the SAII of a spoke SDP bound to a local SAP. The signaling in the reverse direction can now be initiated, which follows the entries installed in the forward path. The PW Routing tables are not consulted for the reverse path. This ensures that the reverse direction of the PW follows exactly the same set of S-PEs as the forward direction.

This solution can be used in either a MAN-WAN environment or in an Inter-AS/Inter-Provider environment as depicted in Figure 43.

![Figure 43: VLL Using Dynamic MS-PWs, Inter-AS Scenario](image)

Note that data plane forwarding at the S-PEs uses pseudowire service label switching, as per the pseudowire switching feature.
Pseudowire Routing

Each S-PE and T-PE has a pseudowire routing table that contains a reference to the T-LDP session to use to signal to a set of next hop S-PEs to reach a given T-PE (or the T-PE if that is the next hop). For VLLs, this table contains aggregated AII Type 2 FECs and may be populated with routes that are learned through MP-BGP or that are statically configured.

MP-BGP is used to automatically distribute T-PE prefixes using the new MS-PW NLRI, or static routes can be used. The MS-PW NLRI is composed of a Length, an 8-byte RD, a 4-byte Global-ID, a 4-byte local prefix, and (optionally) a 4-byte AC-ID. Support for the MS-PW address family is configured in CLI under `config>router>bgp>family ms-pw`.

MS-PW routing parameters are configured in the `config>service>pw-routing` context.

In order to enable support for dynamic MS-PWs on a 7x50 node to be used as a T-PE or S-PE, a single, globally unique, S-PE ID, known as the S-PE Address, is first configured under `config>service>pw-routing` on each 7x50 to be used as a T-PE or S-PE. The S-PE Address has the format global-id:prefix. It is not possible to configure any local prefixes used for pseudowire routing or to configure spoke SPDs using dynamic MS-PWs at a T-PE unless an S-PE address has already been configured. The S-PE address is used as the address of a node used to populate the switching point TLV in the LDP label mapping message and the pseudowire status notification sent for faults at an S-PE.

Each T-PE is also be configured with the following parameters:

- a. Global ID — This is a 4 byte identifier that uniquely identifies an operator or the local network.
- b. Local Prefix — One or more local (Layer 2) prefixes (up to a maximum of 16), which are formatted in the style of a 4-octet IPv4 address. A local prefix identifies a T-PE or S-PE in the PW routing domain.
- c. For each local prefix, at least one 8-byte route distinguisher can be configured. It is also possible to configure an optional BGP community attribute.

For each local prefix, BGP then advertises each global ID/prefix tuple and unique RD and community pseudowire using the MS-PW NLRI, based on the aggregated FEC129 AII Type 2 and the Layer 2 VPN/PW routing AFI/SAFI 25/6, to each T-PE/S-PE that is a T-LDP neighbor, subject to local BGP policies.

The dynamic advertisement of each of these pseudowire routes is enabled for each prefix and RD using the `advertise-bgp` command.

An export policy is also required in order to export MS-PW routes in MP-BGP. This can be done using a default policy, such as the following:
However, this would export all routes. A recommended choice is to enable filtering per-family, as follows:

```
*A:lin-123>config>router>policy-options# info
----------------------------------------------
policy-statement "to-mspw"
    entry 1
        from
        family ms-pw
        exit
        action accept
        exit
    exit
----------------------------------------------
```

The following command is then added in the `config>router>bgp` context.

```
export "to-mspw"
```

Local-preference for iBGP and BGP communities can be configured under such a policy.
**Static Routing**

In addition to support for BGP routing, static MS-PW routes may also be configured using the `config>services>pw-routing>static-route` command. Each static route comprises the target T-PE Global-ID and prefix, and the IP address of the T-LDP session to the next hop S-PE or T-PE that should be used.

If a static route is set to 0, then this represents the default route. If a static route exists to a given T-PE, then this is used in preference to any BGP route that may exist.

**Explicit Paths**

A set of default explicit routes to a remote T-PE or S-PE prefix may be configured on a T-PE under `config>services>pw-routing` using the `path name` command. Explicit paths are used to populate the explicit route TLV used by MS-PW T-LDP signaling. Only strict (fully qualified) explicit paths are supported.

Note that it is possible to configure explicit paths independently of the configuration of BGP or static routing.
Configuring VLLs using Dynamic MS-PWs

One or more spoke SDPs may be configured for distributed Epipe VLL services. Dynamic MS-PWs use FEC129 (also known as the Generalized ID FEC) with Attachment Individual Identifier (AII) Type 2 to identify the pseudowire, as opposed to FEC128 (also known as the PW ID FEC) used for traditional single segment pseudowires and for pseudowire switching. FEC129 spoke SDPs are configured under the `spoke-sdp-fec` command in the CLI.

FEC129 AII Type 2 uses a Source Attachment Individual Identifier (SAII) and a Target Attachment Individual Identifier (TAII) to identify the end of a pseudowire at the T-PE. The SAII identifies the local end, while the TAII identifies the remote end. The SAII and TAII are each structured as follows:

- **Global-ID** — This is a 4 byte identifier that uniquely identifies an operator or the local network.
- **Prefix** — A 4-byte prefix, which should correspond to one of the local prefixes assigned under `pw-routing`.
- **AC-ID** — A 4-byte identifier for this end of the pseudowire. This should be locally unique within the scope of the `global-id:prefix`.


Active/Passive T-PE Selection

Dynamic MS-PWs use single-sided signaling procedures with double-sided configuration, a fully qualified FEC must be configured at both endpoints. That is, one T-PE (the source T-PE, ST-PE) of the MS-PW initiates signaling for the MS-PW, while the other end (the terminating T-PE, TT-PE) passively waits for the label mapping message from the far-end and only responds with a label mapping message to set up the opposite direction of the MS-PW when it receives the label mapping from the ST-PE. By default, the 7x50 will determine which T-PE is the ST-PE (the active T-PE) and which is the TT-PE (the passive T-PE) automatically, based on comparing the SAII with the TAI. The T-PE with SAII>TAII assumes the active role. However, it is possible to override this behavior using the signaling \{master | auto\} command under the spoke-sdp-fec. If master is selected at a given T-PE, then it will assume the active role. If a T-PE is at the endpoint of a spoke SDP that is bound to an VLL SAP and single sided auto-configuration is used (see below), then that endpoint is always passive. Therefore, signaling master should only be used when it is known that the far end will assume a passive behavior.

Automatic Endpoint Configuration

Automatic endpoint configuration allows the configuration of an endpoint without specifying the TAI. It allows a single-sided provisioning model where an incoming label mapping message with a TAI that matches the SAII of that spoke SDP to be automatically bound to that endpoint. This is useful in scenarios where a service provider wishes to separate service configuration from the service activation phase.

Automatic endpoint configuration is supported required for Epipe VLL spoke-sdp-fec endpoints bound to a VLL SAP. It is configured using the spoke-sdp-fec>auto-config command, and excluding the TAI from the configuration. When auto-configuration is used, the node assumed passive behavior from a point of view of T-LDP signaling (see above). Therefore, the far-end T-PE must be configured for signaling master for that spoke-sdp-fec.

Selecting a Path for an MS-PW

Path selection for signaling occurs in the outbound direction (ST-PE to TT-PE) for an MS-PW. In the TT-PE to ST-PE direction, a label mapping message simply follows the reverse of the path already taken by the outgoing label mapping.

A node can use explicit paths, static routes, or BGP routes to select the next hop S-PE or T-PE. The order of preference used in selecting these routes is:

1. Explicit Path
2. Static route
3. BGP route
In order to use an explicit path for an MS-PW, an explicit path must have been configured in the
config>services>pw-routing>path path-name context. The user must then configure the
 corresponding path path-name under spoke-sdp-fec.

If an explicit path name is not configured, then the TT-PE or S-PE will perform a longest match
lookup for a route (static if it exists, and BGP if not) to the next hop S-PE or T-PE to reach the
TAII.

Pseudowire routing chooses the MS-PW path in terms of the sequence of S-PEs to use to reach a
given T-PE. It does not select the SDP to use on each hop, which is instead determined at signaling
time. When a label mapping is sent for a given pseudowire segment, an LDP SDP will be used to
reach the next-hop S-PE/T-PE if such an SDP exists. If not, and a RFC 3107 labeled BGP SDP is
available, then that will be used. Otherwise, the label mapping will fail and a label release will be
sent.

Pseudowire Templates

Dynamic MS-PWs support the use of the pseudowire template for specifying generic pseudowire
parameters at the T-PE. The pseudowire template to use is configured in the spoke-sdp-fec>pw-
template-bind policy-id context. Dynamic MS-PWs do not support the provisioned SDPs
specified in the pseudowire template.
Pseudowire Redundancy

Pseudowire redundancy is supported on dynamic MS-PWs used for VLLs. It is configured in a similar manner to pseudowire redundancy on VLLs using FEC128, whereby each spoke-sdp-fec within an endpoint is configured with a unique SAII/TAII.

Figure 44 illustrates the use of pseudowire redundancy.

Figure 44: Pseudowire Redundancy

The following is a summary of the key points to consider in using pseudowire redundancy with dynamic MS-PWs:

- Each MS-PW in the redundant set must have a unique SAII/TAII set and is signalled separately. The primary pseudowire is configured in the spoke-sdp-fec>primary context.
- Each MS-PW in the redundant set should use a diverse path (from the point of view of the S-PEs traversed) from every other MS-PW in that set if path diversity is possible in a given network topology. There are a number of possible ways to achieve this:
  - Configure an explicit path for each MS-PW.
  - Allow BGP routing to automatically determine diverse paths using BGP policies applied to different local prefixes assigned to the primary and standby MS-PWs.
  - Path diversity can be further provided for each primary pseudowire through the use of a BGP route distinguisher.
If the primary MS-PW fails, fail-over to a standby MS-PW, as per the normal pseudowire redundancy procedures. A configurable retry timer for the failed primary MS-PW is then started. When the timer expires, attempt to re-establish the primary MS-PW using its original path, up to a maximum number of attempts as per the retry count parameter. The T-PE may then optionally revert back to the primary MS-PW on successful reestablishment.

Note that since the SDP ID is determined dynamically at signaling time, it cannot be used as a tie breaker to choose the primary MS-PW between multiple MS-PWs of the same precedence. The user should therefore explicitly configure the precedence values to determine which MS-PW is active in the final selection.
VCCV OAM for Dynamic MS-PWs

The primary difference between dynamic MS-PWs and those using FEC128 is support for FEC129 AII type 2. As in PW Switching, VCCV on dynamic MS-PWs requires the use of the VCCV control word on the pseudowire. Both the vccv-ping and vccv-trace commands support dynamic MS-PWs.

VCCV-Ping on Dynamic MS-PWs

VCCV-ping supports the use of FEC129 AII type 2 in the target FEC stack of the ping echo request message. The FEC to use in the echo request message is derived in one of two ways: Either the user can specify only the spoke-sdp-fec-id of the MS-PW in the vccv-ping command, or the user can explicitly specify the SAIII and TAIII to use.

If the SAIII:TAIII is entered by the user in the vccv-ping command, then those values are be used for the vccv-ping echo request, but their order is be reversed before being sent so that they match the order for the downstream FEC element for an S-PE, or the locally configured SAIII:TAIII for a remote T-PE of that MS-PW. Note that SAIII:TAIII is entered in addition to the spoke-sdp-fec-id, then the system will verify the entered values against the values stored in the context for that spoke-sdp-fec-id.

Otherwise, if the SAIII:TAIII to use in the target FEC stack of the vccv-ping message is not entered by the user, and if a switching point TLV was previously received in the initial label mapping message for the reverse direction of the MS-PW (with respect to the sending PE), then the SAIII:TAIII to use in the target FEC stack of the vccv-ping echo request message is derived by parsing that switching point TLV based on the user-specified TTL (or a TTL of 255 if none is specified). In this case, the order of the SAIII:TAIII in the switching point TLV is maintained for the vccv-ping echo request message.

If no pseudowire switching point TLV was received, then the SAIII:TAIII values to use for the vccv-ping echo request are derived from the MS-PW context, but their order is reversed before being sent so that they match the order for the downstream FEC element for an S-PE, or the locally configured SAIII:TAIII for a remote T-PE of that MS-PW.

Note that the use of spoke-sdp-fec-id in vccv-ping is only applicable at T-PE nodes, since it is not configured for a given MS-PW at S-PE nodes.
VCCV-Trace on Dynamic MS-PWs

The 7x50 supports the MS-PW path trace mode of operation for VCCV trace, as per pseudowire switching, but using FEC129 AII type 2. As in the case of vccv-ping, the SAI1:TAII used in the VCCV echo request message sent from the T-PE or S-PE from which the VCCV trace command is executed is specified by the user or derived from the context of the MS-PW. Note that the use of *spoke-sdp-fec-id* in vccv-trace is only applicable at T-PE nodes, since it is not configured for a given MS-PW at S-PE nodes.
Example Dynamic MS-PW Configuration

This section presents an example of how to configure Dynamic MS-PWs for a VLL service between a set of 7x50 nodes. The network consists of two 7x50 T-PEs and two 7x50 playing the role of S-PEs, as shown in the following figure. Each 7x50 peers with its neighbor using LDP and BGP.

![Figure 45: Dynamic MS-PW Example](image)

The example uses BGP to route dynamic MS-PWs and T-LDP to signal them. Therefore each node must be configured to support the MS-PW address family under BGP, and BGP and LDP peerings must be established between the T-PEs/S-PEs. The appropriate BGP export policies must also be configured.

Next, pseudowire routing must be configured on each node. This includes an S-PE address for every participating node, and one or more local prefixes on the T-PEs. MS-PW paths and static routes may also be configured.

Once this routing and signaling infrastructure is established, spoke-sdp-fecs can be configured on each of the T-PEs.
config
router
  ldp
    targeted-session
      peer 10.20.1.5
      exit
    exit
  policy-options
    begin
      policy-statement "exportMsPw"
        entry 10
          from
          family ms-pw
        exit
        action accept
        exit
      exit
    exit
  commit
config
router
  ldp
    targeted-session
      peer 10.20.1.2
      exit
    exit
  policy-options
    begin
      policy-statement "exportMsPw"
        entry 10
          from
          family ms-pw
        exit
        action accept
        exit
      exit
    exit
config
service
  pw-routing
    spe-address 3:10.20.1.3
    local-prefix 3:10.20.1.3 create
    exit
  path "path1_to_F" create
    hop 1 10.20.1.5
    hop 2 10.20.1.2
    no shutdown
    exit
  epipe 1 customer 1 vpn 1 create
    description "Default epipe"
    description for service id 1"
    service-mtu 1400
    service-name "XYZ Epipe 1"
    sap 2/1/1:1 create
    exit
  spoke-sdp-fec 1 fec 129 aii-type 2 create
    retry-timer 10
    retry-count 10
    sai1-type2 3:10.20.1.3:1
    tai1-type2 6:10.20.1.6:1
    no shutdown
    exit
    no shutdown
    exit
config
  pw-routing
    spe-address 6:10.20.1.6
    local-prefix 6:10.20.1.6 create
    exit
  path "path1_to_F" create
    hop 1 10.20.1.2
    hop 2 10.20.1.5
    no shutdown
    exit
  epipe 1 customer 1 vpn 1 create
    description "Default epipe"
    description for service id 1"
    service-mtu 1400
    service-name "XYZ Epipe 1"
    sap 1/1/3:1 create
    exit
  spoke-sdp-fec 1 fec 129 aii-type 2 create
    retry-timer 10
    retry-count 10
    sai1-type2 6:10.20.1.6:1
    tai1-type2 3:10.20.1.3:1
    no shutdown
    exit
    no shutdown
    exit
config router
  ldp
targeted-session
  peer 10.20.1.3
  exit
  peer 10.20.1.2
  exit
  exit
  bgp
  family ms-pw
  connect-retry 1
  min-route-advertisement 1
  rapid-withdrawal
  group "ebgp"
  neighbor 10.20.1.2
    multihop 255
    peer-as 300
    exit
  neighbor 10.20.1.3
    multihop 255
    peer-as 100
    exit
  exit
  exit
  service
  pw-routing
    spe-address 5:10.20.1.5
    exit

S-PE-1

S-PE-2

config router
  ldp
targeted-session
  peer 10.20.1.5
  exit
  peer 10.20.1.6
  exit
  exit
  bgp
  family ms-pw
  connect-retry 1
  min-route-advertisement 1
  rapid-withdrawal
  group "ebgp"
  neighbor 10.20.1.5
    multihop 255
    peer-as 200
    exit
  neighbor 10.20.1.6
    multihop 255
    peer-as 400
    exit
  exit
  exit
  service
  pw-routing
    spe-address 2:10.20.1.2
    exit
VLL Resilience with Two Destination PE Nodes

Figure 46 illustrates the application of pseudowire redundancy to provide Ethernet VLL service resilience for broadband service subscribers accessing the broadband service on the service provider BRAS.

If the Ethernet SAP on PE2 fails, PE2 notifies PE1 of the failure by either withdrawing the primary pseudowire label it advertised or by sending a pseudowire status notification with the code set to indicate a SAP defect. PE1 will receive it and will immediately switch its local SAP to forward over the secondary standby spoke SDP. In order to avoid black holing of in-flight packets during the switching of the path, PE1 will accept packets received from PE2 on the primary pseudowire while transmitting over the backup pseudowire. However, in other applications such as those described in Access Node Resilience Using MC-LAG and Pseudowire Redundancy on page 315, it will be important to minimize service outage to end users.

When the SAP at PE2 is restored, PE2 updates the new status of the SAP by sending a new label mapping message for the same pseudowire FEC or by sending pseudowire status notification message indicating that the SAP is back up. PE1 then starts a timer and reverts back to the primary at the expiry of the timer. By default, the timer is set to 0, which means PE1 reverts immediately. A special value of the timer (infinity) will mean that PE1 should never revert back to the primary pseudowire.

The behavior of the pseudowire redundancy feature is the same if PE1 detects or is notified of a network failure that brought the spoke SDP operational status to DOWN. The following are the events which will cause PE1 to trigger a switchover to the secondary standby pseudowire:

1. T-LDP peer (remote PE) node withdrew the pseudowire label.
2. T-LDP peer signaled a FEC status indicating a pseudowire failure or a remote SAP failure.
3. T-LDP session to peer node times out.
4. SDP binding and VLL service went down as a result of network failure condition such as the SDP to peer node going operationally down.

The SDP type for the primary and secondary pseudowires need not be the same. In other words, the user can protect a RSVP-TE based spoke SDP with a LDP or GRE based one. This provides the ability to route the path of the two pseudowires over different areas of the network.

Alcatel-Lucent’s routers support the ability to configure multiple secondary standby pseudowire paths. For example, PE1 uses the value of the user configurable precedence parameter associated with each spoke SDP to select the next available pseudowire path after the failure of the current active pseudowire (whether it is the primary or one of the secondary pseudowires). The revertive operation always switches the path of the VLL back to the primary pseudowire though. There is no revertive operation between secondary paths meaning that the path of the VLL will not be switched back to a secondary pseudowire of higher precedence when the latter comes back up again.

Alcatel-Lucent’s routers support the ability for a user-initiated manual switchover of the VLL path to the primary or any of the secondary be supported to divert user traffic in case of a planned outage such as in node upgrade procedures.
Master-Slave Operation

Master-Slave pseudowire redundancy is discussed in this section. It adds the ability for the remote peer to react to the pseudowire standby status notification, even if only one spoke-SDP terminates on the VLL endpoint on the remote peer, by blocking the transmit (Tx) direction of a VLL spoke SDP when the far-end PE signals standby. This solution enables the blocking of the Tx direction of a VLL spoke SDP at both master and slave endpoints when standby is signalled by the master endpoint. This approach satisfies a majority of deployments where bidirectional blocking of the forwarding on a standby spoke SDP is required.

Figure 47 illustrates the operation of master-slave pseudowire redundancy. In this scenario, an Epipe service is provided between CE1 and CE2. CE2 is dual homed to PE2 and PE3, and thus PE1 is dual-homed to PE2 and PE3 using Epipe spoke SDPs. The objectives of this feature is to ensure that only one pseudowire is used for forwarding in both directions by PE1, PE2 and PE3 in the absence of a native dual homing protocol between CE2 and PE2/PE3, such as MC-LAG. In normal operating conditions (the SAPs on PE2 and PE3 towards CE2 are both up and there are no defects on the ACs to CE2), PE2 and PE3 cannot choose which spoke SDP to forward on based on the status of the AC redundancy protocol.
Master-slave pseudowire redundancy adds the ability for the remote peer to react to the pseudowire standby status notification, even if only one spoke SDP terminates on the VLL endpoint on the remote peer. When the CLI command `standby-signaling-slave` is enabled at the spoke SDP or explicit endpoint level in PE2 and PE3, then any spoke SDP for which the remote peer signals PW FWD Standby will be blocked in the transmit direction.

This is achieved as follows. The `standby-signaling-master` state is activated on the VLL endpoint in PE1. In this case, a spoke SDP is blocked in the transmit direction at this master endpoint if it is either in operDown state, or it has lower precedence than the highest precedence spoke SDP, or the given peer PE signals one of the following pseudowire status bits:

- Pseudowire not forwarding (0x01)
- SAP (ingress) receive fault (0x02)
- SAP (egress) transmit fault (0x04)
- SDP binding (ingress) receive fault (0x08)
- SDP binding (egress) transmit fault (0x10)

The fact that the given spoke SDP has been blocked will be signaled to LDP peer through the pseudowire status bit (PW FWD Standby (0x20)). This will prevent traffic being sent over this spoke SDP by the remote peer, but obviously only in case that remote peer supports and reacts to pseudowire status notification. Previously, this applied only if the spoke SDP terminates on an IES, VPRN or VPLS. However, if standby-signaling-slave is enabled at the remote VLL endpoint then the Tx direction of the spoke SDP will also be blocked, according to the rules in Operation of Master-Slave Pseudowire Redundancy with Existing Scenarios on page 293.

Note that although master-slave operation provides bidirectional blocking of a standby spoke SDP during steady-state conditions, it is possible that the Tx directions of more than one slave endpoint can be active for transient periods during a fail-over operation. This is due to slave endpoints.
transitioning a spoke SDP from standby to active receiving and/or processing a pseudowire preferential forwarding status message before those transitioning a spoke SDP to standby. This transient condition is most likely when a forced switch-over is performed, or the relative preferences of the spoke SDPs is changed, or the active spoke SDP is shutdown at the master endpoint. During this period, loops of unknown traffic may be observed. Fail-overs due to common network faults that can occur during normal operation, a failure of connectivity on the path of the spoke SDP or the SAP, would not result in such loops in the data path.
Interaction with SAP-Specific OAM

If all of the spoke SDPs bound to a SAP at a slave PE are selected as standby, then this should be treated from a SAP OAM perspective in the same manner as a fault on the service, an SDP-binding down or remote SAP down. That is, a fault should be indicated to the service manager. If SAP-specific OAM is enabled towards the CE, such as Ethernet CCM, E-LMI, or FR LMI, then this should result in the appropriate OAM message being sent on the SAP. This can enable the remote CE to avoid forwarding traffic towards a SAP which will drop it.

Figure 48 shows an example for the case of Ethernet LMI.

Figure 48: Example of SAP OAM Interaction with Master-Slave Pseudowire Redundancy
Local Rules at Slave VLL PE

It is not possible to configure a standby-signaling-slave on endpoints or spoke SDPs bound to an IES, VPRN, ICB, MC-EP or that form part of an MC-LAG or MC-APS.

If ‘standby-signaling-slave’ is configured on a given spoke SDP or explicit endpoint, then the following rules apply. Note that the rules describe the case of several spoke SDPs in an explicit endpoint. The same rules apply to the case of a single spoke SDP outside of an endpoint where no endpoint exists:

- Rules for processing endpoint SAP active/standby status bits:
  - Since the SAP in endpoint X is never a part of a MC-LAG/MC-APS instance, a forwarding status of ACTIVE is always advertised.
- Rules for processing and merging local and received endpoint object status Up/Down operational status:
  1. Endpoint ‘X’ is operationally UP if at least one of its objects is operationally UP. It is Down if all its objects are operationally down.
  2. If all objects in endpoint ‘X’ transition locally to Down state, and/or received a “SAP Down” notification via remote T-LDP status bits or via SAP specific OAM signal, and/or received status bits of “SDP-binding down”, and/or received status bits of “PW not forwarding”, the node must send status bits of “SAP Down” over all ‘Y’ endpoint spoke SDPs.
  3. Endpoint ‘Y’ is operationally UP if at least one of its objects is operationally UP. It is Down if all its objects are operationally down.
  4. If a spoke SDP in endpoint ‘Y’, including the ICB spoke SDP, transitions locally to Down state, the node must send T-LDP “SDP-binding down” status bits on this spoke SDP.
  5. If a spoke SDP in endpoint ‘Y’, received T-LDP “SAP down” status bits, and/or received T-LDP “SDP-binding down” status bits, and/or received status bits of “PW not forwarding”, the node saves this status and takes no further action. The saved status is used for selecting the active transmit endpoint object as per the pseudo-code in Section 5.1.2.
  6. If, all objects in endpoint ‘Y’, or a single spoke SDP that exists outside of an endpoint (and no endpoint exists), transition locally to down state, and/or received T-LDP “SAP Down” status bits, and/or received T-LDP “SDP-binding down” status bits, and/or received status bits of “PW not forwarding”, and/or the received status bits of ‘PW FWD standby’, the node must send a “SAP down” notification on the ‘X’ endpoint SAP via the SAP specific OAM signal, if applicable.
  7. If the peer PE for a given object in endpoint ‘Y’ signals ‘PW FWD standby’, the spoke SDP must be blocked in the transmit direction and the spoke SDP is not eligible for selection by the active transmit selection rules.
  8. If the peer PE for a given object in endpoint ‘Y’ does not signal ‘PW FWD standby’, then spoke SDP is eligible for selection.
Operation of Master-Slave Pseudowire Redundancy with Existing Scenarios

This section discusses how master-slave pseudowire redundancy could operate.

VLL Resilience

Figure 49 displays a VLL resilience path example. An sample configuration follows.

Note that a revert-time value of zero (default) means that the VLL path will be switched back to the primary immediately after it comes back up.

PE1
configure service epipe 1
  endpoint X
  exit
  endpoint Y
  revert-time 0
  standby-signaling-master
  exit
  sap 1/1/1:100 endpoint X
  spoke-sdp 1:100 endpoint Y
  precedence primary
  spoke-sdp 2:200 endpoint Y
  precedence 1
PE2
configure service epipe 1
  endpoint X
  exit
  sap 2/2/2:200 endpoint X
  spoke-sdp 1:100
    standby-signaling-slave
PE3

configure service epipe 1
  endpoint X
  exit
  sap 3/3/3:300 endpoint X
  spoke-sdp 2:200
    standby-signaling-slave
VLL Resilience for a Switched Pseudowire Path

Figure 50 displays a VLL resilience for a switched pseudowire path example. A sample configuration follows.

![Diagram of VLL Resilience with Pseudowire Switching]

**Figure 50: VLL Resilience with Pseudowire Switching**

**Configuration**

**T-PE1**
configure service epipe 1
    endpoint X
    exit
    endpoint Y
    revert-time 100
    standby-signaling-master
    exit
    sap 1/1/1:100 endpoint X
    spoke-sdp 1:100 endpoint Y
        precedence primary
    spoke-sdp 2:200 endpoint Y
        precedence 1
    spoke-sdp 3:300 endpoint Y
        precedence 1

**T-PE2**
configure service epipe 1
    endpoint X
    exit
    endpoint Y
    revert-time 100
    standby-signaling-slave
    exit
    sap 2/2/2:200 endpoint X
    spoke-sdp 4:400 endpoint Y
S-PE1

VC switching indicates a VC cross-connect so that the service manager does not signal the VC label mapping immediately but will put this into passive mode.

configure service epipe 1 vc-switching
  spoke-sdp 1:100
  spoke-sdp 4:400

---

**Epipe Using BGP-MH Site Support for Ethernet Tunnels**

Using Epipe in combination with G.8031 and BGP Multi-Homing in the same manner as VPLS offers a multi-chassis resiliency option for Epipe services that is a non-learning and non-flooded service. Note that MC-LAG (see, Access Node Resilience Using MC-LAG and Pseudowire Redundancy on page 315) offers access node redundancy with active/stand-by links while Ethernet Tunnels offers per service redundancy with all active links and active or standby services. G.8031 offers an end to end service resiliency for Epipe and VPLS services. BGP-MH Site Support for Ethernet Tunnels offers Ethernet edge resiliency for Epipe services that integrates with MPLS Pseudowire Redundancy.
Figure 51 shows the BGP-MH Site Support for Ethernet Tunnels; where a G.8031 edge device (A) is configured to two provider edge switches (B and C). G.8031 is configured on the Access devices (A and F). An Epipe Endpoint service is configured along with BGP Multi-homing and Pseudowire Redundancy on the provider edge nodes (B,C and D,E). This configuration offers a fully redundant Epipe service.
Operational Overview

G.8031 offers a number of redundant configurations. Normally it offers the ability to control two independent paths for 1:1 protection. In the BGP-MH Site Support for Ethernet Tunnels case, BGP drives G.8031 as a slave service. In this case, the Provider Edge operates using only standard 802.1ag MEPs with CCM to monitor the paths. Figure 52 shows an Epipe service on a Customer Edge (CE) device that uses G.8031 with two paths and two MEPs. The Paths can use a single VLAN of DOT1Q or QinQ encapsulation.

![Diagram of G.8031 for Slave Operation](image)

**Figure 52: G.8031 for Slave Operation**

In a single-service deployment the control (CFM) and data will share the same port and VID. For multiple services for scaling fate sharing is allowed between multiple SAPs, but all SAPs within a group must be on the same physical port.

To get fate sharing for multiple services with this feature, a dedicated G.8031 CE based service (one VLAN) is connect to a Epipe SAP on a PE which uses BGP-MH and operational groups to control other G.8031 tunnels. This dedicated G.8031 still has a data control capabilities, but the data Epipe service is not bearing user data packets. On the CE, this dedicated G.8031 is only used for group control. The choice of making this a dedicated Control for a set of G.8031 tunnels is merely to simplify operation and allow individual disabling of services. Using a dedicated G.8031 for both control and to carry data traffic is allowed.
Fate sharing from the PE side is achieved using BGP and operational groups. G.8031 Epipe services can be configured on the CE as regular non fate shared G.8031 services but due to the configuration on the PE side, these Ethernet Tunnels will be treated as a group following the one designated control service. The G.8031 control logic on the CE is slaved to the BGP-MH control.

On the CE G.8031 allows independent configuration of VIDs on each path. On the PE the Epipe or Endpoint that connects to the G.8031 must have a SAP with the corresponding VID. If the G.8031 service has a Maintenance End Point (MEP) for that VID, the SAP should be configured with a MEP. The MEPs on the paths on the CE signal standard interface status TLV (ifStatusTLV), No Fault (Up) and Fault (Down). The MEPs on the PE (Epipe or Endpoint) also use signaling of ifStatusTlv No Fault, and Fault to control the G.8031 SAP. However in the 7x50 model fate shared Ethernet Tunnels with no MEP are allowed. In this case it is up to the CE to manage these CE based fate shared tunnels.

Interfaces status signaling (ifStatusTLV) is used to control the G.8031 tunnel form the PE side. Normally the CE will signal No Fault in the path SAP MEP inStatusTLV before the BGP-MH will cause the SAP MEP to become active by signaling No Fault.

---

**Detailed Operation**

For this feature, BGP-MH is used the master control and the Ethernet Tunnel is a slave. The G.8031 on the CE is unaware that it is being controlled. While a single Epipe service is configured and will serve as the control for the CE connection allowing fate sharing all signaling to the CE is based on the ifstatusTLV per G.8031 tunnel. Note with G.8031 by controlling it with BGP-MH, the G.8031 CE is forced to be slaved to the PE BGP-MH election. BGP-MH election is control by the received VPLS preference or BGP local-preference or PE Id (IP address of Provider Edge) if local-preference is equal. There may be traps generated on the CE side for some G.8031 implementations but these can be suppressed or filtered to allow this feature to operate.
There are two configuration options:

- Every G.8031 service SAP terminates on a single Epipe that has BGP-MH. These Epipes may utilize endpoints with or without ICBs.
- A control Epipe service that monitors a single SAP that is used for group control of fate shared CE services. In this case, the Epipe service has a SAP that serves as the control termination for one Ethernet Tunnel connection. The group fate sharing SAPs may or may not have MEPs if they use shared fate. In this case the Epipe may have endpoints but will not support ICBs.

The MEP ifStatusTlv and CCM are used for monitoring the PE to CE SAP. MEP ifStatusTlv is used to signal, the Ethernet Tunnel inactive and is used CCM as an aliveness mechanism. There is no G.8031 logic on the PE, the SAP is simply controlling the correspond CE SAP.

---

**Sample Operation of G.8031 BGP-MH**

Any Ethernet tunnel actions (force, lock) on the CE (single site) do not control the action to switch paths directly but they may influence the outcome of BGP-MH if they are on a control tunnel. If a path is disabled on the CE the result may force the SAP with an MEP on the PE to eventually take the SAP down but it is suggested to run commands from the BGP-MH side to control these connections.

---

**Figure 53: Full Redundancy G.8031 Epipe & BGP-MH**
Table 4 lists the SAP MEP signaling shown in Figure 53. For a description of the events shown in this sample operation, see Events in Sample Operation on page 301.

Table 4: SAP MEP Signaling

<table>
<thead>
<tr>
<th></th>
<th>G.8031 ET on CE</th>
<th>Path A MEP Facing Node B Local ifStatus</th>
<th>Path B MEP Facing Node C Local ifStatus</th>
<th>Path B PE MEP ifStatus</th>
<th>Path B PE MEP ifStatus</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Down (inactive)</td>
<td>No Fault&lt;sup&gt;a&lt;/sup&gt;</td>
<td>No Fault</td>
<td>Fault</td>
<td>Fault</td>
</tr>
<tr>
<td>2</td>
<td>Up use Path A</td>
<td>No Fault</td>
<td>No Fault</td>
<td>No Fault</td>
<td>Fault</td>
</tr>
<tr>
<td>3</td>
<td>Up use Path B</td>
<td>No Fault</td>
<td>No Fault</td>
<td>Fault</td>
<td>No Fault</td>
</tr>
<tr>
<td>4</td>
<td>Down Path a fault</td>
<td>Fault&lt;sup&gt;b&lt;/sup&gt;</td>
<td>No Fault</td>
<td>Fault</td>
<td>Fault</td>
</tr>
<tr>
<td>5</td>
<td>Down Path A &amp; B fault at A</td>
<td>Fault</td>
<td>No Fault</td>
<td>Fault</td>
<td>Fault</td>
</tr>
<tr>
<td>6</td>
<td>Partitioned Network Use Path Precedence Up use Path A</td>
<td>No Fault</td>
<td>No Fault</td>
<td>No Fault</td>
<td>No Fault</td>
</tr>
</tbody>
</table>

<sup>a</sup> No Fault = no ifStatusTlv transmit | CCM transmit normally

<sup>b</sup> Fault = ifStatusTlv transmit down | no CCM transmit

Events in Sample Operation

The following represents a walk through of the events for switchover in Figure 53. This configuration uses operational groups. The nodes of interest are A, B and C listed in Table 4.

1. A single G.8031 SAP that represents the control for a group of G.8031 SAPs is configured on the CE.
   → The Control SAP does not normally carry any data, however it can if desired.
   → An Epipe service is provisioned on each PE node (B,C) purely for control (no customer traffic flows over this service).
   → On CE A, there is an Epipe Ethernet Tunnel (G.8031) control SAP.
   → The Ethernet Tunnel has two paths:
      – one facing B
      – one facing C.
   → PE B has an Epipe control SAP that is controlled by BGP-MH site and PE C also has the corresponding SAP that is controlled by the same BGP-MH site.
2. At node A, there are MEPs configured under each path that check connectivity on the A-B and A-C links. At nodes B and C, there is a MEP configured under their respective SAPs with fault propagation enabled with use ifStatusTlv.

3. Initially, assume there is no link failure:
   - SAPs on node A have ifStatusTlv No Fault to B and C (no MEP fault detected at A); see Table 4 row 1 (Fault is signaled in the other direction PE to CE).
   - BGP-MH makes its determination of the master or Designated Forwarder (DF).
   - Assume SAP on node B is picked as the DF.
   - The MEP at Path A-B signals ifStatusTlv No Fault. Due to this signal, the MEP under the node A path facing node B, detects the path to node B is usable by the path manager on A.

4. At the CE node A, Path A-C becomes standby and is brought down; see Table 4 row 2.
   - Since fault propagation is enabled under the SAP node C MEP, and ifStatusTlv is operationally Down remains in the present state.
   - Under these conditions, the MEP under the node A path facing node C detects the fault and informs Ethernet manager on node A.
   - Node A then considers bringing path A-C down.
   - ET port remains up since path A-B is operationally up. This is a stable state.

5. On nodes B and C, each Epipe controlled SAP is the sole (controlling) member of an operational-group.
   - Other data SAPs may be configured for fate shared VLANs (Ethernet Tunnels) and to monitor the control SAP.
   - The SAPs facing the CE node A share the fate of the control SAP and follow the operation.

6. If there is a break in path A-B connectivity (CCM time out or LOS on the port for link A-B), then on node A the path MEP detects connectivity failure and informs Ethernet Tunnel Manager; see Table 4 row 4.

7. At this point the Ethernet Tunnel is down since both path A-B and path A-C are down.

8. The CE node A Ethernet Tunnel goes down.

9. Node B on the PE the SAP also detects the failure and the propagation of fault status goes to BGP-MH; see Table 4 row 4.

10. This in turn feeds into BGP-MH which deems the site non-DF and makes the site standby.

11. Since the SAP at Node B is standby, Service Manager feeds this to CFM, which then propagates a Fault towards Node A. This is a cyclic fault propagation. However, since path A-B is broken, the situation is stable; see Table 4 row 5.

12. There is traffic loss during the BGP-MH convergence.
   - Load sharing mode is recommended when using a 7450 as a CE node A device.
   - BGP-MH signals that node C is now the DF; see Table 4 row 3.
13. BGP-MH on node C elects sap and bring it up.
14. ET port transitions to port A-C is operationally up. This is a stable state. The A-C SAPs monitoring the operational-group on C transitions to operationally up.

Unidirectional failures: At point 6 the failure was detected at both ends. In the case of a unidirectional failure, CCM times out on one side.

1. In the case where the PE detects the failure, it propagates the failure to BGP-MH and the BGP-MH takes the site down causing the SAPs on the PE to signal to the CE Fault.
2. In the case of G.8031 on the CE detecting the failure, it takes the tunnel down and signals a fault to the PE, and then the SAP propagates that to BGP-MH.

---

**BGP-MH Site Support for Ethernet Tunnels Operational-Group Model**

For operational groups, one or more services follow the controlling service. On node A, there is an ET SAP facing nodes B/C, and on nodes B/C there are SAPs of the Epipe on physical ports facing node A. Each of the PE data SAPs monitor their respective operational groups, meaning they are operationally up, or down based on the operational status of the control SAPs. On node A, since the data SAP is on the ET logical port, it goes operationally down whenever the ET port goes down and similarly for going operationally up.

Alternatively, an Epipe Service may be provisioned on each node for each G.8031 data SAP (one for one service with no fate sharing). On CE node A, there will be a G.8031 Ethernet Tunnel. The Ethernet Tunnel has two paths: one facing node B and one facing node C. This option is the same as the control SAP, but there are no operational groups. However, now there is a BGP-MH Site per service. For large sites operational groups are more efficient.

---

**BGP-MH Specifics for MH Site Support for Ethernet Tunnels**

BGP Multi-Homing for VPLS on page 620 describes the procedures for using BGP to control resiliency for VPLS. These procedures are the same except that an Epipe service can be configured for BGP-MH.

---

**PW Redundancy for BGP MH Site Support for Ethernet Tunnels**

Pseudowire Redundancy Service Models on page 319 and Figure 56 on page 317 are used for the MPLS network resiliency. BGP MH Site Support for Ethernet Tunnels reuses this model.
T-LDP Status Notification Handling Rules of BGP-MH Epipes

Using Figure 56 as a reference, the following are the rules for generating, processing, and merging T-LDP status notifications in VLL service with endpoints.

Rules for Processing Endpoint SAP Active/Standby Status Bits

1. The advertised admin forwarding status of Active/Standby reflects the status of the local Epipe SAP in BGP-MH instance. If the SAP is not part of a MC-LAG instance or a BGP-MH instance, the forwarding status of Active is always advertised.

2. When the SAP in endpoint X is part of a BGP-MH instance, a node must send T-LDP forwarding status bit of SAP Active/Standby over all Y endpoint spoke-SDPs, except the ICB spoke-SDP whenever this (BGP-MH designated forwarder) status changes. The status bit sent over the ICB is always zero (Active by default).

3. When the SAP in endpoint X is not part of a MC-LAG instance or BGP-MH instance, then the forwarding status sent over all Y endpoint spoke-SDPs should always be set to zero (Active by default).

4. The received SAP Active/Standby status is saved and used for selecting the active transmit endpoint object Pseudowire Redundancy procedures.

Rules for Processing, Merging Local, and Received Endpoint Operational Status

1. Endpoint X is operationally Up if at least one of its objects is operationally Up. It is Down if all its objects are operationally Down.

2. If the SAP in endpoint X transitions locally to the Down state, or received a SAP Down notification via SAP specific OAM signal (SAP MEP), the node must send T-LDP SAP Down status bits on the Y endpoint ICB spoke-SDP only. BGP-MH SAP support MEPs for ifStatusTlv signaling. All other SAP types cannot exist on the same endpoint as an ICB spoke-SDP since non Ethernet SAP cannot be part of a MC-LAG instance or a BGP-MH Instance.

3. If the ICB spoke-SDP in endpoint X transitions locally to Down state, the node must send T-LDP SDP-binding Down status bits on this spoke-SDP.

4. If the ICB spoke-SDP in endpoint X received T-LDP SDP-binding Down status bits or PW not forwarding status bits, the node saves this status and takes no further action. The saved status is used for selecting the active transmit endpoint object as per the pseudo-code per Pseudowire Redundancy procedures.

5. If all objects in endpoint X transition locally to Down state due to operator or BGP-MH DF election, or received a SAP Down notification via remote T-LDP status bits or via SAP specific OAM signal (SAP MEP), or received status bits of SDP-binding Down, or received sta-
tus bits of PW not forwarding, the node must send status bits of SAP Down over all Y endpoint spoke-SDPs, including the ICB.

6. Endpoint Y is operationally Up if at least one of its objects is operationally Up. It is Down if all its objects are operationally Down.

7. If a spoke-SDP in endpoint Y, including the ICB spoke-SDP, transitions locally to Down state, the node must send T-LDP SDP-binding Down status bits on this spoke-SDP.

8. If a spoke-SDP in endpoint Y, including the ICB spoke-SDP, received T-LDP SAP Down status bits, or received T-LDP SDP-binding Down status bits, or received status bits of PW not forwarding, the node saves this status and takes no further action. The saved status is used for selecting the active transmit endpoint object as per Pseudowire Redundancy procedures.

9. If all objects in endpoint Y, except the ICB spoke-SDP, transition locally to Down state, or received T-LDP SAP Down status bits, or received T-LDP SDP-binding Down status bits, and/or received status bits of PW not forwarding, the node must send status bits of SDP-binding Down over the X endpoint ICB spoke-SDP only.

10. If all objects in endpoint Y transition locally to Down state, or received T-LDP SAP Down status bits, or received T-LDP SDP-binding Down status bits, or received status bits of PW not forwarding, the node must send status bits of SDP-binding Down over the X endpoint ICB spoke-SDP, and must send a SAP Down notification on the X endpoint SAP via the SAP specific OAM signal in this case the SAP MEP ifStatusTlv operationally-Down and also signal the BGP-MH Site, if this SAP is part of a BGP Site.

Operation for BGP MH Site Support for Ethernet Tunnels

A multi-homed site can be configured on up to four PEs although two PEs are sufficient for most applications with each PE having a single object SAP connecting to the multi-homed site. Note that SR OS G.8031 implementation with load sharing allows multiple PEs as well. The designated forwarder election chooses a single connection to be operationally up with the other placed in standby. Only revertive behavior is supported in this release.

Fate-sharing (the status of one site can be inherited from another site) is achievable using monitor-groups.

The following are supported:

- All Ethernet-tunnels G.8031 SAPs on CE:
  - 7x50 G.8031 in load sharing mode (recommended)
  - 7x50 G.8031 in non-load sharing mode
- Epipe and Endpoint with SAPs on PE devices.
- Endpoints with PW.
- Endpoints with active/standby PWs.
There are the following constraints with this feature:

- Not supported with PBB Epipes.
- Spoke SDP (pseudowire).
  - BGP signaling is not supported.
  - Cannot use BGP MH for auto-discovered pseudowire. This is achieved in a VPLS service using SHGs, which are not available in Epipes.
- Other multi-chassis redundancy features are not supported on the multi-homed site object, namely:
  - MC-LAG
  - MC-EP
  - MC-ring
  - MC-APS
- Master and Slave pseudowire is not supported.

Figure 54: Sample Topology Full Redundancy

Refer to Configuration Examples on page 307 for configuration examples derived from Figure 54.
Configuration Examples

Node-1: Using operational groups and Ethernet CFM per SAP

#--------------------------------------------------
# Echo "Eth-CFM Configuration"
#--------------------------------------------------
eth-cfm
  domain 100 format none level 3
  association 2 format icc-based name "node-3-site-1-0"
    bridge-identifier 1
    remote-mepid 310
  exit
  association 2 format icc-based name "node-3-site-1-1"
    bridge-identifier 100
    remote-mepid 311
  exit
exit
exit

#--------------------------------------------------
# Echo "Service Configuration"
#--------------------------------------------------
service
  customer 1 create
    description "Default customer"
  exit
  sdp 2 mpls create
    far-end 1.1.1.4
    lsp "to-node-4-lsp-1"
    keep-alive
    shutdown
  exit
  no shutdown
  exit
  sdp 3 mpls create // Etcetera
  pw-template 1 create
    vc-type vlan
  exit
  oper-group "og-name-et" create
  exit
  oper-group "og-name-et100" create
  exit
  epipe 1 customer 1 create
    service-mtu 500
  bgp
    route-distinguisher 65000:1
    route-target export target:65000:1 import target:65000:1
  exit
  site "site-1" create
    site-id 1
    sap 1/1/2:1.1
    boot-timer 100
    site-activation-timer 2
    no shutdown
exit
endpoint "x" create
exit
endpoint "y" create
exit
sap 1/1/2:1.1 endpoint "x" create
  eth-cfm
    mep 130 domain 100 association 2 direction down
      fault-propagation-enable use-if-tlv
      ccm-enable
      no shutdown
    exit
  exit
oper-group "og-name-et"
exit
spoke-sdp 2:1 endpoint "y" create
  precedence primary
  no shutdown
exit
spoke-sdp 3:1 endpoint "y" create
  precedence 2
  no shutdown
exit
no shutdown
exit
epipe 100 customer 1 create
  description "Epipe 100 in separate opergroup"
  service-mtu 500
  bgp
    route-distinguisher 65000:2
    route-target export target:65000:2 import target:65000:2
  exit
site "site-name-et100" create
  site-id 1101
  sap 1/1/4:1.100
  boot-timer 100
  site-activation-timer 2
  no shutdown
exit
endpoint "x" create
exit
endpoint "y" create
exit
sap 1/1/4:1.100 endpoint "x" create
  eth-cfm
    mep 131 domain 1 association 2 direction down
      fault-propagation-enable use-if-tlv
      ccm-enable
      no shutdown
    exit
  exit
oper-group "og-name-et100"
exit
spoke-sdp 2:2 vc-type vlan endpoint "y" create
  precedence 1
  no shutdown
exit
spoke-sdp 3:2 vc-type vlan endpoint "y" create
precedence 2
no shutdown
exit
no shutdown
exit

exit
#

Node-3: Using operational groups and Ethernet CFM per SAP
#

echo "Eth-CFM Configuration"
#

eth-cfm
domain 100 format none level 3
  association 2 format icc-based name "node-3-site-1-0"
    bridge-identifier 1
    exit
    ccm-interval 1
    remote-mepid 130
  exit
  association 2 format icc-based name "node-3-site-1-1"
    bridge-identifier 100
    exit
    ccm-interval 1
    remote-mepid 131
association 3 format icc-based name "node-3-site-2-0"
  bridge-identifier 1
  exit
  ccm-interval 1
  remote-mepid 120
association 3 format icc-based name "node-3-site-2-1"
  bridge-identifier 100
  exit
  ccm-interval 1
  remote-mepid 121
exit
exit
#--------------------------------------------------
# echo "Service Configuration"
#--------------------------------------------------

eth-tunnel 1
description "Eth Tunnel loadsharing mode QinQ example"
protection-type loadsharing
ethernet
encap-type qinq
exit
path 1
member 1/1/3
control-tag 1.1
eth-cfm
  mep 310 domain 100 association 2
  ccm-enable
  control-mep
  no shutdown
exit
exit
no shutdown
exit
eth-tunnel 2
description "Eth Tunnel QinQ"
revert-time 10
path 1
  precedence primary
  member 1/1/1
  control-tag 1.100
  eth-cfm
  mep 311 domain 100 association 2
  ccm-enable
  control-mep
  no shutdown
exit
exit
no shutdown
exit

#--------------------------------------------------
# echo "Ethernet Tunnel Configuration"
#--------------------------------------------------

eth-tunnel 2
description "Eth Tunnel QinQ"
revert-time 10
path 1
  precedence primary
  member 1/1/1
  control-tag 1.100
  eth-cfm
  mep 320 domain 100 association 3
  ccm-enablepath
  control-mep
  no shutdown
exit
exit
no shutdown
exit
path 2
  member 1/1/2
  control-tag 1.100
  eth-cfm
Configuration with Fate Sharing on Node-3

In this example the SAPs monitoring the operational groups do not need CFM if the corresponding SAP on the CE side is using fate sharing.

Node-1:

#--------------------------------------------------
echo "Service Configuration"  Oper-groups
#--------------------------------------------------
  service
customer 1 create
description "Default customer"
exit
sdp 2 mpls create
...
exit
pw-template 1 create
  vc-type vlan
exit
oper-group "og-name-et" create
exit
epipe 1 customer 1 create
  service-mtu 500
  bgp
    route-distinguisher 65000:1
    route-target export target:65000:1 import target:65000:1
exit
site "site-1" create
    site-id 1
    sap 1/1/2:1.1
    boot-timer 100
    site-activation-timer 2
    no shutdown
exit
endpoint "x" create
exit
endpoint "y" create
exit
sap 1/1/2:1.1 endpoint "x" create
eth-cfm
    mep 130 domain 100 association 1 direction down
    fault-propagation-enable use-if-tlv
    ccm-enable
    no shutdown
exit
exit
oper-group "og-name-et"
exit
spoke-sdp 2:1 endpoint "y" create
   precedence primary
   no shutdown
exit
spoke-sdp 3:1 endpoint "y" create
   precedence 2
   no shutdown
exit
no shutdown
exit
epipe 2 customer 1 create
   description "Epipe 2 in opergroup with Epipe 1"
   service-mtu 500
   bgp
       route-distinguisher 65000:2
       route-target export target:65000:2 import target:65000:2
   exit
   endpoint "x" create
   exit
   endpoint "y" create
   exit
   sap 1/1/2:1.2 endpoint "x" create
   monitor-oper-group "og-name-et"
   exit
   spoke-sdp 2:2 vc-type vlan endpoint "y" create
       precedence 1
       no shutdown
   exit
   spoke-sdp 3:2 vc-type vlan endpoint "y" create
       precedence 2
       no shutdown
   exit
   no shutdown
exit
exit
Node-3:

#--------------------------------------------------
echo "Eth-CFM Configuration"
#--------------------------------------------------
eth-cfm
   domain 100 format none level 3
   association 1 format icc-based name "node-3-site-1-0"
      bridge-identifier 1
      exit
      ccm-interval 1
      remote-mepid 130
      exit
   association 2 format icc-based name "node-3-site-2-0"
      bridge-identifier 2
      exit
      ccm-interval 1
      remote-mepid 120
      exit
   exit
   exit

#--------------------------------------------------
echo "Service Configuration"
#--------------------------------------------------
eth-tunnel 2
   description "Eth Tunnel loadsharing mode QinQ example"
   protection-type loadsharing
   ethernet
      encap-type qinq
      exit
path 1
   member 1/1/1
   control-tag 1.1
   eth-cfm
      mep 310 domain 100 association 1
      ccm-enable
      control-mep
      no shutdown
      exit
   exit
   no shutdown
   exit
path 2
   member 1/1/2
   control-tag 1.1
   eth-cfm
      mep 320 domain 100 association 2
      ccm-enablepath
      control-mep
      no shutdown
      exit
   exit
   no shutdown
   exit
   exit
#--------------------------------------------------
echo "Service Configuration"
#--------------------------------------------------
  service
epipe 1 customer 1 create
  sap 1/10/1:1 create
  exit
  sap eth-tunnel-1 create
  exit
  no shutdown
  exit
#--------------------------------------------------
  echo "Service Configuration for a shared fate Ethernet Tunnel"
  #--------------------------------------------------
epipe 2 customer 1 create
  sap 1/10/2:3 create
  exit
  sap eth-tunnel-1:2 create
  eth-tunnel
    path 1 tag 1.2
    path 2 tag 1.2
    exit
  exit
  no shutdown
  exit
Access Node Resilience Using MC-LAG and Pseudowire Redundancy

Figure 55 shows the use of both Multi-Chassis Link Aggregation (MC-LAG) in the access network and pseudowire redundancy in the core network to provide a resilient end-to-end VLL service to the customers.

In this application, a new pseudowire status bit of active or standby indicates the status of the SAP in the MC-LAG instance in the SR-Series aggregation node. All spoke SDPs are of secondary type and there is no use of a primary pseudowire type in this mode of operation. Node A is in the active...
state according to its local MC-LAG instance and thus advertises active status notification messages to both its peer pseudowire nodes, for example, nodes C and D. Node D performs the same operation. Node B is in the standby state according to the status of the SAP in its local MC-LAG instance and thus advertises standby status notification messages to both nodes C and D. Node C performs the same operation.

An SR-Series node selects a pseudowire as the active path for forwarding packets when both the local pseudowire status and the received remote pseudowire status indicate active status. However, an SR-Series device in standby status according to the SAP in its local MC-LAG instance is capable of processing packets for a VLL service received over any of the pseudowires which are up. This is to avoid black holing of user traffic during transitions. The SR-Series standby node forwards these packets to the active node by the Inter-Chassis Backup pseudowire (ICB pseudowire) for this VLL service. An ICB is a spoke SDP used by a MC-LAG node to backup a MC-LAG SAP during transitions. The same ICB can also be used by the peer MC-LAG node to protect against network failures causing the active pseudowire to go down.

Note that at configuration time, the user specifies a precedence parameter for each of the pseudowires which are part of the redundancy set as described in the application in VLL Resilience with Two Destination PE Nodes on page 286. An SR-Series node uses this to select which pseudowire to forward packet to in case both pseudowires show active/active for the local/remote status during transitions.

Only VLL service of type Epipe is supported in this application. Furthermore, ICB spoke SDP can only be added to the SAP side of the VLL cross-connect if the SAP is configured on a MC-LAG instance.
VLL Resilience for a Switched Pseudowire Path

Figure 56 illustrates the use of both pseudowire redundancy and pseudowire switching to provide a resilient VLL service across multiple IGP areas in a provider network.

Pseudowire switching is a method for scaling a large network of VLL or VPLS services by removing the need for a full mesh of T-LDP sessions between the PE nodes as the number of these nodes grows over time.

Like in the application in VLL Resilience with Two Destination PE Nodes on page 286, the T-PE1 node switches the path of a VLL to a secondary standby pseudowire in the case of a network side failure causing the VLL binding status to be DOWN or if T-PE2 notified it that the remote SAP went down. This application requires that pseudowire status notification messages generated by either a T-PE node or a S-PE node be processed and relayed by the S-PE nodes.

Note that it is possible that the secondary pseudowire path terminates on the same target PE as the primary, for example, T-PE2. This provides protection against network side failures but not against a remote SAP failure. When the target destination PE for the primary and secondary
pseudowires is the same, T-PE1 will normally not switch the VLL path onto the secondary pseudowire upon receipt of a pseudowire status notification indicating the remote SAP is down since the status notification is sent over both the primary and secondary pseudowires. However, the status notification on the primary pseudowire may arrive earlier than the one on the secondary pseudowire due to the differential delay between the paths. This will cause T-PE1 to switch the path of the VLL to the secondary standby pseudowire and remain there until the status notification is cleared. At that point in time, the VLL path is switched back to the primary pseudowire due to the revertive behavior operation. The path will not switch back to a secondary path when it becomes up even if it has a higher precedence than the currently active secondary path.
Pseudowire Redundancy Service Models

This section describes the various MC-LAG and pseudowire redundancy scenarios as well as the algorithm used to select the active transmit object in a VLL endpoint.

The redundant VLL service model is described in the following section, Redundant VLL Service Model.

Redundant VLL Service Model

In order to implement pseudowire redundancy, a VLL service accommodates more than a single object on the SAP side and on the spoke SDP side. Figure 57 illustrates the model for a redundant VLL service based on the concept of endpoints.

A VLL service supports by default two implicit endpoints managed internally by the system. Each endpoint can only have one object, a SAP or a spoke SDP.
In order to add more objects, up to two (2) explicitly named endpoints may be created per VLL service. The endpoint name is locally significant to the VLL service. They are referred to as endpoint 'X' and endpoint 'Y' as illustrated in Figure 57.

Note that Figure 57 is merely an example and that the “Y” endpoint can also have a SAP and/or an ICB spoke SDP. The following details the four types of endpoint objects supported and the rules used when associating them with an endpoint of a VLL service:

- **SAP** — There can only be a maximum of one SAP per VLL endpoint.
- **Primary spoke SDP** — The VLL service always uses this pseudowire and only switches to a secondary pseudowire when it is down. The VLL service switches the path to the primary pseudowire when it is back up. The user can configure a timer to delay reverting back to primary or to never revert. There can only be a maximum of one primary spoke SDP per VLL endpoint.
- **Secondary spoke SDP** — There can be a maximum of four secondary spoke SDP per endpoint. The user can configure the precedence of a secondary pseudowire to indicate the order in which a secondary pseudowire is activated.
- **Inter-Chassis Backup (ICB) spoke SDP** — Special pseudowire used for MC-LAG and pseudowire redundancy application. Forwarding between ICBs is blocked on the same node. The user has to explicitly indicate the spoke SDP is actually an ICB at creation time.

A VLL service endpoint can only use a single active object to transmit at any given time but can receive from all endpoint objects.

An explicitly named endpoint can have a maximum of one SAP and one ICB. Once a SAP is added to the endpoint, only one more object of type ICB spoke SDP is allowed. The ICB spoke SDP cannot be added to the endpoint if the SAP is not part of a MC-LAG instance. Conversely, a SAP which is not part of a MC-LAG instance cannot be added to an endpoint which already has an ICB spoke SDP.

An explicitly named endpoint, which does not have a SAP object, can have a maximum of four spoke SDPs and can include any of the following:

- A single primary spoke SDP.
- One or many secondary spoke SDPs with precedence.
- A single ICB spoke SDP.
T-LDP Status Notification Handling Rules

Referring to Figure 57 on page 319 as a reference, the following are the rules for generating, processing, and merging T-LDP status notifications in VLL service with endpoints. Note that any allowed combination of objects as specified in Redundant VLL Service Model on page 319 can be used on endpoints “X” and “Y”. The following sections refer to the specific combination objects in Figure 57 as an example to describe the more general rules.

Processing Endpoint SAP Active/Standby Status Bits

The advertised admin forwarding status of active/standby reflects the status of the local LAG SAP in MC-LAG application. If the SAP is not part of a MC-LAG instance, the forwarding status of active is always advertised.

When the SAP in endpoint “X” is part of a MC-LAG instance, a node must send T-LDP forwarding status bit of “SAP active/standby” over all “Y” endpoint spoke SDPs, except the ICB spoke SDP, whenever this status changes. The status bit sent over the ICB is always zero (active by default).

When the SAP in endpoint “X” is not part of a MC-LAG instance, then the forwarding status sent over all “Y” endpoint spoke SDP's should always be set to zero (active by default).

Processing and Merging

Endpoint “X” is operationally up if at least one of its objects is operationally up. It is down if all its objects are operationally down.

If the SAP in endpoint “X” transitions locally to the down state, or received a SAP down notification by SAP-specific OAM signal, the node must send T-LDP SAP down status bits on the “Y” endpoint ICB spoke SDP only. Note that Ethernet SAP does not support SAP OAM protocol. All other SAP types cannot exist on the same endpoint as an ICB spoke SDP since non Ethernet SAP cannot be part of a MC-LAG instance.

If the ICB spoke SDP in endpoint “X” transitions locally to down state, the node must send T-LDP SDP-binding down status bits on this spoke SDP.

If the ICB spoke SDP in endpoint “X” received T-LDP SDP-binding down status bits or pseudowire not forwarding status bits, the node saves this status and takes no further action. The saved status is used for selecting the active transmit endpoint object.

If all objects in endpoint “X” transition locally to down state, and/or received a SAP down notification by remote T-LDP status bits or by SAP specific OAM signal, and/or received status
bits of SDP-binding down, and/or received status bits of pseudowire not forwarding, the node must send status bits of SAP down over all “Y” endpoint spoke SDPs, including the ICB.

Endpoint “Y” is operationally up if at least one of its objects is operationally up. It is down if all its objects are operationally down.

If a spoke SDP in endpoint “Y”, including the ICB spoke SDP, transitions locally to down state, the node must send T-LDP SDP-binding down status bits on this spoke SDP.

If a spoke SDP in endpoint “Y”, including the ICB spoke SDP, received T-LDP SAP down status bits, and/or received T-LDP SDP-binding down status bits, and/or received status bits of pseudowire not forwarding, the node saves this status and takes no further action. The saved status is used for selecting the active transmit endpoint object.

If all objects in endpoint “Y”, except the ICB spoke SDP, transition locally to down state, and/or received T-LDP SAP down status bits, and/or received T-LDP SDP-binding down status bits, and/or received status bits of pseudowire not forwarding, the node must send status bits of SDP-binding down over the “X” endpoint ICB spoke SDP only.

If all objects in endpoint “Y” transition locally to down state, and/or received T-LDP SAP down status bits, and/or received T-LDP SDP-binding down status bits, and/or received status bits of pseudowire not forwarding, the node must send status bits of SDP-binding down over the “X” endpoint ICB spoke SDP, and must send a SAP down notification on the “X” endpoint SAP by the SAP specific OAM signal if applicable. An Ethernet SAP does not support signaling status notifications.
BGP Virtual Private Wire Service (VPWS)

BGP Virtual Private Wire Service (VPWS) is a point-to-point L2 VPN service based on RFC 6624 (Layer 2 Virtual Private Networks using BGP for Auto-Discovery and Signaling) which in turn uses the BGP pseudowire signaling concepts from RFC 4761, Virtual Private LAN Service Using BGP for Auto-Discovery and Signaling.

Single-Homed BGP VPWS

A single-homed BGP VPWS service is implemented as an Epipe connecting a SAP and a BGP signaled pseudowire, maintaining the Epipe properties such as no MAC learning. The pseudowire data plane uses a two label stack, the inner label is derived from the BGP signaling and identifies the Epipe service while the outer label is the tunnel label of an LSP transporting the traffic between the two end systems.

Figure 58 shows how this service would be used to provide a virtual lease-line service across an MPLS network between two sites, A and B.

An Epipe is configured on PE1 and PE2 with BGP VPWS enabled. PE1 and PE2 are connected to site A and B, respectively, each using a SAP. The interconnection between the two PEs is achieved through a pseudowire which is signaled using BGP VPWS updates over a given tunnel LSP.
Dual-Homed BGP VPWS

A BGP-VPWS service can benefit from dual-homing, as described in draft-ietf-l2vpn-vpls-multihoming-03. When using dual-homing, two PEs connect to a site with one PE being the designated forwarder for the site and the other blocking its connection to the site. On failure of the active PE, its pseudowire or its connection to the site, the other PE becomes the designated forwarder and unblocks its connection to the site.

Single Pseudowire Example:

A pseudowire is established between the designated forwarder of the dual-homed PEs and the remote PE. If a failure causes a change in the designated forwarder, the pseudowire is deleted and re-established between the remote PE and the new designated forwarder. This topology requires that the VE IDs on the dual-homed PEs are set to the same value.

An example is shown in Figure 59.

![Figure 59: Dual-Homed BGP VPWS with Single Pseudowire](image)

An Epipe with BGP VPWS enabled is configured on each PE. Site A is dual-homed to PE1 and PE2 with the remote PE, PE3, connecting to site B. An Epipe service is configured on each PE in which there is a SAP connecting to the local site.

The pair of dual-homed PEs perform a designated forwarder election, which is influenced by BGP route selection, the site state, and by configuring the site-preference. A site will only be eligible to be the designated forwarder if it is up (note that the site state will be down if there is no pseudowire established or if the pseudowire is in an oper down state). The winner, for example PE1, becomes the active switch for traffic sent to and from site A, while the loser blocks its
connection to site A. Pseudowires are signaled using BGP from PE1 and PE2 to PE3 but only from PE3 to the designated forwarder in the opposite direction (thereby only one bi-directional pseudowire is established). There is no pseudowire between PE1 and PE2; this is achieved by configuration.

Traffic is sent and received traffic on the pseudowire connected between PE3 and the designated forwarder, PE1.

If the site state is oper down then both the D and CSV bits (see below for more details) are set in the BGP-VPWS update which will cause the remote PE to use the pseudowire to the new designated forwarder.

Active/Standby Pseudowire Example:

Pseudowires are established between the remote PE and each dual-homed PE. The remote PE can receive traffic on either pseudowire but will only send on the one to the designated forwarder. This creates an active/standby pair of pseudowires. At most one standby pseudowire will be established; this being determined using the tie-breaking rules defined in the multi-homing draft. This topology requires each PE to have a different VE ID.

A dual-homed topology example is shown in Figure 60.

Figure 60: Dual-homed BGP VPWS with Active/Standby Pseudowires

An Epipe with BGP VPWS enabled is configured on each PE. Site A is dual-homed to PE1 and PE2 with the remote PE, PE3, connecting to site B. An Epipe service is configured on each PE in which there is a SAP connecting to the local site.
The pair of dual-homed PEs perform a designated forwarder election, which is influenced by configuring the site-preference. The winner, PE1 (based on its higher site-preference) becomes the active switch for traffic sent to and from site A, while the loser, PE2, blocks its connection to site A. Pseudowires are signaled using BGP between PE1 and PE3, and between PE2 and PE3. There is no pseudowire between PE1 and PE2; this is achieved by configuration. The active/standby pseudowires on PE3 are part of an endpoint automatically created in the Epipe service.

Traffic is sent and received traffic on the pseudowire connected to the designated forwarder, PE1.

---

**Pseudowire Signaling**

The BGP signaling mechanism used to establish the pseudowires is described in the BGP VPWS with the following differences:

- As stated in Section 3 of RFC 6624, there are two modifications of messages when compared to RFC 4761.
  - The Encaps Types supported in the associated extended community.
  - The addition of a circuit status vector sub-TLV at the end of the VPWS NLRI.
- The Control Flags and VPLS preference in the associated extended community are based on draft-ietf-l2vpn-vpls-multihoming-03.

Figure 61 displays the format of the BGP VPWS update extended community:

```plaintext
+------------------------------------+
| Extended community type (2 octets) |
+------------------------------------+
| Encaps Type (1 octet)              |
+------------------------------------+
| Control Flags (1 octet)            |
+------------------------------------+
| Layer-2 MTU (2 octet)              |
+------------------------------------+
| VPLS Preference (2 octets)         |
+------------------------------------+
```

**Figure 61: BGP VPWS Update Extended Community Format**

- Extended community type — The value allocated by IANA for this attribute is 0x800A
- Encaps Type — Encapsulation type, identifies the type of pseudowire encapsulation. Ethernet VLAN (4) and Ethernet Raw mode (5), as described in RFC 4448, are the only values supported. If there is a mismatch between the Encaps Type signaled and the one received, the pseudowire is created but with the oper state down.
- Control Flags — Control information regarding the pseudowires, see below for details.
• Layer-2 MTU is the Maximum Transmission Unit to be used on the pseudowires. If the received Layer-2 MTU is zero no MTU check is performed and the related pseudowire is established. If there is a mismatch between the local service-mtu and the received Layer-2 MTU the pseudowire is created with the oper state down and a MTU/Parameter mismatch indication.

• VPLS preference – VPLS preference has a default value of zero for BGP-VPWS updates sent by the system, indicating that it is not in use. If the site-preference is configured, its value is used for the VPLS preference and is also used in the local designated forwarder election. On receipt of a BGP VPWS update containing a non-zero value, it will be used to determine to which system the pseudowire is established as part of the VPWS update process tie-breaking rules. The BGP local preference of the BGP VPWS update sent by the system is set to the same value as the VPLS preference if the latter is non-zero, as required by the draft (as long as the D bit in the extended community is not set to 1). Consequently, attempts to change the BGP local preference when exporting a BGP VPWS update with a non-zero VPLS preference will be ignored. This prevents the updates being treated as malformed by the receiver of the update.

The control flags are described below:

```
 0 1 2 3 4 5 6 7
+--------+
|D|A|F|Z|Z|Z|C|S| (Z = MUST Be Zero)
+--------+
```

The following bits in the Control Flags are defined:

D — Access circuit down indicator from draft-kothari-l2vpn-auto-site-id-01. D is 1 if all access circuits are down, otherwise D is 0.

A — Automatic site id allocation, which is not supported. This is ignored on receipt and set to 0 on sending.

F — MAC flush indicator. This is not supported as it relates to a VPLS service. This is set to 0 and ignored on receipt.

C — Presence of a control word. Control word usage is not supported. This is set to 0 on sending (control word not present) and if a non-zero value is received (indicating a control word is required) the pseudowire will not be created.

S — Sequenced delivery. Sequenced delivery is not supported. This is set to 0 on sending (no sequenced delivery) and if a non-zero value is received (indicating sequenced delivery required) the pseudowire will not be created.

The BGP VPWS NLRI is based on that defined for BGP VPLS but is extended with a circuit status vector, as shown in Figure 62.
The VE ID value is configured within each BGP VPWS service, the label base is chosen by the system and the VE block offset corresponds to the remote VE ID as a VE block size of 1 is always used.

The circuit status vector is encoded as a TLV as shown in Figure 63.

The circuit status vector is used to indicate the status of both the SAP and the status of the spoke-SDP within the local service. As the VE block size used is 1, the most significant bit in the circuit status vector TLV value will be set to 1 if either the SAP or spoke-SDP is down, otherwise it will be set to 0.
A pseudowire will be established when a BGP VPWS update is received which matches the service configuration, specifically the configured route-targets and remote VE ID. If multiple matching updates are received, the system to which the pseudowire is established is determined by the tie-breaking rules, as described in draft-ietf-l2vpn-vpls-multihoming-03.

Traffic will be sent on the active pseudowire connected to the remote designated forwarder. It can be received on either the active or standby pseudowire, though no traffic should be received on the standby pseudowire as the SAP on the non-designated forwarder should be blocked.
BGP VPWS Configuration Procedure

In addition to configuring the associated BGP and MPLS infrastructure, the provisioning of a BGP VPWS service requires:

- Configure BGP Route Distinguisher, Route Target
  → Updates are accepted into the service only if they contain the configured import route-target

- Configure a binding to the pseudowire template
  → Multiple pseudowire template bindings can be configure with their associated route-targets used to control which is applied

- Configure the SAP

- Configure the name of the local VE and its associate VE ID

- Configure the name of the remote VE and its associated VE ID

- For a dual-homed PE
  → Enable the site
  → Configure the site with non-zero site-preference

- For a remote PE
  → Up to two remove VE names and associated VE IDs can be configured

- Enable BGP VPWS
Use of Pseudowire Template for BGP VPWS

The pseudowire template concept used for BGP AD is re-used for BGP VPWS to dynamically instantiate pseudowire (SDP-bindings) and the related SDP (provisioned or automatically instantiated).

The settings for the L2-Info extended community in the BGP Update sent by the system are derived from the pseudowire-template attributes. The following rules apply:

- If multiple pseudowire-template-bindings (with or without import-rt) are specified for the VPWS instance, the first (numerically lowest id) pseudowire-template entry will be used.
- Both Ethernet VLAN and Ethernet Raw Mode encaps types are supported; these are selected by configuring the vc-type in the pseudowire template to be either vlan or ether, respectively. The default is ether.
  - The same value must be used by the remote BGP VPWS instance to ensure the related pseudowire will come up
- Layer 2 MTU – derived from service vpls service-mtu parameter.
  - The same value must be used by the remote BGP VPWS instance to ensure the related pseudowire will come up.
- Control Flag C – always 0.
- Control Flag S – always 0.

On reception the values of the parameters in the L2-Info extended community of the BGP update are compared with the settings from the corresponding pseudowire-template. The following steps are used to determine the local pseudowire-template:

- The route-target values are matched to determine the pseudowire-template.
- If no matches are found from the previous step, the first (numerically lowest id) pw-template-binding configured without an import-rt is used.
- If the values used for encaps type or Layer 2 MTU do not match the pseudowire is created but with the oper state down.
  - In order to interoperate with existing implementations if the received MTU value = 0, then MTU negotiation does not take place; the related pseudowire is setup ignoring the MTU.
- If the values of the C/S flags are not zero the pseudowire is not created.
The following pseudowire template parameters is are supported when applied within a BGP VPWS service, the remainder are ignored:

```
configure service pw-template policy-id [use-provisioned-sdp] [create]
    accounting-policy acct-policy-id
    [no] collect-stats
    egress
      filter ipv6 ipv6-filter-id
      filter ip ip-filter-id
      filter mac mac-filter-id
      no filter [ip ip-filter-id] [mac mac-filter-id] [ipv6 ipv6-filter-id]
      qos [network-policy-id port-redirect-group queue-group-name instance instance-id]
      no qos [network-policy-id]
    [no] force-vlan-vc-forwarding
    hash-label [signal-capability]
    no hash-label
    ingress
      filter ipv6 ipv6-filter-id
      filter ip ip-filter-id
      filter mac mac-filter-id
      no filter [ip ip-filter-id] [mac mac-filter-id] [ipv6 ipv6-filter-id]
      qos [network-policy-id port-redirect-group queue-group-name instance instance-id]
      no qos [network-policy-id]
    [no] sdp-exclude
    [no] sdp-include
    vc-type {ether|vlan}
    vlan-vc-tag vlan-id
    no vlan-vc-tag
```

The **use-provisioned-sdp** command is permitted when creating the pseudowire template if a pre-provisioned SDP is to be used. Pre-provisioned SDPs must be configured whenever RSVP or BGP signaled transport tunnels are used.

The **tools perform** command can be used similarly as for BGP-AD to force the application of changes in pseudowire-template using the format described below:

```
tools perform service [id service-id] eval-pw-template policy-id [allow-service-impact]
```
Use of Endpoint for BGP VPWS

An Endpoint is required on a remote PE connecting to two dual-homed PEs to associate the active/standby pseudowires with the Epipe service. An endpoint is automatically created within the Epipe service such that active/standby pseudowires are associated with that endpoint. The creation of the endpoint occurs when bgp-vpws is enabled (and deleted when it is disabled) and so will exist in both a single and dual homed scenario (this simplifies converting a single homed service to a dual-homed service). The naming convention used is _tmmx_BgpVpws-x, where x is the service identifier. The automatically created endpoint has the default parameter values, although all are ignored in a BGP-VPWS service with the description field being defined by the system.

Note that the command:

```
tools perform service id <service-id> endpoint <endpoint-name> force-switchover
```

will have no affect on an automatically created VPWS endpoint.
VLL Service Considerations

This section describes various of the general 7950 SR service features and any special capabilities or considerations as they relate to VLL services.

SDPs

The most basic SDPs must have the following:

- A locally unique SDP identification (ID) number.
- The system IP address of the originating and far-end routers.
- An SDP encapsulation type, either GRE or MPLS.
The simple three-node network described in Figure 65 shows two MPLS SDPs and one GRE SDP defined between the nodes. These SDPs connect VPLS1 and VPLS2 instances that are defined in the three nodes. With this feature the operator will have local CLI based as well as SNMP based statistics collection for each VC used in the SDPs. This will allow for traffic management of tunnel usage by the different services and with aggregation the total tunnel usage.
SAP Encapsulations and Pseudowire Types

The Epipe service is designed to carry Ethernet frame payloads, so it can provide connectivity between any two SAPs that pass Ethernet frames. The following SAP encapsulations are supported on the 7950 SR Epipe service:

- Ethernet null
- Ethernet dot1q
- QinQ

Note that while different encapsulation types can be used, encapsulation mismatching can occur if the encapsulation behavior is not understood by connecting devices and are unable to send and receive the expected traffic. For example if the encapsulation type on one side of the Epipe is dot1q and the other is null, tagged traffic received on the null SAP will be double tagged when it is transmitted out of the Dot1q SAP.
QoS Policies

When applied to SR-OS Epipe services, service ingress QoS policies only create the unicast queues defined in the policy. The multipoint queues are not created on the service.

With Epipe services, egress QoS policies function as with other services where the class-based queues are created as defined in the policy. Note that both Layer 2 or Layer 3 criteria can be used in the QoS policies for traffic classification in a service.

Filter Policies

SR-OS Epipe services can have a single filter policy associated on both ingress and egress. Both MAC and IP filter policies can be used on Epipe services.

MAC Resources

Epipe services are point-to-point layer 2 VPNs capable of carrying any Ethernet payloads. Although an Epipe is a Layer 2 service, the SR-OS Epipe implementation does not perform any MAC learning on the service, so Epipe services do not consume any MAC hardware resources.
Configuring a VLL Service with CLI

This section provides information to configure Virtual Leased Line (VLL) services using the command line interface.

Topics in this section include:

- Basic Configurations on page 340
- Common Configuration Tasks on page 340
  - Configuring VLL Components on page 341
    - Creating an Epipe Service on page 342
    - Using Spoke SDP Control Words on page 353
  - Configuring Pseudowire Scenarios
    - Pseudowire Configuration Notes on page 354
    - Configuring Two VLL Paths Terminating on T-PE2 on page 355
    - Configuring VLL Resilience on page 358
    - Configuring VLL Resilience for a Switched Pseudowire Path on page 359
    - Configuring BGP Virtual Private Wire Service (VPWS) on page 361
- Service Management Tasks on page 369
  - Epipe:
    - Modifying Epipe Service Parameters on page 370
    - Disabling an Epipe Service on page 370
    - Re-Enabling an Epipe Service on page 371
    - Deleting an Epipe Service on page 371
Basic Configurations

- Creating an Epipe Service on page 342
- Using Spoke SDP Control Words on page 353
- Pseudowire Configuration Notes on page 354
  - Configuring Two VLL Paths Terminating on T-PE2 on page 355
  - Configuring VLL Resilience on page 358
  - Configuring VLL Resilience for a Switched Pseudowire Path on page 359

Common Configuration Tasks

This section provides a brief overview of the tasks that must be performed to configure the VLL services and provides the CLI commands.

- Associate the service with a customer ID.
- Define SAP parameters
  - Optional - select egress and ingress QoS and/or scheduler policies (configured in the \texttt{config>qos} context).
  - Optional - select accounting policy (configured in the \texttt{config>log} context).
- Define spoke SDP parameters.
- Enable the service.
Configuring VLL Components

This section provides VLL configuration examples for the VLL services:

- Creating an Epipe Service on page 342
  → Configuring Epipe SAP Parameters on page 343
    - Local Epipe SAPs on page 344
    - Distributed Epipe SAPs on page 346
    - Configuring Ingress and Egress SAP Parameters on page 349
Creating an Epipe Service

Use the following CLI syntax to create an Epipe service.

**CLI Syntax:**
```
config>service# epipe service-id [customer customer-id] [vpn vpn-id] [vc-switching]
        description description-string
        no shutdown
```

The following displays an Epipe configuration example:

```
A:ALA-1>config>service# info
-------------------------------------------
... epipe 500 customer 5 vpn 500 create
description "Local epipe service"
no shutdown
exit
-------------------------------------------
A:ALA-1>config>service#
```
Configuring Epipe SAP Parameters

A default QoS policy is applied to each ingress and egress SAP. Additional QoS policies can be configured in the `config>qos` context. Filter policies are configured in the `config>filter` context and explicitly applied to a SAP. There are no default filter policies.

Use the following CLI syntax to create:

- Local Epipe SAPs on page 344
- Distributed Epipe SAPs on page 346

**CLI Syntax:**
```
config>service# epipe service-id [customer customer-id]
sap sap-id [endpoint endpoint-name]
sap sap-id [no-endpoint]
  accounting-policy policy-id
  collect-stats
  description description-string
  no shutdown
  egress
  filter {ip ip-filter-name | mac mac-filter-name}
  qos sap-egress-policy-id
  scheduler-policy scheduler-policy-name
  ingress
  filter {ip ip-filter-name | mac mac-filter-name}
  match-qinq-dot1p {top|bottom}
  qos policy-id
  scheduler-policy scheduler-policy-name
```
Local Epipe SAPs

To configure a basic local Epipe service, enter the sap sap-id command twice with different port IDs in the same service configuration.

By default, QoS policy ID 1 is applied to ingress and egress service SAPs. Existing filter policies or other existing QoS policies can be associated with service SAPs on ingress and egress ports.

An existing scheduler policy can be applied to ingress and egress SAPs to be used by the SAP queues. The schedulers comprising the policy are created at the time the scheduler policy is applied to the SAP. If any orphaned queues (queues with a non-existent local scheduler defined) exist on a SAP and the policy application creates the required scheduler, the status on the queue becomes non-orphaned at this time.

Ingress and Egress SAP parameters can be applied to local and distributed Epipe service SAPs.

This example displays the SAP configurations for local Epipe service 500 on SAP 1/1/2 and SAP 1/1/3 on ALA-1.

```
A:ALA-1>config>service# epipe 500 customer 5 create
config>service>epipe$ description "Local epipe service"
config>service>epipe# sap 1/1/2:0 create
config>service>epipe>.sap? ingress
config>service>epipe> sap>ingress# qos 20
config>service>epipe> sap>ingress# filter ip 1
config>service>epipe> sap>egress
config>service>epipe> sap>egress# qos 20
config>service>epipe> sap>egress# scheduler-policy test1
config>service>epipe> sap# no shutdown
config>service>epipe> sap# exit

config>service>epipe# sap 1/1/3:0 create
config>service>epipe> sap# ingress
config>service>epipe> sap>ingress# qos 555
config>service>epipe> sap>ingress# filter ip 1
config>service>epipe> sap>egress
config>service>epipe> sap>egress# qos 627
config>service>epipe> sap>egress# scheduler-policy alpha
config>service>epipe> sap# no shutdown
config>service>epipe> sap# exit
```

Table 5: Supported SAP Types

<table>
<thead>
<tr>
<th>Uplink Type</th>
<th>Svc SAP Type</th>
<th>Cust. VID</th>
<th>Access SAPs</th>
<th>Network SAPs</th>
</tr>
</thead>
<tbody>
<tr>
<td>L2</td>
<td>Null-star</td>
<td>N/A</td>
<td>Null, dot1q</td>
<td>Q.*</td>
</tr>
<tr>
<td>L2</td>
<td>Dot1q</td>
<td>N/A</td>
<td>Dot1q</td>
<td>Q.*</td>
</tr>
<tr>
<td>L2</td>
<td>Dot1q-preserve</td>
<td>X</td>
<td>Dot1q (encap = X)</td>
<td>Q1.Q2 (where Q2 = X)</td>
</tr>
</tbody>
</table>

To configure a basic local Epipe service, enter the sap sap-id command twice with different port IDs in the same service configuration.

By default, QoS policy ID 1 is applied to ingress and egress service SAPs. Existing filter policies or other existing QoS policies can be associated with service SAPs on ingress and egress ports.

An existing scheduler policy can be applied to ingress and egress SAPs to be used by the SAP queues. The schedulers comprising the policy are created at the time the scheduler policy is applied to the SAP. If any orphaned queues (queues with a non-existent local scheduler defined) exist on a SAP and the policy application creates the required scheduler, the status on the queue becomes non-orphaned at this time.

Ingress and Egress SAP parameters can be applied to local and distributed Epipe service SAPs.

This example displays the SAP configurations for local Epipe service 500 on SAP 1/1/2 and SAP 1/1/3 on ALA-1.
The following example displays the local Epipe configuration:

```
A:ALA-1>config>service# info
----------------------------------------------
...  
epipe 500 customer 5 vpn 500 create
    description "Local epipe service"
    sap 1/1/2:0 create
        ingress
            qos 20
            filter ip 1
        exit
    egress
        scheduler-policy "test1"
            qos 20
        exit
    exit
    sap 1/1/3:0 create
        ingress
            qos 555
            filter ip 1
        exit
    egress
        scheduler-policy "alpha"
            qos 627
        exit
    exit
    no shutdown
exit
----------------------------------------------
A:ALA-1>config>service# 
```
Distributed Epipe SAPs

To configure a distributed Epipe service, you must configure service entities on the originating and far-end nodes. You should use the same service ID on both ends (for example, Epipe 5500 on ALA-1 and Epipe 5500 on ALA-2). The `spoke-sdp sdp-id:vc-id` must match on both sides. A distributed Epipe consists of two SAPs on different nodes.

By default, QoS policy ID 1 is applied to ingress and egress service SAPs. Existing filter policies or other existing QoS policies can be associated with service SAPs on ingress and egress.

An existing scheduler policy can be applied to ingress and egress SAPs to be used by the SAP queues. The schedulers comprising the policy are created at the time the scheduler policy is applied to the SAP. If any orphaned queues (queues with a non-existent local scheduler defined) exist on a SAP and the policy application creates the required scheduler, the status on the queue becomes non-orphaned at this time.

Ingress and egress SAP parameters can be applied to local and distributed Epipe service SAPs.

For SDP configuration information, see Configuring an SDP on page 87. For SDP binding information, see Configuring SDP Bindings on page 350.

This example configures a distributed service between ALA-1 and ALA-2.

```
A:ALA-1>epipe 5500 customer 5 create
config>service>epipe$ description "Distributed epipe service to east coast"
config>service>epipe# sap 221/1/3:21 create
config>service>epipe>.sap# ingress
config>service>epipe>.sap>ingress# qos 555
config>service>epipe>.sap>ingress# filter ip 1
config>service>epipe>.sap>ingress# exit
config>service>epipe>.sap# egress
config>service>epipe>.sap>egress# qos 627
config>service>epipe>.sap>egress# scheduler-policy alpha
config>service>epipe>.sap>egress# exit
config>service>epipe>.sap# no shutdown
config>service>epipe>

A:ALA-2>config>service$ epipe 5500 customer 5 create
config>service>epipe$ description "Distributed epipe service to west coast"
config>service>epipe# sap 441/1/4:550 create
config>service>epipe>.sap# ingress
config>service>epipe>.sap>ingress# qos 654
config>service>epipe>.sap>ingress# filter ip 1020
config>service>epipe>.sap>ingress# exit
config>service>epipe>.sap# egress
config>service>epipe>.sap>egress# qos 432
config>service>epipe>.sap>egress# filter ip 6
config>service>epipe>.sap>egress# scheduler-policy test1
config>service>epipe>.sap>egress# exit
config>service>epipe>.sap# no shutdown
config>service>epipe>
```
The following example displays the SAP configurations for ALA-1 and ALA-2:

A:ALA-1>config>service# info
----------------------------------------------
... epipe 5500 customer 5 vpn 5500 create
    description "Distributed epipe service to east coast"
    sap 221/1/3:21 create
        ingress
            qos 555
            filter ip 1
            exit
        egress
            scheduler-policy "alpha"
            qos 627
            exit
            exit
    exit
    exit
    exit
    ...
----------------------------------------------
A:ALA-1>config>service#

A:ALA-2>config>service# info
----------------------------------------------
... epipe 5500 customer 5 vpn 5500 create
    description "Distributed epipe service to west coast"
    sap 441/1/4:550 create
        ingress
            qos 654
            filter ip 1020
            exit
        egress
            scheduler-policy "test1"
            qos 432
            filter ip 6
            exit
            exit
    exit
    ...
----------------------------------------------
A:ALA-2>config>service#
PBB Epipe Configuration

The following example displays the PBB Epipe configuration:

*A:Wales-1>config>service>epipe# info
-----------------------------------------------------------------------
... description "Default epipe description for service id 20000"
    pbb-tunnel 200 backbone-dest-mac 00:03:fa:15:d3:a8 isid 20000
    sap 1/1/2:1.1 create
        description "Default sap description for service id 20000"
            ingress
                filter mac 1
            exit
        exit
    no shutdown
-----------------------------------------------------------------------
*A:Wales-1>config>service>epipe#

CLI Syntax:   configure service vpls 200 customer 1 b-vpls create

*A:Wales-1>config>service>vpls# info
-----------------------------------------------------------------------
... service-mtu 2000
    fdb-table-size 131071
    stp
    no shutdown
    exit
    sap 1/1/8 create
    exit
    sap 1/2/3:200 create
    exit
    mesh-sdp 1:200 create
    exit
    mesh-sdp 100:200 create
    exit
    mesh-sdp 150:200 create
    exit
    mesh-sdp 500:200 create
    exit
    no shutdown
-----------------------------------------------------------------------
*A:Wales-1>config>service>vpls#
Configuring Ingress and Egress SAP Parameters

By default, QoS policy ID 1 is applied to ingress and egress service SAPs. Existing filter policies or other existing QoS policies can be associated with service SAPs on ingress and egress ports.

An existing scheduler policy can be applied to ingress and egress SAPs to be used by the SAP queues. The schedulers comprising the policy are created at the time the scheduler policy is applied to the SAP. If any orphaned queues (queues with a non-existent local scheduler defined) exist on a SAP and the policy application creates the required scheduler, the status on the queue becomes non-orphaned at this time.

Ingress and egress SAP parameters can be applied to local and distributed Epipe service SAPs.

This example displays SAP ingress and egress parameters.

```
ALA-1(config-service) epipe 5500
  config-service>epipe# sap /1/3:21
  config-service>epipe>.sap# ingress
  config-service>epipe>.sap# ingress# qos 555
  config-service>epipe>.sap# ingress# filter ip 1
  config-service>epipe>.sap# ingress# exit
  config-service>epipe>.sap# egress
  config-service>epipe>.sap# egress# scheduler-policy alpha
  config-service>epipe>.sap# egress# qos 627
  config-service>epipe>.sap# egress# exit

The following example displays the Epipe SAP ingress and egress configuration:

A:ALA-1(config-service)#
----------------------------------------------
... epipe 5500 customer 5 vpn 5500 create
  description "Distributed epipe service to east coast"
  sap /1/3:21 create
    ingress
      qos 555
      filter ip 1
    exit
    egress
      scheduler-policy "alpha"
      qos 627
    exit
  exit
  spoke-sdp 2:123 create
    ingress
      vc-label 6600
    exit
    egress
      vc-label 5500
    exit
  exit
  no shutdown
  exit
----------------------------------------------
A:ALA-1(config-service)#
```
Configuring SDP Bindings

Figure 66 displays an example of a distributed Epipe service configuration between two routers, identifying the service and customer IDs, and the uni-directional SDPs required to communicate to the far-end routers.

A spoke SDP is treated like the equivalent of a traditional bridge “port” where flooded traffic received on the spoke SDP is replicated on all other “ports” (other spoke and mesh SDPs or SAPs) and not transmitted on the port it was received.

Use the following CLI syntax to create a spoke SDP binding with an Epipe service:

**CLI Syntax:**
```
config>service# epipe service-id [customer customer-id]
   spoke-sdp sdp-id:vc-id [vc-type {ether | vlan}]
       vlan-vc-tag 0..4094
       egress
           filter {ip ip-filter-id}
           vc-label egress-vc-label
       ingress
           filter {ip ip-filter-id}
           vc-label ingress-vc-label
   no shutdown
```
The following example displays the command usage to bind an Epipe service between ALA-1 and ALA-2. This example assumes the SAPs have already been configured (see Distributed Epipe SAPs on page 346).

A:ALA-1>config>service# epipe 5500

```
config>service>epipe# spoke-sdp 2:123
config>service>epipe>spoke-sdp# egress
config>service>epipe>spoke-sdp>egress# vc-label 5500
config>service>epipe>spoke-sdp>egress# exit
config>service>epipe>spoke-sdp# ingress
config>service>epipe>spoke-sdp>ingress# vc-label 6600
config>service>epipe>spoke-sdp>ingress# exit
config>service>epipe>spoke-sdp# no shutdown
```

ALA-2>config>service# epipe 5500

```
config>service>epipe# spoke-sdp 2:456
config>service>epipe>spoke-sdp# egress
config>service>epipe>spoke-sdp>egress# vc-label 6600
config>service>epipe>spoke-sdp>egress# exit
config>service>epipe>spoke-sdp# ingress
config>service>epipe>spoke-sdp>ingress# vc-label 5500
config>service>epipe>spoke-sdp>ingress# exit
config>service>epipe>spoke-sdp# no shutdown
```

This example displays the SDP binding for the Epipe service between ALA-1 and ALA-2:

```
A:ALA-1>config>service# info
----------------------------------------------
... epipe 5500 customer 5 vpn 5500 create
description "Distributed epipe service to east coast"
sap /1/3:21 create
  ingress
  qos 555
  filter ip 1
  exit
  egress
  scheduler-policy "alpha"
  qos 627
  exit
  exit
spoke-sdp 2:123 create
  ingress
  vc-label 6600
  exit
  egress
  vc-label 5500
  exit
  exit
  no shutdown
  exit
... ----------------------------------------------
A:ALA-1>config>service#
```

```
A:ALA-2>config>service# info
...----------------------------------------------
...----------------------------------------------
```
... exit
epipe 5500 customer 5 vpn 5500 create
description "Distributed epipe service to west coast"
sap 441/1/4:550 create
  ingress
    qos 654
    filter ip 1020
  exit
egress
  scheduler-policy "test1"
  qos 432
  filter ip 6
  exit
exit
spoke-sdp 2:456 create
  ingress
    vc-label 5500
  exit
  egress
    vc-label 6600
  exit
exit
no shutdown
exit
...
----------------------------------------------
A:ALA-2>config>service#
Using Spoke SDP Control Words

The control word command provides the option to add a control word as part of the packet encapsulation for PW types for which the control word is optional. The control word might be needed because when ECMP is enabled on the network, packets of a given pseudowire may be spread over multiple ECMP paths if the hashing router mistakes the PW packet payload for an IPv4 or IPv6 packet. This occurs when the first nibble following the service label corresponds to a value of 4 or 6.

The control word negotiation procedures described in Section 6.2 of RFC 4447 are not supported and therefore the service will only come up if the same C bit value is signaled in both directions. If a spoke-sdp is configured to use the control word but the node receives a label mapping message with a C-bit clear, the node releases the label with an “Illegal C-bit” status code per Section 6.1 of RFC 4447. As soon as the user enables control of the remote peer, the remote peer withdraws its original label and sends a label mapping with the C-bit set to 1 and the VLL service is up in both nodes.

When the control word is enabled, VCCV packets also include the VCCV control word. In that case, the VCCV CC type 1 (OAM CW) is signaled in the VCCV parameter in the FEC. If the control word is disabled on the spoke-sdp, then the Router Alert label is used. In that case, VCCV CC type 2 is signaled. Note that for a multi-segment pseudowire (MS-PW), the CC type 1 is the only supported and thus the control word must be enabled on the spoke-sdp to be able to use VCCV-ping and VCCV-trace.

The following displays a spoke SDP control word configuration example:

```
-Dut-B>config>service>epipe# info
----------------------------------------------
    description  "Default epipe description for service id 2100"
    sap 1/2/7:4 create
        description  "Default sap description for service id 2100"
    exit
    spoke-sdp 1:2001 create
        control-word
    exit
    no shutdown
----------------------------------------------
*A:ALA-Dut-B>config>service>epipe#
To disable the control word on spoke-sdp 1:2001:
*A:ALA-Dut-B>config>service>epipe# info
----------------------------------------------
    description  "Default epipe description for service id 2100"
    sap 1/2/7:4 create
        description  "Default sap description for service id 2100"
    exit
    spoke-sdp 1:2001 create
    exit
    no shutdown
----------------------------------------------
*A:ALA-Dut-B>config>service>epipe#
```
Pseudowire Configuration Notes

The **vc-switching** parameter must be specified at the time the VLL service is created. Note that when the **vc-switching** parameter is specified, you are configuring an S-PE. This is a pseudowire switching point (switching from one pseudowire to another). Therefore, you cannot add a SAP to the configuration.

The following example show the configuration when a SAP is added to a pseudowire. The CLI generates an error response if you attempt to create a SAP. VC switching is only needed on the pseudowire at the S-PE.

*A:ALA-701>config>service# epipe 28 customer 1 create vc-switching
*A:ALA-701>config>service>epipe$ sap 1/1/3 create
MINOR: SVCMGR #1311 SAP is not allowed under PW switching service
*A:ALA-701>config>service>epipe$

Use the following CLI syntax to create pseudowire switching VLL services.

**CLI Syntax:**
```
config>service# epipe service-id [customer customer-id][vpn vpn-id][vc-switching]
        description description-string
        spoke-sdp sd-p-id:vc-id
```

The following displays an example of the command usage to configure VLL pseudowire switching services:
Configuring Two VLL Paths Terminating on T-PE2

**T-PE1**

The following displays an example of the T-PE1 configuration.

```
*A:ALA-T-PE1>config>service>epipe# info
------------------------------------------------------------------------
     endpoint "x" create
     exit
     endpoint "y" create
     exit
     spoke-sdp 1:100 endpoint "y" create
           precedence primary
           revert-time 0
     exit
     spoke-sdp 4:400 endpoint "y" create
           precedence 0
     exit
     no shutdown
------------------------------------------------------------------------
*A:ALA-T-PE1>config>service>epipe#
```

The following displays an example of the T-PE2 configuration.

**T-PE2**

```
*A:ALA-T-PE2>config>service>epipe# info
------------------------------------------------------------------------
     endpoint "x" create
     exit
     endpoint "y" create
     exit
     sap   endpoint "x" create
     exit
     spoke-sdp 3:300 endpoint "y" create
           precedence primary
           revert-time 0
     exit
     spoke-sdp 6:600 endpoint "y" create
           precedence 0
     exit
     no shutdown
------------------------------------------------------------------------
*A:ALA-T-PE2>config>service>epipe#
```

**S-PE1:** Note that specifying the **vc-switching** parameter enables a VC cross-connect so the service manager does not signal the VC label mapping immediately but will put this into passive mode.

The following example displays the configuration:
*A:ALA-S-PE1>config>service>epipe# info

----------------------------------------------
...
    spoke-sdp 2:200 create
    exit
    spoke-sdp 3:300 create
    exit
    no shutdown

----------------------------------------------
*A:ALA-S-PE1>config>service>epipe#
S-PE2: Note that specifying the **vc-switching** parameter enables a VC cross-connect so the service manager does not signal the VC label mapping immediately but will put this into passive mode.

The following example displays the configuration:

```
*A:ALA-S-PE2>config>service>epipe# info
----------------------------------------------
... spoke-sdp 2:200 create
exit
spoke-sdp 3:300 create
exit
no shutdown
----------------------------------------------
*A:ALA-S-PE2>config>service>epipe#
```
Configuring VLL Resilience

Figure 67 displays an example to create VLL resilience. Note that the zero revert-time value means that the VLL path will be switched back to the primary immediately after it comes back up.

Figure 67: VLL Resilience

PE1:

The following displays an example for the configuration on PE1.

*A:ALA-48>config>service>epipe# info
-------------------------------------------------------------
endpoint "x" create
exit
endpoint "y" create
exit
spoke-sdp 1:100 endpoint "y" create
precedence primary
exit
spoke-sdp 2:200 endpoint "y" create
precedence 1
exit
no shutdown
-------------------------------------------------------------
*A:ALA-48>config>service>epipe#
Configuring VLL Resilience for a Switched Pseudowire Path

Figure 68: VLL Resilience with Pseudowire Switching

T-PE1

The following displays an example for the configuration on TPE1.

*A:ALA-48>config>service>epipe# info
----------------------------------------------
    endpoint "x" create
    exit
    endpoint "y" create
    exit
    sap 1/1/1:100 endpoint "x" create
    exit
    spoke-sdp 1:100 endpoint "y" create
    precedence primary
    exit
    spoke-sdp 2:200 endpoint "y" create
    precedence 1
    exit
    spoke-sdp 3:300 endpoint "y" create
    precedence 1
    exit
    no shutdown
----------------------------------------------
*A:ALA-48>config>service>epipe#
**T-PE2**

The following displays an example for the configuration on TPE2.

*A:ALA-49>config>service>epipe# info

---------------------------------------------------------
endpoint "x" create
exit
endpoint "y" create
  revert-time 100
exit
spoke-sdp 4:400 endpoint "y" create
  precedence primary
exit
spoke-sdp 5:500 endpoint "y" create
  precedence 1
exit
spoke-sdp 6:600 endpoint "y" create
  precedence 1
exit
no shutdown

---------------------------------------------------------
*A:ALA-49>config>service>epipe#

**S-PE1**

The following displays an example for the configuration on S-PE1.

*A:ALA-50>config>service>epipe# info

---------------------------------------------------------
...
  spoke-sdp 1:100 create
exit
  spoke-sdp 4:400 create
exit
no shutdown

---------------------------------------------------------
*A:ALA-49>config>service>epipe#
Configuring BGP Virtual Private Wire Service (VPWS)

Single-Homed BGP VPWS

Figure 69 shows an example topology for a BGP VPWS service used to create a virtual lease-line across an MPLS network between two sites, A and B.

Figure 69: Single-Homed BGP VPWS Configuration Example

An Epipe is configured on PE1 and PE2 with BGP VPWS enabled. PE1 and PE2 are connected to site A and B, respectively, each using a SAP. The interconnection between the two PEs is achieved through a pseudowire, using Ethernet VLAN encaps, which is signaled using BGP VPWS over a tunnel LSP between PE1 and PE2.

The following displays the BGP VPWS configuration on each PE.

PE1:
```
pw-template 1 create  
  vc-type vlan  
  exit  
epipe 1 customer 1 create  
  bgp  
    route-distinguisher 65536:1  
    route-target export target:65536:1 import target:65536:1  
    pw-template-binding 1  
  exit  
exit  
bgp-vpws  
  ve-name PE1  
  ve-id 1  
  exit  
remote-ve-name PE2  
  ve-id 2  
  exit  
  no shutdown  
exit  
sap 1/1/1:1 create  
exit  
  no shutdown  
exit  
```

PE2:
pw-template 1 create
  vc-type vlan
  exit
epipe 1 customer 1 create
  bgp
    route-distinguisher 65536:2
    route-target export target:65536:1 import target:65536:1
  exit
exit
epipe 1 customer 1 create
  bgp
    route-distinguisher 65536:2
    route-target export target:65536:1 import target:65536:1
  exit
exit
bgp-vpws
  ve-name PE2
  ve-id 2
  exit
  remote-ve-name PE1
  ve-id 1
  exit
  no shutdown
  exit
  sap 1/1/1:1 create
  exit
  no shutdown
exit

The BGP-VPWS update can be shown using the following command:

A:PE1# show service l2-route-table bgp-vpws detail
===============================================================================
Services: L2 Bgp-Vpws Route Information - Summary
===============================================================================
Svc Id         : 1
VeId           : 2
PW Temp Id     : 1
RD             : *65536:2
Next Hop       : 1.1.1.2
State (D-Bit)  : up(0)
Path MTU       : 1514
Control Word   : 0
Seq Delivery   : 0
Status         : active
Tx Status      : active
CSV            : 0
Preference     : 0
Sdp Bind Id    : 17407:4294967295
===============================================================================
A:PE1#
Dual-Homed BGP VPWS

Single Pseudowire Example:

Figure 70 shows an example topology for a dual-homed BGP VPWS service used to create a virtual lease-line across an MPLS network between two sites, A and B. A single pseudowire is established between the designated forwarder of the dual-homed PEs and the remote PE.

![Figure 70: Example of Dual-Homed BGP VPWS with Single Pseudowire](image)

An Epipe with BGP VPWS enabled is configured on each PE. Site A is dual-homed to PE1 and PE2 with a remote PE, PE3, connected to site B; each connection uses a SAP. A single pseudowire using Ethernet Raw Mode encaps connects PE3 to PE1. The pseudowire is signaled using BGP VPWS over a tunnel LSPs between the PEs.

Site A is configured on PE1 and PE2 with the BGP route selection, the site state, and the site-preference used to ensure PE1 is the designated forwarder when the network is fully operational.

The following displays the BGP VPWS configuration on each PE.

PE1:

```
pw-template 1 create
exit
epipe 1 customer 1 create
  bgp
    route-distinguisher 65536:1
    route-target export target:65536:1 import target:65536:1
  pw-template-binding 1
exit
```
bgp-vpws
    ve-name PE1
    ve-id 1
    exit
    remote-ve-name PE3
    ve-id 3
    exit
    no shutdown
    exit
    sap 1/1/1:1 create
    exit
    site "siteA" create
    site-id 1
    sap 1/1/1:1
    boot-timer 20
    site-activation-timer 5
    no shutdown
    exit
    no shutdown
    exit

PE2:

pw-template 1 create
exit
epipe 1 customer 1 create
    bgp
        route-distinguisher 65536:2
        route-target export target:65536:1 import target:65536:1
        pw-template-binding 1
        exit
    exit
bgp-vpws
    ve-name PE2
    ve-id 1
    exit
    remote-ve-name PE3
    ve-id 3
    exit
    no shutdown
    exit
    sap 1/1/1:1 create
    exit
    site "siteA" create
    site-id 1
    sap 1/1/1:1
    boot-timer 20
    site-activation-timer 5
    no shutdown
    exit
    no shutdown
    exit

PE3:

pw-template 1 create
exit
epipe 1 customer 1 create
    bgp
        route-distinguisher 65536:3
route-target export target:65536:1 import target:65536:1
pw-template-binding 1
exit
exit
bgp-vpws
  ve-name PE3
  ve-id 3
  exit
  remote-ve-name PE1orPE2
  ve-id 1
  exit
  no shutdown
exi
  sap 1/1/1:1 create
  exit
  no shutdown
  exit
Active/Standby Pseudowire Example:

Figure 71 shows an example topology for a dual-homed BGP VPWS service used to create a virtual lease-line across an MPLS network between two sites, A and B. Two pseudowires are established between the remote PE and the dual-homed PEs. The active pseudowire used for the traffic is the one connecting the remote PE to the designated forwarder of the dual-homed PEs.

![Figure 71: Example of Dual-homed BGP VPWS with Active/Standby Pseudowires](image)

An Epipe with BGP VPWS enabled is configured on each PE. Site A is dual-homed to PE1 and PE2 with a remote PE, PE3, connected to site B; each connection uses a SAP. Active/standby pseudowires using Ethernet Raw Mode encaps connect PE3 to PE1 and PE2, respectively. The pseudowires are signaled using BGP VPWS over a tunnel LSPs between the PEs.

Site A is configured on PE1 and PE2 with the site-preference set to ensure that PE1 is the designated forwarder when the network is fully operational. An endpoint is automatically created on PE3 in which the active/standby pseudowires are created.

The following displays the BGP VPWS configuration on each PE.

**PE1:**

```
pw-template 1 create
exit
epipe 1 customer 1 create
bgp
    route-distinguisher 65536:1
    route-target export target:65536:1 import target:65536:1
    pw-template-binding 1
exit
```
exit
bgp-vpws
  ve-name PE1
  ve-id 1
  exit
  remote-ve-name PE3
  ve-id 3
  exit
  no shutdown
exit
sap 1/1/1:1 create
exit
site "siteA" create
  site-id 1
  sap 1/1/1:1
  boot-timer 20
  site-activation-timer 5
  site-preference 200
  no shutdown
exit
  no shutdown
exit

PE2:

pw-template 1 create
exit
epipe 1 customer 1 create
  bgp
    route-distinguisher 65536:2
    route-target export target:65536:1 import target:65536:1
    pw-template-binding 1
  exit
exit
bgp-vpws
  ve-name PE2
  ve-id 2
  exit
  remote-ve-name PE3
  ve-id 3
  exit
  no shutdown
exit
sap 1/1/1:1 create
exit
site "siteA" create
  site-id 1
  sap 1/1/1:1
  boot-timer 20
  site-activation-timer 5
  site-preference 10
  no shutdown
exit
  no shutdown
exit

PE3:

pw-template 1 create
exit
epipe 1 customer 1 create
  bgp
    route-distinguisher 65536:3
    route-target export target:65536:1 import target:65536:1
    pw-template-binding 1
    exit
exit
bgp-vpws
  ve-name PE3
  ve-id 3
  exit
  remote-ve-name PE1
  ve-id 1
  exit
  remote-ve-name PE2
  ve-id 2
  exit
  no shutdown
exit
sap 1/1/1:1 create
exit
  no shutdown
exit
Service Management Tasks

This section discusses the following Epipe service management tasks:

- Modifying Epipe Service Parameters on page 370
- Disabling an Epipe Service on page 370
- Re-Enabling an Epipe Service on page 371
- Deleting an Epipe Service on page 371
Modifying Epipe Service Parameters

The following displays an example of adding an accounting policy to an existing SAP:

Example:config>service# epipe 2
        config>service>epipe# sap /1/3:21
        config>service>epipe>sap# accounting-policy 14
        config>service>epipe>sap# exit

The following output displays the SAP configuration:

ALA-1>config>service# info
----------------------------------------------
  epipe 2 customer 6 vpn 2 create
    description "Distributed Epipe service to east coast"
    sap /1/3:21 create
    accounting-policy 14
    exit
    spoke-sdp 2:6000 create
    exit
    no shutdown
    exit
----------------------------------------------
ALA-1>config>service#

Disabling an Epipe Service

You can shut down an Epipe service without deleting the service parameters.

**CLI Syntax:** config>service> epipe service-id
                   shutdown

**Example:** config>service# epipe 2
            config>service>epipe# shutdown
            config>service>epipe# exit
Re-Enabling an Epipe Service

To re-enable an Epipe service that was shut down.

**CLI Syntax:**
```
config>service# epipe service-id
   no shutdown
```

*Example:* `config>service# epipe 2
               config>service>epipe# no shutdown
               config>service>epipe# exit`

Deleting an Epipe Service

Perform the following steps prior to deleting an Epipe service:

1. Shut down the SAP and SDP.
2. Delete the SAP and SDP.
3. Shut down the service.

Use the following CLI syntax to delete an Epipe service:

**CLI Syntax:**
```
config>service
   [no] epipe service-id
   shutdown
   [no] sap sap-id
   shutdown
   [no] spoke-sdp sdp-id:vc-id
   shutdown
```

*Example:* `config>service# epipe 2
               config>service>epipe# sap /1/3:21
               config>service>epipe>epipe# shutdown
               config>service>epipe>epipe# exit
               config>service>epipe# no sap /1/3:21
               config>service>epipe# spoke-sdp 2:6000
               config>service>epipe>spoke-sdp# shutdown
               config>service>epipe>spoke-sdp# exit
               config>service>epipe# no spoke-sdp 2:6000
               config>service>epipe# epipe 2
               config>service>epipe# shutdown
               config>service>epipe# exit
               config>service# no epipe 2`
VLL Services Command Reference

Command Hierarchies

- Apipe Service Configuration Commands on page 373
- Cpipe Service Configuration Commands on page 378
- Epipe Service Configuration Commands on page 381
- Fpipe Service Configuration Commands on page 390
- Ipipe Service Configuration Commands on page 393

Apipe Service Configuration Commands

```bash
config
  — service
    — apipe service-id [customer customer-id] [vpn vpn-id] [vc-type atm vcc atm-sdu atm-vpc atm-cell] [vc-switching]
    — no apipe service-id
      — description description-string
      — no description
      — [no] endpoint endpoint-name
        — active-hold-delay active-hold-delay
        — no active-hold-delay
        — description description-string
        — no description
        — revert-time revert-time
        — no revert-time
    — interworking {frf-5}
    — no interworking
    — sap {port-id|aps-id}:vpi|vci|vpi1.vpi2|cp.conn-prof-id
    — sap sap-id [no-endpoint]
    — sap sap-id [endpoint endpoint-name]
    — no sap sap-id
      — accounting-policy acct-policy-id
      — no accounting-policy
      — atm
        — egress
          — traffic-desc traffic-desc-profile-id
          — no traffic-desc
        — ingress
          — traffic-desc traffic-desc-profile-id
          — no traffic-desc
        — [no] llf
        — oam
          — [no] alarm-cells
          — [no] terminate
        — [no] collect-stats
        — cpu-protection
```
— no cpu-protection
— description description-string
— no description
— dist-cpu-protection policy-name
— no dist-cpu-protection
— egress
  — [no] agg-rate
    — rate {max | rate}
    — no rate
    — [no] limit-unused-bandwidth
    — [no] queue-frame-based-accounting
— policer-control-override [create]
— no policer-control-override
  — max-rate {rate | max}
  — priority-mbs-thresholds
    — min-thresh-separation
    — [no] priority level
  — mbs-contribution size [bytes | kilobytes]
— policer-control-policy policy-name
— no policer-control-policy
— [no] policer-override
  — policer policer-id [create]
  — no policer policer-id
    — cbs size [bytes | kilobytes]
    — no cbs
    — mbs size [bytes | kilobytes]
    — no mbs
    — packet-byte-offset add add-bytes | subtract sub-bytes
    — percent-rate pir-percent [cir cir-percent]
    — no percent-rate
    — rate {rate | max} [cir {max | rate}]
    — stat-mode stat-mode
    — no stat-mode
  — [no] qinq-mark-top-only
— qos policy-id [port-redirect-group queue-group-name instance instance-id]
— no qos
— [no] queue-override
  — [no] queue queue-id
    — adaptation-rule [pir adaptation-rule] [cir adaptation-rule]
    — no adaptation-rule
    — avg-frame-overhead percentage
    — no avg-frame-overhead
    — burst-limit size-in-kbytes
    — no burst-limit
    — high-prio-only percent
    — no high-prio-only
    — mbs {size-in-kbytes | default}
    — no mbs
    — parent [{weight weight} [cir-weight cir-weight]]
    — no parent
    — percent-rate pir-percent [cir cir-percent]
Virtual Leased Line Services

— no percent-rate
— rate pir-rate [cir cir-rate]
— no rate

— [no] scheduler-override
  — [no] scheduler scheduler-name
    — rate pir-rate [cir cir-rate]
    — no rate
  — scheduler-policy scheduler-policy-name
    — no scheduler-policy

— frame-relay
  — scheduling-class class-id
  — no scheduling-class

— ingress
  — policer-control-override [create]
    — no policer-control-override
      — max-rate {rate | max}
      — priority-mbs-thresholds
        — min-thresh-separation
        — [no] priority level
          — mbs-contribution size [bytes | kilobytes]
    — [no] policer-override
      — policer policer-id [create]
        — no policer policer-id
          — cbs size [bytes | kilobytes]
          — no cbs
          — mbs size [bytes | kilobytes]
          — no mbs
          — packet-byte-offset add add-bytes | subtract sub-bytes
            — percent-rate pir-percent [cir cir-percent]
            — no percent-rate
            — rate {rate | max} [cir {max | rate}]
            — stat-mode stat-mode
            — no stat-mode

— qos policy-id [shared-queuing] [fp-redirect-group queue-group-name instance instance-id]
  — no qos

— [no] queue-override
  — [no] queue queue-id
    — adaptation-rule [pir adaptation-rule] [cir adaptation-rule]
      — no adaptation-rule
        — burst-limit size-in-kbytes
        — no burst-limit
        — high-prio-only percent
        — no high-prio-only
        — mbs {size-in-kbytes | default}
        — no mbs
        — rate pir-rate [cir cir-rate]
        — no rate

— [no] scheduler-override
  — [no] scheduler scheduler-name
    — rate pir-rate [cir cir-rate]
    — no rate
— scheduler-policy scheduler-policy-name
  — no scheduler-policy
— multi-service-site customer-site-name
  — no multi-service-site
— [no] shutdown
— tod-suite tod-suite-name
  — no tod-suite
— service-mtu octets
  — no service-mtu
— service-name service-name
  — no service-name
— [no] shutdown
— signaled-vc-type-override {atm-vcc}
  — no signaled-vc-type-override
— spoke-sdp [sdp-id]:[vc-id] [no-endpoint]
  — spoke-sdp [sdp-id]:[vc-id] endpoint endpoint-name [ich]
  — no spoke-sdp [sdp-id]:[vc-id]
    — bandwidth
      — no bandwidth
    — cell-concatenation
      — [no] aal5-frame-aware
      — [no] clp-change
      — max-cells cell-count
      — [no] max-cells [cell-count>]
      — max-delay delay-time
      — [no] max-delay [delay-time]
— [no] control-word
— egress
  — qos network-policy-id port-redirect-group queue-group-name
    [instance instance-id]
  — no qos
  — vc-label ingress-vc-label
    — no vc-label [ingress-vc-label]
— ingress
  — qos network-policy-id fp-redirect-group queue-group-name
    instance instance-id
  — no qos
  — vc-label ingress-vc-label
    — no vc-label [ingress-vc-label]
  — precedence [precedence-value| primary ]
  — no precedence
  — [no] shutdown

config
— connection-profile conn-prof-id [create]
— no connection-profile conn-prof-id
Related Apipe Commands

Connection Profile Commands

config
  — connection-profile conn-prof-id [create]
  — no connection-profile conn-prof-id
    — description description-string
    — no description
    — member encap-value [create]
    — no member encap-value
Cpipe Service Configuration Commands

config
  — service
    — cpipe service-id [customer customer-id] [vpn vpn-id] [vc-type {satop-e1 | satop-t1 | satop-e3 | satop-t3 | cesopsn | cesopsn-cas}] [vc-switching] [create]
    — no cpipe service-id
      — description description-string
      — no description [description-string]
      — endpoint endpoint-name [create]
      — no endpoint endpoint-name
        — active-hold-delay active-endpoint-delay
        — revert-time revert-time
        — no revert-time
      — sap sap-id [no-endpoint] [create]
      — no sap sap-id
        — accounting-policy acct-policy-id
        — no accounting-policy [acct-policy-id]
        — cem
          — packet jitter-buffer milliseconds [payload-size bytes]
          — packet payload-size bytes
          — no packet
          — [no] report-alarm [stray] [malformed] [pktlss] [overrun]
            [underun] [rpktloss] [rfault] [rrdi]
          — [no] rtp-header
          — [no] collect-stats
          — cpu-protection
          — description description-string
          — no description [description-string]
          — dist-cpu-protection policy-name
          — no dist-cpu-protection
          — egress
            — [no] agg-rate
              — rate {max | rate}
              — no rate
              — [no] limit-unused-bandwidth
              — [no] queue-frame-based-accounting
            — [no] qinq-mark-top-only
            — [no] qos [policy-id]
            — [no] queue-override
              — queue queue-id [create]
              — no queue queue-id
                — adaptation-rule [pir adaptation-rule] [cir adaptation-rule]
                — no adaptation-rule
                — avg-frame-overhead percent
                — no avg-frame-overhead
                — burst-limit size-in-kbytes
                — no burst-limit
                — high-prio-only percent
                — no high-prio-only
— mbs size-in-kbytes
— no mbs
— rate pir-rate [cir cir-rate]
— no rate
— [no] scheduler-override
  — scheduler scheduler-name [create]
  — no scheduler scheduler-name
  — rate pir-rate [cir cir-rate]
  — no rate
— scheduler-policy scheduler-policy-name
— no scheduler-policy
— ingress
  — [no] qos [policy-id]
  — [no] queue-override
  — queue queue-id [create]
    — no queue queue-id
      — adaptation-rule [pir adaptation-rule] [cir adaptation-rule]
    — no adaptation-rule
    — avg-frame-overhead percent
    — no avg-frame-overhead
    — burst-limit size-in-kbytes
    — no burst-limit
    — high-prio-only percent
    — no high-prio-only
    — mbs size-in-kbytes
    — no mbs
    — rate pir-rate [cir cir-rate]
    — no rate
— [no] scheduler-override
  — scheduler scheduler-name [create]
  — no scheduler scheduler-name
  — rate pir-rate [cir cir-rate]
  — no rate
— scheduler-policy scheduler-policy-name
— no scheduler-policy
  — multi-service-site customer-site-name
  — no multi-service-site
— tod-suite tod-suite-name
— no tod-suite
— service-mtu octets
— no service-mtu
— service-name service-name
— no service-name
— [no] shutdown
— spoke-sdp sdp-id[:vc-id] [no-endpoint] [create]
— spoke-sdp sdp-id[:vc-id] [create] endpoint endpoint-name [icb]
— no spoke-sdp sdp-id[:vc-id]
  — accounting-policy acct-policy-id
  — no accounting-policy
  — bandwidth bw-value
  — bandwidth max
  — no bandwidth
  — [no] collect-stats
— [no] control-word
— egress
  — qos network-policy-id port-redirect-group queue-group-name
      [instance instance-id]
  — no qos
  — vc-label egress-vc-label
  — no vc-label [egress-vc-label]
— ingress
  — qos network-policy-id fp-redirect-group queue-group-name
      [instance instance-id]
  — no qos
  — vc-label ingress-vc-label
  — no vc-label [ingress-vc-label]
— precedence [precedence-value | primary]
  — no precedence
  — [no] shutdown
Epipe Service Configuration Commands

- Epipe Global Commands on page 381
- Epipe SAP Configuration Commands on page 383
- Epipe Spoke SDP Configuration Commands on page 387

Epipe Global Commands

```plaintext
cfg
  - service [no] epipe service-id [customer customer-id] [create] [vpn vpn-id] [ve-switching]
    - [no] bgp
      - pw-template-binding policy-id [import rt {[ext-community ..,(upto 5 max)}]]
      - no pw-template-binding policy-id
      - route-distinguisher [ip-addr:comm-val | as-number:ext-comm-val]
      - no route-distinguisher
      - route-target {[ext-community] {[export ext-community] [import ext-community]}}
      - no route-target
    - [no] bgp-vpws
      - [no] remote-ve-name name
        - ve-id value
        - no ve-id
      - [no] shutdown
      - [no] ve-name name
        - ve-id value
        - no ve-id
    - description description-string
    - no description
    - [no] endpoint endpoint-name
      - active-hold-delay active-endpoint-delay
      - no active-hold-delay
      - description description-string
      - no description
      - revert-time [revert-time | infinite]
      - no revert-time
      - [no] standby-signaling-master
      - [no] standby-signaling-slave
    - tunnel service-id backbone-dest-mac mac-name ieee-address sid ISID
      - no tunnel
      - service-mtu octets
      - no service-mtu
      - service-name service-name
      - no service-name
      - site name [create]
      - no site
        - boot-timer seconds
        - no boot-timer
        - sap sap-id
```
— no sap
— site-activation-timer seconds
— no site-activation-timer
— site-id value
— no site-id
— site-preference preference-value
— no site-preference
— [no] shutdown
— spoke-sdp sdp-id[:vc-id] [vc-type {ether | vlan}] [create] [no-endpoint]
— spoke-sdp sdp-id[:vc-id] [vc-type {ether | vlan}] [create] endpoint
— no spoke-sdp sdp-id[:vc-id]
  — [no] control-word
  — hash-label
  — no hash-label
  — [no] standby-signaling-slave
Epipe SAP Configuration Commands

```bash
config
  — service
    — epipe service-id
      — sap sap-id [create] [no-endpoint]
      — sap sap-id [create] endpoint endpoint-name
      — no sap sap-id
        — accounting-policy acct-policy-id
        — no accounting-policy acct-policy-id
        — [no] cflowd
        — [no] collect-stats
        — description description-string
        — no description
        — egress
          — [no] agg-rate
            — [no] limit-unused-bandwidth
            — [no] queue-frame-based-accounting
            — rate kilobits-per-second
            — no rate
          — filter [ip ip-filter-id]
          — filter [ipv6 ipv6-filter-id]
          — filter [mac mac-filter-id]
            — no filter [ip ip-filter-id] [ipv6 ipv6-filter-id] [mac mac-filter-id]
              — policer-control-override [create]
              — no policer-control-override
                — max-rate {rate | max}
                — priority-mbs-thresholds
                  — min-thresh-separation
                  — [no] priority-level
                    — mbs-contribution size [bytes | kilobytes]
              — policer-control-policy policy-name
              — no policer-control-policy
              — [no] policer-override
                — policer policier-id [create]
                — no policer policier-id
                  — cbs size [bytes | kilobytes]
                  — no cbs
                  — mbs size [bytes | kilobytes]
                  — no mbs
                  — packet-byte-offset add add-bytes | subtract sub-bytes
                    — percent-rate pir-percent [cir cir-percent]
                    — no percent-rate
                    — rate {rate | max} [cir {max | rate}]
                    — stat-mode stat-mode
                    — no stat-mode
              — [no] qinq-mark-top-only
              — qos policy-id [port-redirect-group queue-group-name instance instance-id]
                — no qos
                — [no] queue-override
                  — queue queue-id [create]
```
— no queue queue-id
— adaptation-rule [pir adaptation-rule] [cir adaptation-rule]
— no adaptation-rule
— avg-frame-overhead percentage
— no avg-frame-overhead
— cbs size-in-kbytes
— no cbs
— high-prio-only percent
— no high-prio-only
— mbs size [bytes|kilobytes]
— no mbs
— parent [{weightweight} [cir-weight cir-weight]]
— percent-rate pir-percent [cir cir-percent]
— no percent-rate
— rate pir-rate [cir cir-rate]
— no rate
— [no] scheduler-override
— [no] scheduler scheduler-name
— rate pir-rate [cir cir-rate]
— no rate
— scheduler-policy scheduler-policy-name
— no scheduler-policy

— eth-cfm
— [no] ais-enable
— [no] interface-support-enable
— [no] mep mep-id domain md-index association ma-index
  [direction {up | down}] primary-vlan-enable [vlan vlan-id]
— [no] ais-enable
— [no] client-meg-level [{level [level ...]}]
— [no] interval [1 | 60]
— [no] priority priority-value
— [no] ccm-enable
— [no] ccm-ltm-priority priority
— ccm-padding-size ccm-padding
— no ccm-padding-size ccm-padding
— [no] csf-enable
— multiplier multiplier-value
— no multipler
— [no] description description-string
— [no] eth-test-enable
— [no] bit-error-threshold bit-errors
— test-pattern {all-zeros | all-ones} [crc-enable]
— no test-pattern
— [no] fault-propagation-enable {use-if-tlv | suspend-ccm}
— low-priority-defect {allDef | macRemErrXcon | remErrXcon | errXcon | xcon | noXcon}
— mac-address mac-address
— no mac-address
— one-way-delay-threshold seconds
— [no] shutdown
— mip [mac mac-address] primary-vlan-enable [vlan vlan-id]
— mip default-mac
— no mip
— [no] squelch-ingress-levels [md-level [md-level ...]]
— tunnel-fault [accept | ignore]

— ethernet
— [no] l1f
— [no] ignore-oper-down
— ingress
— agg-rate-limit agg-rate
— no agg-rate-limit
— filter [ip ip-filter-id]
— filter [ipv6 ipv6-filter-id]
— filter [mac mac-filter-id]
— no filter [ip ip-filter-id] [ipv6 ipv6-filter-id] [mac mac-filter-id]
— qos network-policy-id fp-redirect-group queue-group-name
  instance instance-id
— no qos
— match-qinq-dot1p {top | bottom}
— no match-qinq-dot1p
— policer-control-override [create]
— no policer-control-override
  — max-rate {rate | max}
  — priority-mbs-thresholds
    — min-thresh-separation
  — [no] priority level
  — mbs-contribution size [bytes | kilobytes]
— policer-control-policy policy-name
— no policer-control-policy
— [no] policer-override
  — policer policyer-id [create]
  — no policer policyer-id
  — cbs size-in-kilobytes
  — no cbs
  — mbs size [bytes | kilobytes]
  — no mbs
  — packet-byte-offset add add-bytes | subtract sub-byte
    — percent-rate pir-percent [cir cir-percent]
    — no percent-rate
    — rate {rate | max} [cir {max | rate}]
    — stat-mode stat-mode
    — no stat-mode
— qos policy-id [shared-queuing] [fp-redirect-group queue-group-name instance instance-id]
— no qos
— [no] queue-override
  — [no] queue queue-id
  — adaptation-rule [pir adaptation-rule] [cir adaptation-rule]
  — no adaptation-rule
  — cbs size-in-kilobytes
  — no cbs
  — high-prio-only percent
  — no high-prio-only
  — mbs size [bytes | kilobytes]
— no mbs
— parent {[weight weight] [cir-weight cir-weight]}
— no parent
— percent-rate pir-percent [cir cir-percent]
— no percent-rate
— rate pir-rate [cir cir-rate]
— no rate
— [no] scheduler-override
— [no] scheduler scheduler-name
— rate pir-rate [cir cir-rate]
— no rate
— scheduler-policy scheduler-policy-name
— no scheduler-policy
— vlan-translation {vlan-id | copy-outer}
— no vlan-translation
— monitor-oper-group group-name
— no monitor-oper-group
— multi-service-site customer-site-name
— no multi-service-site
— oper-group group-name
— no oper-group
— ring-node ring-node-name
— no ring-node
— [no] shutdown
— tod-suite tod-suite-name
— no tod-suite
— transit-policy prefix prefix-aasub-policy-id
— no transit-policy
— lag-link-map-profile link-map-profile-id
— no lag-link-map-profile
Epipe Spoke SDP Configuration Commands

```plaintext
config
  service
    epipe service-id
      spoke-sdp sdp-id[vc-id] [vc-type {ether | vlan}] [create] [no-endpoint]
      spoke-sdp sdp-id[vc-id] [vc-type {ether | vlan}] [create] endpoint [icb]
    no spoke-sdp sdp-id[vc-id]
      accounting-policy acct-policy-id
      no accounting-policy
      bandwidth bandwidth
      no bandwidth
      [no] block-on-peer-fault
      [no] collect-stats
      [no] control-word
      [no] description
    [no] egress
      filter [ip ip-filter-id]
      filter [ipv6 ipv6-filter-id]
      filter [mac mac-filter-id]
      no filter [ip ip-filter-id] [ipv6 ipv6-filter-id] [mac mac-filter-id]
    12tpv3
      cookie cookie
      no cookie
      qos network-policy-id port-redirect-group queue-group-name
        instance instance-id
      no qos
      [no] vc-label egress-vc-label
    eth-efm
      [no] ais-enable
        [no] client-meg-level [(level [level ...])]
        [no] interface-support-enable
        [no] interval {1 | 60}
        [no] priority priority-value
      [no] ccm-enable
      [no] ccm-ltm-priority priority
      ccm-padding-size ccm-padding
      no ccm-padding-size ccm-padding
      [no] csf-enable
        multiplier multiplier-value
        no multiplier
      [no] description
      [no] eth-test-enable
        [no] test-pattern {all-zeros | all-ones} [crc-enable]
      [no] fault-propagation-enable {use-if-itl | suspend-ccm}
      [no] one-way-delay-threshold seconds
      [no] mip [{mac mac-address | default-mac}]
      mep mep-id domain md-index association ma-index [direction {up | down}]
    no mep mep-id domain md-index association ma-index
      [no] ccm-enable
      ccm-ltm-priority priority
      no ccm-ltm-priority
      [no] description
```
Epipe Service Configuration Commands

— [no] eth-test-enable
— ccm-padding-size ccm-padding
— no ccm-padding-size ccm-padding
— fault-propagation-enable {use-if-tlv | suspend-ccm}
— no fault-propagation-enable
— low-priority-defect {all | macRemErrXcon | remErrXcon | errXcon | xcon | noXcon}
— mac-address mac-address
— no mac-address
— [no] shutdown
— [no] squelch-ingress-levels [md-level [md-level...]]
— [no] force-vlan-vc-forwarding
— [no] when used with IES and VPRN services
— [no] ingress
— filter [ip ip-filter-id]
— filter [ipv6 ipv6-filter-id]
— filter [mac mac-filter-id]
— no filter [ip ip-filter-id] [ipv6 ipv6-filter-id] [mac mac-filter-id]
— 12tv3
— cookie cookie
— no cookie
— qos network-policy-id fp-redirect-group queue-group-name
— instance instance-id
— no qos
— [no] ve-label egress-vc-label
— monitor-oper-group group-name
— no monitor-oper-group
— precedence [precedence-value | primary]
— no precedence
— [no] pw-status-signaling
— [no] shutdown
— [no] standby-signaling-slave
— [no] use-sdp-bmac
— vlan-vc-tag 0..4094
— no vlan-vc-tag [0..4094]
— spoke-sdp-fec spoke-sdp-fec-id [fec fec-type] [aii-type aii-type] [create]
— spoke-sdp-fec spoke-sdp-fec-id no-endpoint
— spoke-sdp-fec spoke-sdp-fec-id [fec fec-type] [aii-type aii-type] [create] endpoint
— name [icb]
— no spoke-sdp-fec spoke-sdp-fec-id
— [no] auto-config
— path name
— no path
— precedence prec-value
— precedence primary
— no precedence
— pw-template-bind policy-id
— no pw-template-bind
— retry-count retry-count
— no retry-count
— retry-timer retry-timer
— no retry-timer
— sai-type2 global-id:prefix:ac-id
— no sai-type2
— [no] shutdown
— signaling signaling
— [no] standby-signaling-slave
— tali-type2 global-id:prefix:ac-id
— no tali-type2
Fpipe Service Configuration Commands

config
  — service
    — fpipe service-id [customer customer-id] [vpn vpn-id] [ve-type {fr-dlci}] [ve-switching]
    — no fpipe service-id
      — description description-string
      — no description
    — [no] endpoint endpoint-name
      — active-hold-delay active-endpoint-delay
      — no active-hold-delay
      — description description-string
      — no description
      — revert-time revert-time
      — no revert-time
    — sap sap-id [no-endpoint]
      — sap-id endpoint endpoint-name
      — no sap sap-id
        — accounting-policy acct-policy-id
        — no accounting-policy
        — [no] collect-stats
        — cpu-protection policy-id [mac-monitoring] | [eth-cfm-monitoring
          [aggregate][car]]
          — description description-string
          — no description
          — dist-cpu-protection policy-name
          — no dist-cpu-protection
          — egress
            — [no] agg-rate
              — rate {max | rate}
              — no rate
              — [no] limit-unused-bandwidth
              — [no] queue-frame-based-accounting
            — filter [ip ip-filter-id]
            — filter [ipv6 ipv6-filter-id]
            — no filter [ip ip-filter-id] [ipv6 ipv6-filter-id]
            — policer-control-override [create]
            — no policer-control-override
              — max-rate {rate | max}
              — priority-mbs-thresholds
                — min-thresh-separation
                — [no] priority level
                — mbs-contribution size [bytes | kilobytes]
            — policer-control-policy policy-name
            — no policer-control-policy
            — [no] policer-override
              — policer policer-id [create]
              — no policer policer-id
                — cbs size [bytes | kilobytes]
                — no cbs
                — mbs size [bytes | kilobytes]
                — no mbs
                — packet-byte-offset add add-bytes | subtract sub-
                  bytes
                — percent-rate pir-percent [cir cir-percent]
— no percent-rate
— rate {rate | max} [cir {max | rate}]
— stat-mode stat-mode
— no stat-mode
— [no] qinq-mark-top-only
— qos policy-id
— no qos
— [no] queue-override
  — [no] queue queue-id
    — adaptation-rule [pir adaptation-rule] [cir adaptation-rule]
    — no adaptation-rule
    — avg-frame-overhead percent
    — no avg-frame-overhead
    — burst-limit size-in-kbytes
    — no burst-limit
    — high-prio-only percent
    — no high-prio-only
    — mbs {size-in-kbytes | default}
    — no mbs
    — rate pir-rate [cir cir-rate]
    — no rate
— [no] scheduler-override
  — [no] scheduler scheduler-name
    — rate pir-rate [cir cir-rate]
    — no rate
  — scheduler-policy scheduler-policy-name
  — no scheduler-policy
— frame-relay
  — scheduling-class class-id
  — no scheduling-class
— ingress
  — filter [ip ip-filter-id]
  — filter [ipv6 ipv6-filter-id]
  — no filter [ip ip-filter-id] [ipv6 ipv6-filter-id]
  — qos policy-id [shared-queuing]
  — no qos
— [no] queue-override
  — [no] queue queue-id
    — adaptation-rule [pir adaptation-rule] [cir adaptation-rule]
    — no adaptation-rule
    — avg-frame-overhead percent
    — no avg-frame-overhead
    — burst-limit size-in-kbytes
    — no burst-limit
    — high-prio-only percent
    — no high-prio-only
    — mbs {size-in-kbytes | default}
    — no mbs
    — rate pir-rate [cir cir-rate]
    — no rate
— [no] scheduler-override
  — [no] scheduler scheduler-name
— rate pir-rate [cir cir-rate]
— no rate
— scheduler-policy scheduler-policy-name
— no scheduler-policy
— scheduler-policy scheduler-policy-name
— no scheduler-policy
— multi-service-site customer-site-name
— no multi-service-site
— [no] shutdown
— tod-suite tod-suite-name
— no tod-suite
— service-mtu octets
— no service-mtu
— service-name service-name
— no service-name
— [no] shutdown
— spoke-sdp sdp-id[:vc-id] [no-endpoint]
— spoke-sdp sdp-id[:vc-id] endpoint endpoint-name [icb]
— no spoke-sdp sdp-id[:vc-id]
— bandwidth bandwidth
— no bandwidth
— egress
— filter [ip ip-filter-id]
— filter [ipv6 ipv6-filter-id]
— no filter [ip ip-filter-id] [ipv6 ipv6-filter-id]
— qos network-policy-id port-redirect-group queue-group-name
— instance instance-id
— no qos
— vc-label ingress-vc-label
— no vc-label [ingress-vc-label]
— hash-label
— no hash-label
— ingress
— filter [ip ip-filter-id]
— filter [ipv6 ipv6-filter-id]
— no filter [ip ip-filter-id] [ipv6 ipv6-filter-id]
— qos network-policy-id fp-redirect-group queue-group-name
— instance instance-id
— no qos
— vc-label ingress-vc-label
— no vc-label [ingress-vc-label]
— precedence [precedence-value| primary]
— no precedence
— [no] shutdown
Ipipe Service Configuration Commands

```
config
    service
        ipipe service-id [customer customer-id] [vpn vpn-id] [vc-switching]
        no ipipe service-id
            [no] ce-address-discovery [ipv6]
            description description-string
            no description
            [no] endpoint endpoint-name
                active-endpoint-delay
                no active-endpoint-delay
                description description-string
                no description
                revert-time revert-time
                no revert-time
            sap sap-id [no-endpoint]
            sap sap-id endpoint endpoint-name
            [no] sap eth-tunnel-tunnel-id [eth-tunnel-sap-id] [create]
            no sap sap-id
                accounting-policy acct-policy-id
                no accounting-policy
                atm
                    egress
                        traffic-desc traffic-desc-profile-id
                        no traffic-desc
                    encapsulation atm-encap-type
                    ingress
                        traffic-desc traffic-desc-profile-id
                        no traffic-desc
                    oam
                        [no] alarm-cells
                    ce-address ip-address
                    no ce-address
                    collect-stats
                    no collect-stats
                    cpu-protection
                    no cpu-protection
                    description description-string
                    no description
                    dist-cpu-protection policy-name
                    no dist-cpu-protection
                    egress
                        agg-rate-limit agg-rate
                        no agg-rate-limit
                        [no] agg-rate
                            rate {max | rate}
                            no rate
                            [no] limit-unused-bandwidth
                            [no] queue-frame-based-accounting
                        filter {ip ip-filter-id | ipv6 ipv6-filter-id}
                        no filter {ip ip-filter-id | ipv6 ipv6-filter-id}
                        [no] hsmda-queue-override
```
— secondary-shaper secondary-shaper-name
— no secondary-shaper
— wrr-policy hsmda-wrr-policy-name
— no wrr-policy
— packet-byte-offset {add add-bytes | subtract sub-bytes}
— no packet-byte-offset
— queue queue-id
— no queue queue-id
— wrr-weight weight
— no wrr-weight
— mbs size {{bytes | kilobytes} | default}
— no mbs
— rate pir-rate
— no rate
— slope-policy hsmda-slope-policy-name allowable
— no slope-policy
— [no] qinq-mark-top-only
— qos policy-id
— no qos
— [no] queue-override
— [no] queue queue-id
— adaptation-rule [pir adaptation-rule] [cir adaptation-rule]
— no adaptation-rule
— avg-frame-overhead percent
— no avg-frame-overhead
— burst-limit size-in-kbytes
— no burst-limit
— high-prio-only percent
— no high-prio-only
— mbs {size-in-kbytes | default}
— no mbs
— rate pir-rate [cir cir-rate]
— no rate
— [no] scheduler-override
— [no] scheduler scheduler-name
— rate pir-rate [cir cir-rate]
— no rate
— scheduler-policy scheduler-policy-name
— no scheduler-policy
— eth-cfm
— [no] mep mep-id domain md-index association ma-index
  [direction {up | down}]
  — [no] ccm-enable
  — [no] ccm-ltm-priority priority
  — [no] description
  — [no] eth-test-enable
  — [no] bit-error-threshold bit-errors
  — [no] test-pattern {all-zeros | all-ones} [crc-enable]
  — [no] fault-propagation-enable {use-if-tlv | suspend-ccm}
  — low-priority-defect {allDef | macRemErrXcon | remErrXcon | errXcon | xcon | noXcon}
Virtual Leased Line Services

---

- [no] mac-address mac-address
- [no] one-way-delay-threshold <seconds>
- [no] shutdown
- [no] mip {mac mac-address | default-mac}
- [no] squelch-ingress-levels [md-level [md-level...]]
- tunnel-fault [accept | ignore]

- eth-tunnel
- path path-index tag qtag[.qtag]
- no path path-index

- ingress
- filter {ip ip-filter-id | ipv6 ipv6-filter-id}
- no filter {ip ip-filter-id | ipv6 ipv6-filter-id}
- match-qinq-dot1p [top | bottom]
- no match-qinq-dot1p
- qos policy-id [shared-queuing]
- no qos
- [no] queue-override
- [no] queue queue-id
- adaptation-rule [pir adaptation-rule] [cir adaptation-rule]
- no adaptation-rule
- burst-limit size-in-kbytes
- no burst-limit
- high-prio-only percent
- no high-prio-only
- mbs {size-in-kbytes | default}
- no mbs
- rate pir-rate [cir cir-rate]
- no rate

- [no] scheduler-override
- [no] scheduler scheduler-name
- rate pir-rate [cir cir-rate]
- no rate

- scheduler-policy scheduler-policy-name
- no scheduler-policy
- lag-link-map-profile link-map-profile-id
- no lag-link-map-profile
- mac {ieee-address}
- no mac
- mac-refresh [refresh interval]
- no mac-refresh
- multi-service-site customer-site-name
- no multi-service-site
- [no] shutdown
- tod-suite tod-suite-name
- no tod-suite
- [no] use-broadcast-mac

- service-mtu octets
- no service-mtu
- service-name service-name
- no service-name
- [no] shutdown
- spoke-sdp [sdp-id[:vc-id] [no-endpoint]
- spoke-sdp [sdp-id[:vc-id] endpoint endpoint-name [icb]
— **no spoke-sdp** sap-id
  — bandwidth bandwidth
  — no bandwidth
  — ce-address ip-address
  — no ce-address
  — [no] control-word
  — egress
    — filter {ip ip-filter-id | ipv6 ipv6-filter-id}
    — no filter {ip ip-filter-id | ipv6 ipv6-filter-id}
    — qos network-policy-id port-redirect-group queue-group-name
      [instance instance-id]
    — no qos
    — [no] vc-label vc-label
  — hash-label
  — no hash-label
  — ingress
    — filter {ip ip-filter-id | ipv6 ipv6-filter-id}
    — no filter {ip ip-filter-id | ipv6 ipv6-filter-id}
    — qos network-policy-id fp-redirect-group queue-group-name
      instance instance-id
    — no qos
    — vc-label ingress-vc-label
    — no vc-label [ingress-vc-label]
    — precedence [precedence-value] primary
    — no precedence
    — [no] shutdown
  — [no] stack-capability-signaling
Virtual Leased Line Services

VLL Service Configuration Commands

- Generic Commands on page 397
- VLL Global Commands on page 401
- VLL SAP Commands on page 414
- VLL SDP Commands on page 468

Generic Commands

**shutdown**

**Syntax**

[no] shutdown

**Context**

config>service>epipe
config>service>epipe>bgp-vpws
config>service>epipe>sap
config>service>epipe>spoke-sdp
config>service>epipe>sap>eth-cfm>mep
config>service>epipe>spoke-sdp>eth-cfm>mep

**Description**

This command administratively disables an entity. When disabled, an entity does not change, reset, or remove any configuration settings or statistics.

The operational state of the entity is disabled as well as the operational state of any entities contained within. Many objects must be shut down before they may be deleted.

Services are created in the administratively down (**shutdown**) state. When a **no shutdown** command is entered, the service becomes administratively up and then tries to enter the operationally up state. Default administrative states for services and service entities is described below in Special Cases.

The **no** form of this command places the entity into an administratively enabled state.

**Special Cases**

**Service Admin State** — Bindings to an SDP within the service will be put into the out-of-service state when the service is shutdown. While the service is shutdown, all customer packets are dropped and counted as discards for billing and debugging purposes.

**Service Operational State** — A service is regarded as operational providing that at least one SAP and one SDP are operational or if two SAP’s are operational.

**SDP (global)** — When an SDP is shutdown at the global service level, all bindings to that SDP are put into the out-of-service state and the SDP itself is put into the administratively and operationally down states. Packets that would normally be transmitted using this SDP binding will be discarded and counted as dropped packets.

**SDP (service level)** — Shutting down an SDP within a service only affects traffic on that service from entering or being received from the SDP. The SDP itself may still be operationally up for other services.
description

Syntax  
description description-string  
no description

Context  
config>service>epipe  
config>service>epipe>sap  
config>service>epipe>spoke-sdp  
config>service>epipe>endpoint

Description  
This command creates a text description stored in the configuration file for a configuration context. The description command associates a text string with a configuration context to help identify the content in the configuration file.

The no form of this command removes the string from the configuration.

Default  
No description associated with the configuration context.

Parameters  
string — The description character string. Allowed values are any string up to 80 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.
Service Commands

apipe

Syntax  
apipe service-id [customer customer-id] [vpn vpn-id] [vc-type {atm-vcc | atm-sdu | atm-vpc | atm-cell}] [vc-switching]  
no apipe service-id

Context  
config>service

Description  
The Apipe service provides a point-to-point Layer 2 VPN connection to a remote SAP or to another local SAP. An Apipe can connect an ATM or Frame Relay endpoint either locally or over a PSN to a remote endpoint of the same type or of a different type and perform interworking between the two access technologies.

Parameters  
service-id — The unique service identification number or string identifying the service in the service domain. This ID must be unique to this service and may not be used for any other service of any type. The service-id must be the same number used for every 7750 SR, 7450 ESS and 7710 SR on which this service is defined.

Values  
service-id: 1 — 2147483648  
svc-name: 64 characters maximum

customer customer-id — Specifies the customer ID number to be associated with the service. This parameter is required on service creation and optional for service editing or deleting.

Values  
1 — 2147483647

vpn vpn-id — Specifies the VPN ID number which allows you to identify virtual private networks (VPNs) by a VPN identification number.

Values  
1 — 2147483647  
Default null (0)

vc-type — Keyword that specifies a 15 bit value that defines the type of the VC signaled to the peer. Its values are defined in draft-ietf-pwe3-iana-allocation and it defines both the signaled VC type as well as the resulting datapath encapsulation over the Apipe.

Values  
atm-vcc, atm-sdu, atm-vpc, atm-cell

Default  
atm-sdu

vc-switching — Specifies if the pseudowire switching signalling is used for the spoke SDPs configured in this service.

epipe

Syntax  
epipe service-id customer customer-id [vpn vpn-id] [vc-switching] [create]  
epipe service-id

7950 SR OS Services Guide  Page 399
no epipe service-id

Context config>service

This command configures an Epipe service instance. This command is used to configure a point-to-point epipe service. An Epipe connects two endpoints defined as Service Access Points (SAPs). Both SAPs may be defined in one 7950 XRS or they may be defined in separate devices connected over the service provider network. When the endpoint SAPs are separated by the service provider network, the far end SAP is generalized into a Service Distribution Point (SDP). This SDP describes a destination and the encapsulation method used to reach it.

No MAC learning or filtering is provided on an Epipe.

When a service is created, the customer keyword and customer-id must be specified and associates the service with a customer. The customer-id must already exist having been created using the customer command in the service context. Once a service has been created with a customer association, it is not possible to edit the customer association. The service must be deleted and recreated with a new customer association.

Once a service is created, the use of the customer customer-id is optional for navigating into the service configuration context. Attempting to edit a service with the incorrect customer-id specified will result in an error.

By default, no epipe services exist until they are explicitly created with this command.

The no form of this command deletes the epipe service instance with the specified service-id. The service cannot be deleted until the service has been shutdown.

Parameters

service-id — The unique service identification number or string identifying the service in the service domain. This ID must be unique to this service and may not be used for any other service of any type. The service-id must be the same number used for every 7950 XRS on which this service is defined.

Values

 svc-name: 64 characters maximum

customer customer-id — Specifies the customer ID number to be associated with the service. This parameter is required on service creation and optional for service editing or deleting.

Values

1 — 2147483647

vpn vpn-id — Specifies the VPN ID number which allows you to identify virtual private networks (VPNs) by a VPN ID. If this parameter is not specified, the VPN ID uses the same service ID number.

Values

1 — 2147483647

Default null (0)

cvc-switching — Specifies if the pseudowire switching signalling is used for the spoke SDPs configured in this service.

create — Keyword used to create the service instance. The create keyword requirement can be enabled/disabled in the environment>create context.
**VLL Global Commands**

**bgp**

**Syntax**

```
bgp
```

**Context**

```
config>service>epipe
```

**Description**

This command enables the context to configure the BGP related parameters BGP used for Multi-Homing and BGP VPWS.

The **no** form of this command removes the string from the configuration.

**pw-template-binding**

**Syntax**

```
pw-template-binding policy-id [import-rt {ext-community..(upto 5 max)}]
no pw-template-binding policy-id
```

**Context**

```
config>service>epipe>bgp
```

**Description**

This command binds the advertisements received with the route targets (RT) that match the configured list (either the generic or the specified import) to a specific pw-template. If the RT list is not present, or if multiple matches are found, the numerically lowest pw-template is used.

The evil form of the command applies to BGP-VPWS when enabled in the Epipe.

For BGP VPWS, the following additional rules govern the use of pseudowire-template:

- On transmission, the settings for the L2-Info extended community in the BGP updates are derived from the pseudowire template attributes. If multiple pseudowire template bindings (with or without import-rt) are specified for the same VPWS instance the first pw-template entry will be used.

- On reception, the values of the parameters in the L2-Info extended community of the BGP updates are compared with the settings from the corresponding pseudowire template bindings. The following steps are used to determine the local pw-template:
  - The RT values are matched to determine the pw-template.
  - If multiple pw-template-binding matches are found from the previous step, the first (numerically lowest) configured pw-template entry will be considered.
  - If the value used for Layer 2 MTU (unless the value zero is received) does not match the pseudowire is created but with the oper state down.
  - If the values used for the C (control word) or S (sequenced delivery) flags are not zero the pseudowire is not created.

The **tools perform** commands can be used to control the application of changes in pw-template for BGP-VPWS.

The **no** form of the command removes the values from the configuration.

**Parameters**

`policy-id` — Specifies an existing policy ID.
Values 1 — 2147483647

**import-rt ext-comm** — Specify communities allowed to be accepted from remote PE neighbors. An extended BGP community in the type:x:y format. The value x can be an integer or IP address. The type can be the target or origin.

Values

- **target:** \{ip-addr:comm-val | 2byte-asnumber:ext-comm-val | 4byte-asnumber:comm-val\}
  - ip-addr a.b.c.d
  - comm-val 0 — 65535
  - 2byte-asnumber 0 — 65535
  - ext-comm-val 0 — 4294967295
  - 4byte-asnumber 0 — 4294967295

---

**route-distinguisher**

**Syntax**


**Context**

```config > service > epipe > bgp```

**Description**

This command configures the Route Distinguisher (RD) component that is signaled in the MPBGP NLRI for L2VPN AFI. This value is used for BGP Multi-Homing and BGP-VPWS. An RD value must be configured under BGP node.

**Format:** Six bytes, other 2 bytes of type will be automatically generated.

**Parameters**

- **ip-addr:comm-val** — Specifies the IP address.
  - **Values**
    - ip-addr a.b.c.d
    - comm-val 0 — 65535
  - **as-number:**
    - **Values**
      - as-number 1 — 65535
      - ext-comm-val 0 — 4294967295

---

**route-target**

**Syntax**

```route-target {ext-community}{[export ext-community][import ext-community]} no route-target```

**Context**

```config > service > epipe > bgp```

**Description**

This command configures the route target (RT) component that is signaled in the related MPBGP attribute to be used for BGP Multi-Homing and BGP-VPWS when configured in the Epipe service. The ext-comm can have two formats:

- A two-octet AS-specific extended community, IPv4 specific extended community.
- An RT value must be configured under BGP node when BGP Epipe is configured.
Virtual Leased Line Services

**Parameters**

*export ext-community* — Specifies communities allowed to be sent to remote PE neighbors.

*import ext-community* — Specifies communities allowed to be accepted from remote PE neighbors.

### bgp-vpws

**Syntax**  

```plaintext
[no] bgp-vpws
```

**Context**  

```
config>service>epipe
```

**Description**  

This command enables the context to configure BGP-VPWS parameters and addressing.

**Default**  

```
no bgp-vpws
```

### remote-ve-name

**Syntax**  

```plaintext
[no] remote-ve-name name
```

**Context**  

```
config>service>epipe
config>service>epipe:bgp-vpws
```

**Description**  

This command creates or edits a remote-ve-name. A single remote-ve-name can be created per BGP VPWS instance if the service is single-homed or uses a single pseudowire to connect to a pair of dual-homed systems. When the service requires active/standby pseudowires to be created to remote dual-homed systems then two remote-ve-names must be configured.

This context defines the remote PE to which a pseudowire will be signaled. `remote-ve-name` commands can be added even if bgp-vpws is not shutdown.

The `no` form of the command removes the configured remote-ve-name from the bgp vpws node. It can be used when the BGP VPWS status is either shutdown or “no shutdown”.

**Parameters**  

*name* — Specifies a site name up to 32 characters in length.

### ve-id

**Syntax**  

```plaintext
ve-id value
no ve-id
```

**Context**  

```
config>service>epipe:bgp-vpws>ve-name
config>service>epipe:bgp-vpws>remote-ve-name
```

**Description**  

This command configures a ve-id for either the local VPWS instance when configured under the ve-name, or for the remote VPWS instance when configured under the remote-ve-name.

A single ve-id can be configured per ve-name or remote-ve-name. The ve-id can be changed without shutting down the VPWS instance. When the ve-name ve-id changes, BGP withdraws the previously advertised route and sends a route-refresh to all the peers which would result in reception of all the remote routes again. The old PWs are removed and new ones are instantiated for the new ve-id value.
When the remote-ve-name ve-id changes, BGP withdraws the previously advertised route and send a new update matching the new ve-id. The old pseudowires are removed and new ones are instantiated for the new ve-id value.

NLRIs received whose advertised ve-id does not match the list of ve-ids configured under the remote ve-id will not have a spoke-SDP binding auto-created but will remain in the BGP routing table but not in the L2 route table. A change in the locally configured ve-ids may result in auto-sdp-bindings either being deleted or created, based on the new matching results.

Each ve-id configured within a service must be unique.

The no form of the command removes the configured ve-id. It can be used just when the BGP VPWS status is shutdown. Command “no shutdown” cannot be used if there is no ve-id configured.

**Default**

no ve-id

**Parameters**

- **value** — A two bytes identifier that represents the local or remote VPWS instance and is advertised through the BGP NLRI.

  **Values**

  1 — 65535

**ve-name**

**Syntax**

[no] ve-name name

**Context**

config>service>epipe>bgp-vpws

**Description**

This command configures the name of the local VPWS instance in this service.

The no form of the command removes the ve-name.

**Parameters**

- **name** — Specifies a site name up to 32 characters in length.

**shutdown**

**Syntax**

[no] shutdown

**Context**

config>service>epipe>bgp-vpws

**Description**

This command administratively enables/disables the local BGP VPWS instance. On de-activation an MP-UNREACH-NLRI is sent for the local NLRI.

The no form of the command enables the BGP VPWS addressing and the related BGP advertisement. The associated BGP VPWS MP-REACH-NLRI will be advertised in an update message and the corresponding received NLRIs must be considered to instantiate the data plane.

**Default**

shutdown

**site**

**Syntax**

site name [create]

no site name
Virtual Leased Line Services

**Context**
config>service>epipe

**Description**
This command configures a Epipe site.
The **no** form of the command removes the name from the configuration.

**Parameters**
- *name* — Specifies a site name up to 32 characters in length.
- *create* — This keyword is mandatory while creating a Epipe service.

**boot-timer**

**Syntax**
```plaintext
boot-timer seconds
no boot-timer
```

**Context**
config>service>epipe>site

**Description**
This command configures for how long the service manger waits after a node reboot before running the DF election algorithm. The boot-timer value should be configured to allow for the BGP sessions to come up and for the NLRI information to be refreshed/exchanged.
The **no** form of the command reverts the default.

**Default**
10

**Parameters**
- *seconds* — Specifies the site boot-timer in seconds.

**Values**
0 — 600

**sap**

**Syntax**
```plaintext
sap sap-id
no sap
```

**Context**
config>service>epipe>site

**Description**
This command configures a SAP for the site.
The **no** form of the command removes the SAP ID from the configuration.

**Parameters**
- *sap-id* — Specifies the physical port identifier portion of the SAP definition.

**site-activation-timer**

**Syntax**
```plaintext
site-activation-timer seconds
no site-activation-timer
```

**Context**
config>service>epipe>site

**Description**
This command configures the time-period the system keeps the local sites in standby status, waiting for BGP updates from remote PEs before running the DF (designated-forwarder) election algorithm.
to decide whether the site should be unblocked. This timer is terminated if an update is received for which the remote PE has transitioned from DF to non-DF.

The **no** form of the command removes the value from the configuration.

**Default**: 2

**Parameters**

- *seconds* — Specifies the site activation timer in seconds.
  
  **Values**: 0 — 100

---

**site-id**

**Syntax**

```
site-id value
no site-id
```

**Context**

```
cfg>service>epipe>site
```

**Description**

This command configures the identifier for the site in this service. It must match between services but it is local to the service.

**Parameters**

- *value* — Specifies the site identifier.
  
  **Values**: 1 — 65535

---

**site-preference**

**Syntax**

```
site-preference preference-value
no site-preference
```

**Context**

```
cfg>service>epipe>site
```

**Description**

This command defines the value to advertise in the VPLS preference field of the BGP VPWS and BGP Multi-homing NLRI extended community. This value can be changed without having to shutdown the site itself. The site-preference is only applicable to VPWS services.

When not configured, the default is zero, indicating that the VPLS preference is not in use.

**Default**: no site-preference, value=0

**Parameters**

- *preference-value* — Specifies the preference value to advertise in the NLRI L2 extended community for this site.
  
  **Values**: 1 — 65535

- *primary* — Sets the site-preference to 65535.

- *backup* — Sets the site-preference to 1.

---

**endpoint**

**Syntax**

```
[no] endpoint endpoint-name
```
Virtual Leased Line Services

Context
config>service>apipe
config>service>epipe
config>service>ipipe

Description
This command configures a service endpoint.

Parameters
endpoint-name — Specifies an endpoint name.

tunnel

Syntax
```
tunnel service-id backbone-dest-mac ieee-address isid ISID
no tunnel
```

Context
config>service>epipe>pbb

Description
This command configures a Provider Backbone Bridging (PBB) tunnel with Backbone VPLS (B-VPLS) service information.

Parameters
service-id — Specifies the B-VPLS service for the PBB tunnel associated with this service.

Values
- service-id: 1 — 2147483648
- svc-name: 64 characters maximum

backbone-dest-mac  ieee-address — Specifies the backbone destination MAC-address for PBB packets.

isid ISID — Specifies a 24 bit service instance identifier for the PBB tunnel associated with this service. As part of the PBB frames, it is used at the destination PE as a demultiplexor field.

Values
- 0 — 16777215

active-hold-delay

Syntax
```
active-hold-delay active-hold-delay
no active-hold-delay
```

Context
config>service>apipe>endpoint
config>service>epipe>endpoint

Description
This command specifies that the node will delay sending the change in T-LDP status bits for the VLL endpoint when the MC-LAG transitions the LAG subgroup which hosts the SAP for this VLL endpoint from active to standby or when any object in the endpoint. For example, SAP, ICB, or regular spoke SDP, transitions from up to down operational state.

By default, when the MC-LAG transitioned the LAG subgroup which hosts the SAP for this VLL endpoint from active to standby, the node sends immediately new T-LDP status bits indicating the new value of "standby" over the spoke SDPs which are on the mate-endpoint of the VLL. The same applies when any object in the endpoint changes an operational state from up to down.

There is no delay applied to the VLL endpoint status bit advertisement when the MC-LAG transitions the LAG subgroup which hosts the SAP from standby to active or when any object in the endpoint transitions to an operationally up state.
Default 0 — A value of zero means that when the MC-LAG transitioned the LAG subgroup which hosts the SAP for this VLL endpoint from active to standby, the node sends immediately new T-LDP status bits indicating the new value of standby over the spoke SDPs which are on the mate-endpoint of the VLL. The same applies when any object in the endpoint changes an operational state from up to down.

Parameters active-hold-delay — Specifies the active hold delay in 100s of milliseconds.

Values 0 — 60

revert-time

Syntax revert-time [revert-time | infinite]
no revert-time

Context config>service>apipe>endpoint
config>service>epipe>endpoint

Description This command configures the time to wait before reverting back to the primary spoke SDP defined on this service endpoint, after having failed over to a backup spoke SDP.

Parameters revert-time — Specify the time, in seconds, to wait before reverting to the primary SDP.

Values 0 — 600

Values 0

infinite — Causes the endpoint to be non-revertive.

standby-signaling-master

Syntax [no] standby-signaling-master

Context config>service>vll>endpoint

Description When this command is enabled, the pseudowire standby bit (value 0x00000020) will be sent to T-LDP peer for each spoke-sdp of the endpoint that is selected as a standby.

This command is mutually exclusive with a VLL mate SAP created on a mc-lag/mc-aps or ICB. It is also mutually exclusive with vc-switching.

Default standby-signaling-master

standby-signaling-slave

Syntax [no] standby-signaling-slave

Context config>service>epipe>endpoint
config>service>epipe>spoke-sdp

Page 408 7950 SR OS Services Guide
**Description**  
When this command is enabled, the node will block the transmit forwarding direction of a spoke SDP based on the pseudowire standby bit received from a T-LDP peer.

This command is present at the endpoint level as well as the spoke-SDP level. If the spoke SDP is part of an explicit-endpoint, it will not be possible to change this setting at the spoke-sdp level. An existing spoke SDP can be made part of the explicit endpoint only if the settings do not conflict. A newly created spoke SDP, which is part of a given explicit-endpoint, will inherit this setting from the endpoint configuration.

This command is mutually exclusive with an endpoint that is part of an mc-lag, mc-aps or an ICB.

If the command is disabled, the node assumes the existing independent mode of behavior for the forwarding on the spoke SDP.

**Default**  
disabled

---

**interworking**

**Syntax**  
interworking (frf-5)  
no interworking

**Context**  
config>service>apipe

**Description**  
This command specifies the interworking function that should be applied for packets that ingress/egress SAPs that are part of an Apipe service.

Interworking is applicable only when the two endpoints (i.e., the two SAPs or the SAP and the spoke-sdp) are of different types. Also, there are limitations on the combinations of SAP type, vc-type, and interworking values as shown in the following table.

<table>
<thead>
<tr>
<th>SAP Type</th>
<th>Allowed VC-Type Value</th>
<th>Allowed Interworking Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ATM VC</td>
<td>atm-vcc, atm-sdu</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>fr-dlci</td>
<td>Not Supported</td>
</tr>
<tr>
<td>FR DLCI</td>
<td>fr-dlci</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td>atm-sdu</td>
<td>frf-5</td>
</tr>
</tbody>
</table>

**Default**  
none (Interworking must be configured before adding a Frame-Relay SAP to an Apipe service.)

**Parameters**  
frf-5 — Specify Frame Relay to ATM Network Interworking (FRF.5).

---

**service-name**

**Syntax**  
service-name service-name  
no service-name

**Context**  
config>service>epipe

**Description**  
This command configures an optional service name, up to 64 characters in length, which adds a name identifier to a given service to then use that service name in configuration references as well as
display and use service names in show commands throughout the system. This helps the service provider/administrator to identify and manage services within the SR OS platforms.

All services are required to assign a service ID to initially create a service. However, either the service ID or the service name can be used to identify and reference a given service once it is initially created.

**Parameters**

*service-name* — Specifies a unique service name to identify the service. Service names may not begin with an integer (0-9).

---

**service-mtu**

**Syntax**

```
service-mtu octets
no service-mtu
```

**Context**

```
config>service>epipe
```

**Description**

This command configures the service payload (Maximum Transmission Unit – MTU), in bytes, for the service. This MTU value overrides the service-type default MTU. The *service-mtu* defines the payload capabilities of the service. It is used by the system to validate the SAP and SDP binding’s operational state within the service.

The service MTU and a SAP’s service delineation encapsulation overhead (4 bytes for a dot1q tag) is used to derive the required MTU of the physical port or channel on which the SAP was created. If the required payload is larger than the port or channel MTU, then the SAP will be placed in an inoperative state. If the required MTU is equal to or less than the port or channel MTU, the SAP will be able to transition to the operative state.

When binding an SDP to a service, the service MTU is compared to the path MTU associated with the SDP. The path MTU can be administratively defined in the context of the SDP. The default or administrative path MTU can be dynamically reduced due to the MTU capabilities discovered by the tunneling mechanism of the SDP or the egress interface MTU capabilities based on the next hop in the tunnel path. If the service MTU is larger than the path MTU, the SDP binding for the service will be placed in an inoperative state. If the service MTU is equal to or less than the path MTU, then the SDP binding will be placed in an operational state.

In the event that a service MTU, port or channel MTU, or path MTU is dynamically or administratively modified, then all associated SAP and SDP binding operational states are automatically re-evaluated.

Binding operational states are automatically re-evaluated.

For i-VPLS and Epipes bound to a b-VPLS, the service-mtu must be at least 18 bytes smaller than the b-VPLS service MTU to accommodate the PBB header.

Because this connects a Layer 2 to a Layer 3 service, adjust either the service-mtu under the Epipe service. The MTU that is advertised from the Epipe side is service-mtu minus EtherHeaderSize.

The *no* form of this command returns the default *service-mtu* for the indicated service type to the default value.

By default if no service-mtu is configured it is (1514 - 14) = 1500.

**Default**

epipe: 1514

The following table displays MTU values for specific VC types.
<table>
<thead>
<tr>
<th>SAP VC-Type</th>
<th>Example Service MTU</th>
<th>Advertised MTU</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet</td>
<td>1514</td>
<td>1500</td>
</tr>
<tr>
<td>Ethernet (with preserved dot1q)</td>
<td>1518</td>
<td>1504</td>
</tr>
<tr>
<td>VPLS</td>
<td>1514</td>
<td>1500</td>
</tr>
<tr>
<td>VPLS (with preserved dot1q)</td>
<td>1518</td>
<td>1504</td>
</tr>
<tr>
<td>VLAN (dot1p transparent to MTU value)</td>
<td>1514</td>
<td>1500</td>
</tr>
<tr>
<td>VLAN (Q-in-Q with preserved bottom Qtag)</td>
<td>1518</td>
<td>1504</td>
</tr>
</tbody>
</table>

*octets* — The size of the MTU in octets, expressed as a decimal integer, between 1 — 9194.
signaled-vc-type-override

**Syntax**

```
signaled-vc-type-override atm-vcc
no signaled-vc-type-override
```

**Context**

```
<root>
```

**Description**

This command overrides the pseudowire type signaled to type 0x0009 N:1 VCC cell within an Apipe VLL service of vc-type atm-cell. Normally, this service vc-type signals a pseudowire of type 0x0003 ATM Transparent Cell.

This command is not allowed in an Apipe VLL of vc-type value atm-cell if a configured ATM SAP is not using a connection profile. Conversely, if the signaling override command is enabled, only an ATM SAP with a connection profile assigned will be allowed.

The `override` command is not allowed on Apipe VLL service of vc-type value other than atm-cell. It is also not allowed on a VLL service with the vc-switching option enabled since signaling of the PW FEC in a Multi-Segment PW (MS-PW) is controlled by the T-PE nodes. Thus for this feature to be used on a MS-PW, it is required to configure an Apipe service of vc-type atm-cell at the T-PE nodes with the signaled-vc-type-override enabled, and to configure a Apipe VLL service of vc-type atm-vcc at the S-PE node with the vc-switching option enabled.

The `no` form of this command returns the Apipe VLL service to signal its default pseudowire type

**Default**

```
one
```

**Parameters**

```
atm-vcc  —  Specifies the pseudowire type to be signaled in the pseudowire establishment.
```

connection-profile

**Syntax**

```
connection-profile conn-prof-id [create]
no connection-profile conn-prof-id
```

**Context**

```
<root>
```

**Description**

This command creates a profile for the user to configure the list of discrete VPI/VCI values to be assigned to an ATM SAP of an Apipe VLL of `vc-type atm-cell`. A connection profile can only be applied to a SAP which is part of an Apipe VLL service of `vc-type atm-cell`. The ATM SAP can be on a regular port or APS port.

A maximum of 8000 connection profiles can be created on the system.

The `no` form of this command deletes the profile from the configuration.

**Default**

```
one
```

**Parameters**

```
conn-prof-id  —  Specifies the profile number.
```

Values

```
1 — 8000
```

member

**Syntax**

```
member encap-value [create]
```

Page 412

7950 SR  OS Services Guide
no member encaps-value

Context config>connection-profile

Description This command allows the adding of discrete VPI/VCI values to an ATM connection profile for assignment to an ATM SAP of an Apipe VLL of vc-type atm-cell.

Up to a maximum of 16 discrete VPI/VCI values can be configured in a connection profile. The user can modify the content of a profile which triggers a re-evaluation of all the ATM SAPs which are currently using the profile.

The no form of this command deletes the member from the configuration.

Default none

Parameters encaps-value — Specifies the VPI and VCI values of this connection profile member.

Values

<table>
<thead>
<tr>
<th>VPI</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>NNI</td>
<td>0 — 4095</td>
</tr>
<tr>
<td>UNI</td>
<td>0 — 255</td>
</tr>
<tr>
<td>VCI</td>
<td>1, 2, 5 — 65535</td>
</tr>
</tbody>
</table>
**VLL SAP Commands**

**sap**

**Syntax**  
sap sap-id [create] [no-endpoint]
sap sap-id [create] endpoint endpoint-name
no sap sap-id

**Context**  
config>service>apipe
config>service>epipe

**Description**  
This command creates a Service Access Point (SAP) within a service. A SAP is a combination of port and encapsulation parameters which identifies the service access point on the interface and within the device. Each SAP must be unique.

All SAPs must be explicitly created. If no SAPs are created within a service or on an IP interface, a SAP will not exist on that object.

Enter an existing SAP without the `create` keyword to edit SAP parameters. The SAP is owned by the service in which it was created.

A SAP can only be associated with a single service. A SAP can only be defined on a port that has been configured as an access port. Channelized TDM ports are always access ports.

If a port is shutdown, all SAPs on that port become operationally down. When a service is shutdown, SAPs for the service are not displayed as operationally down although all traffic traversing the service will be discarded.

The operational state of a SAP is relative to the operational state of the port on which the SAP is defined.

The following are supported:
- Ethernet SAPs support null, dot1q, and qinq

The `no` form of this command deletes the SAP with the specified port. When a SAP is deleted, all configuration parameters for the SAP will also be deleted. For Internet Enhanced Service (IES), the IP interface must be shutdown before the SAP on that interface may be removed.

**Default**  
No SAPs are defined.

**Special Cases**  
A SAP can be defined with Ethernet ports, SONET/SDH or TDM channels. At most, only one sdp-id can be bound to an VLL service. Since a VLL is a point-to-point service, it can have, at most, two end points. The two end points can be one SAP and one SDP or two SAPs. Up to 49 SDPs can be associated with a service in a single router. Each SDP must have a unique router destination or an error will be generated.

A default SAP has the following format: port-id:* . This type of SAP is supported only on Ethernet MDAs and its creation is allowed only in the scope of Layer 2 services (Epipe and VPLS). This type of SAP is mutually exclusive with a SAP defined by explicit null encapsulation (for example, 1/1/1:0).
sap-id — Specifies the physical port identifier portion of the SAP. See Common CLI Command Descriptions on page 1783 for command syntax.

port-id — Specifies the physical port ID in the slot/mda/port format.

If the card in the slot has Media Dependent Adapters (MDAs) installed, the port-id must be in the slot_number/MDA_number/port_number format. For example 6/2/3 specifies port 3 on MDA 2 in slot 6.

The port-id must reference a valid port type. When the port-id parameter represents SONET/SDH and TDM channels, the port ID must include the channel ID. A period “.” separates the physical port from the channel-id. The port must be configured as an access port.

If the SONET/SDH port is configured as clear-channel then only the port is specified.

endpoint — Adds a SAP endpoint association.

no endpoint — removes the association of a SAP or a spoke-sdp with an explicit endpoint name.

create — Keyword used to create a SAP instance. The create keyword requirement can be enabled/disabled in the environment>create context.

sap

Syntax [no] sap eth-tunnel-tunnel-id[:eth-tunnel-sap-id] [create]

Context config>service>epipe

config>service>vpls

Description This command configures an Ethernet tunnel SAP.

An Ethernet tunnel control SAP has the format eth-tunnel-id and is not configured with an Ethernet tunnel SAP ID. No Ethernet tunnel tags can be configured under a control SAP since the control SAP uses the control tags configured under the Ethernet tunnel port. This means that at least one member port and control tag must be configured under the Ethernet tunnel port before this command is executed. The control SAP is needed for carrying G.8031 and 802.1ag protocol traffic. This SAP can also carry user data traffic.

An Ethernet tunnel same-fate SAP has the format eth-tunnel-id:eth-tunnel-sap-id. Same-fate SAPs carry only user data traffic. Multiple same-fate SAPs can be configured on one Ethernet tunnel port and share the fate of that port, provided the SAPs are properly configured with corresponding tags.

Ethernet tunnel SAPs are supported under VPLS, Epipe and Ipipe services only.

Default no sap

Parameters tunnel-id — Specifies the tunnel ID.

Values 1 — 1024

eth-tunnel-sap-id — Specifies a SAP ID of a same-fate SAP.

Values 0 — 4094
lag-link-map-profile

Syntax

    lag-link-map-profile  link-map-profile-id
    no lag-link-map-profile

Context

    config>service>epipe>sap
    config>service>ipipe>sap

Description

This command assigns a pre-configured lag link map profile to a SAP/network interface configured on a LAG or a PW port that exists on a LAG. Once assigned/de-assigned, the SAP’s/network interface’s egress traffic will be re-hashed over LAG as required by the new configuration.

The no form of this command reverts the SAP/network interface to use per-flow, service or link hash as configured for the service/LAG.

Default

    no lag-link-map-profile

Parameters

    link-map-profile-id — An integer from 1 to 64 that defines a unique lag link map profile on the LAG the SAP/network interface exists on.

monitor-oper-group

Syntax

    monitor-oper-group  group-name
    no monitor-oper-group

Context

    config>service>if
    config>service>ies>spoke-sdp
    config>service>ies>sap

Description

This command specifies the operational group to be monitored by the object under which it is configured. The oper-group name must be already configured under the config>service context before its name is referenced in this command.

The no form of the command removes the association.

agg-rate-limit

Syntax

    agg-rate-limit  agg-rate
    no agg-rate-limit

Context

    config>service>epipe>sap>ingress

Description

This command defines a maximum total rate for all egress queues on a service SAP or multi-service site. The agg-rate-limit command is mutually exclusive with the egress scheduler policy. When an egress scheduler policy is defined, the agg-rate-limit command will fail. If the agg-rate-limit command is specified, an attempt to bind a scheduler-policy to the SAP or multi-service site will fail.

A multi-service site must have a port scope defined that ensures all queues associated with the site are on the same port or channel. If the scope is not set to a port, the agg-rate-limit command will fail.

Once an agg-rate-limit has been assigned to a multi-service site, the scope cannot be changed to card level.
A port scheduler policy must be applied on the egress port or channel the SAP or multi-service site are bound to in order for the defined agg-rate-limit to take effect. The egress port scheduler enforces the aggregate queue rate as it distributes its bandwidth at the various port priority levels. The port scheduler stops offering bandwidth to member queues once it has detected that the aggregate rate limit has been reached.

If a port scheduler is not defined on the egress port, the queues are allowed to operate based on their own bandwidth parameters.

The no form of the command removes the aggregate rate limit from the SAP or multi-service site.

**Parameters**

**agg-rate** — Defines the rate, in kilobits-per-second, that the maximum aggregate rate the queues on the SAP or MSS can operate.

| Values  | 1 — 40000000, max |

**Syntax**

```
[no] agg-rate
```

**Context**

config>service>apipe>sap>egress
cfg>service>cpipe>sap>egress
cfg>service>epipe>sap>egress
cfg>service>fpipe>sap>egress
cfg>service>ipipe>sap>egress

**Description**

This command is used to control an HQoS aggregate rate limit. It is used in conjunction with the following parameter commands: rate, limit-unused-bandwidth, and queue-frame-based-accounting.

**rate**

```
rate {max | rate}
```

**no rate**

**Context**

config>service>apipe>sap>egress>agg-rate
cfg>service>cpipe>sap>egress>agg-rate
cfg>service>epipe>sap>egress>agg-rate
cfg>service>fpipe>sap>egress>agg-rate
cfg>service>ipipe>sap>egress>agg-rate

**Description**

This command defines the enforced aggregate rate for all queues associated with the agg-rate context. A rate must be specified for the agg-rate context to be considered to be active on the context’s object (SAP, subscriber, VPORT etc.).

**limit-unused-bandwidth**

```
[no] limit-unused-bandwidth
```

**Context**

config>service>apipe>sap>egress>agg-rate
VLL SAP Commands

```
config>service>cpipe>sap>egress>agg-rate
config>service>epipe>sap>egress>agg-rate
config>service>fpipe>sap>egress>agg-rate
config>service>ipipe>sap>egress>agg-rate
```

**Description**
This command is used to enable (or disable) aggregate rate overrun protection on the agg-rate context.

**queue-frame-based-accounting**

**Syntax**

```
[no] queue-frame-based-accounting
```

**Context**

```
config>service>apipe>sap>egress>agg-rate
config>service>cpipe>sap>egress>agg-rate
config>service>fpipe>sap>egress>agg-rate
config>service>ipipe>sap>egress>agg-rate
```

**Description**
This command is used to enabled (or disable) frame based accounting on all queues associated with the agg-rate context. Only supported on Ethernet ports. Not supported on HSMDA Ethernet ports.

**policer-control-override**

**Syntax**

```
policer-control-override [create]
no policer-control-override
```

**Context**

```
config>service>epipe>sap>egress
```

**Description**
This command, within the SAP ingress or egress contexts, creates a CLI node for specific overrides to the applied policer-control-policy. A policy must be applied for a policer-control-overrides node to be created. If the policer-control-policy is removed or changed, the policer-control-overrides node is automatically deleted from the SAP.

The **no** form of the command removes any existing policer-control-policy overrides and the policer-control-overrides node from the SAP.

**Default**

no policer-control-override

**Parameters**

**create** — The create keyword is required when the policer-control-overrides node is being created and the system is configured to expect explicit confirmation that a new object is being created. When the system is not configured to expect explicit confirmation, the create keyword is not required.

**max-rate**

**Syntax**

```
max-rate {rate | max}
```

**Context**

```
config>service>epipe>sap>egress>policer-control-override
```
**Description**  
This command, within the SAP ingress and egress contexts, overrides the root arbiter parent policer max-rate that is defined within the policer-control-policy applied to the SAP.

When the override is defined, modifications to the policer-control-policy max-rate parameter have no effect on the SAP’s parent policer until the override is removed using the `no max-rate` command within the SAP.

**Parameters**  
`rate | max` — Specifies the max rate override in kilobits-per-second or use the maximum.

**Values**  
1 — 2000000000 Kbps, max

**priority-mbs-thresholds**

**Syntax**  
priority-mbs-thresholds

**Context**  
config>service>epipe>sap>egress>policer-control-override

**Description**  
This command overrides the CLI node contains the configured min-thresh-separation and the various priority level mbs-contribution override commands.

**min-thresh-separation**

**Syntax**  
`min-thresh-separation size [bytes | kilobytes]`

**Context**  
config>service>epipe>sap>egress>policer-control-override>priority-mbs-threshold

**Description**  
This command within the SAP ingress and egress contexts is used to override the root arbiter’s parent policer min-thresh-separation parameter that is defined within the policer-control-policy applied to the SAP.

When the override is defined, modifications to the policer-control-policy min-thresh-separation parameter have no effect on the SAP’s parent policer until the override is removed using the no min-thresh-separation command within the SAP.

The no form of the command removes the override and allows the min-thresh-separation setting from the policer-control-policy to control the root arbiter’s parent policer’s minimum discard threshold separation size.

**Default**  
no min-thresh-separation

**Parameters**  
`bytes` — Signifies that size is expressed in bytes. The bytes and kilobytes keywords are mutually exclusive and are optionally used to qualify whether size is expressed in bytes or kilobytes. The default is kilobytes.

`kilobytes` — The size parameter is required when specifying the min-thresh-separation override. It is specified as an integer representing either a number of bytes or kilobytes that are the minimum separation between the parent policer’s priority level discard thresholds.

**Values**  
0 – 16777216 or default

**Default**  
kilobytes
priority

Syntax  [no] priority level
Context  config>service>epipe>sap>egress>policer-control-override>priority-mbs-thresholds
Description  The priority-level level override CLI node contains the specified priority level’s mbs-contribution override value.
This node does not need to be created and will not be output in show or save configurations unless an mbs-contribution override exist for level.
Parameters  level — The level parameter is required when specifying priority-level and identifies which of the parent policer instances priority level’s the mbs-contribution is overriding.

Values  1 — 8

mbs-contribution

Syntax  mbs-contribution size [bytes | kilobytes]
Context  config>service>epipe>sap>egress>policer-control-override>priority-mbs-thresholds>priority
Description  The mbs-contribution override command within the SAP ingress and egress contexts is used to override a parent policer’s priority level’s mbs-contribution parameter that is defined within the policer-control-policy applied to the SAP. This override allow the priority level’s burst tolerance to be tuned based on the needs of the SAP’s child policers attached to the priority level.
When the override is defined, modifications to the policer-control-policy priority level’s mbs-contribution parameter have no effect on the SAP’s parent policer priority level until the override is removed using the no mbs-contribution command within the SAP.
The no form of the command removes the override and allows the mbs-contribution setting from the policer-control-policy to control the parent policer’s priority level’s burst tolerance.

Default  no mbs-contribution
Parameters  bytes — This keyword signifies that size is expressed in bytes.

kilobytes — The optional kilobytes keyword signifies that size is expressed in kilobytes.

Values  0 – 16777216 or default

policer-control-policy

Syntax  policer-control-policy policy-name [create]
no policer-control-policy
Context  config>service>epipe>sap>egress
Description  This command, within the QoS CLI node, is used to create, delete or modify policer control policies. A policer control policy is very similar to the scheduler-policy which is used to manage a set of queues by defining a hierarchy of virtual schedulers and specifying how the virtual schedulers interact.
to provide an aggregate SLA. In a similar fashion, the policer-control-policy controls the aggregate bandwidth available to a set of child policers. Once created, the policy can be applied to ingress or egress SAPs.

Policer Control Policy Instances

On the SAP side, an instance of a policy is created each time a policy is applied. Each instance of the policer-control-policy manages the policers associated with the object that owns the policy instance (SAP). If a policer on the object is parented to an appropriate arbiter name that exists within the policy, the policer will be managed by the instance. If a policer is not parented or is parented to a non-existent arbiter, the policer will be orphaned and will not be subject to bandwidth control by the policy instance.

Maximum Rate and Root Arbiter

The policer-control-policy supports an overall maximum rate (max-rate) that defines the total amount of bandwidth that may be distributed to all associated child policers. By default, that rate is set to max which provides an unlimited amount of bandwidth to the policers. Once the policy is created, an actual rate should be configured in order for the policy instances to be effective. At the SAP level, the maximum rate may be overridden on a per instance basis.

The maximum rate is defined within the context of the root arbiter which is always present in a policer-control-policy. The system creates a parent policer which polices the output of all child policers attached to the policy instance to the configured rate. Child policers may be parented directly to the root arbiter (parent root) or parented to one of the tiered arbiters (parent arbiter-name). Since each tiered arbiter must be parented to either another tiered arbiter or the root arbiter (default), every parented child policer is associated with the root arbiter and thus the root arbiter’s parent policer.

Parent Policer PIR Leaky Bucket Operation

The parent policer is a single leaky bucket that monitors the aggregate throughput rate of the associated child policers. Forwarded packets increment the bucket by the size of each packet. The rate of the parent policer is implemented as a bucket decrement function which attempts to drain the bucket. If the rate of the packets flowing through the bucket is less than the decrement rate, the bucket does not accumulate depth. Each packet that flows through the bucket is accompanied by a derived discard threshold. If the current depth of the bucket is less than the discard threshold, the packet is allowed to pass through, retaining the colors derived from the packet’s child policer. If the current depth is equal to or greater than the threshold value, the packet is colored red and the bucket depth is not incremented by the packet size. Also, any increased bucket depths in the child policer are canceled making any discard event an atomic function between the child and the parent.

Due to the fact that multiple thresholds are supported by the parent policer, the policer control policy is able to protect the throughput of higher priority child policers from the throughput of the lower priority child policers within the aggregate rate.

Tier 1 and Tier 2 Arbiters

As stated above, each child is attached either to the always available root arbiter or to an explicitly created tier 1 or tier 2 arbiter. Unlike the hardware parent policer based root arbiter, the arbiters at tier 1 and tier 2 are only represented in software and are meant to provide an arbitrary hierarchical bandwidth distribution capability. An arbiter created on tier 2 must parent to either an arbiter on tier 1 or to the root arbiter. Arbiters created on tier 1 always parent to the root arbiter. In this manner, every arbiter ultimately is parented or grand-parented by the root arbiter.

Each tiered arbiter supports an optional rate parameter that defines a rate limit for all child arbiters or child policers associated with the arbiter. Child arbiters and policers attached to the arbiter have a level attribute that defines the strict level at which the child is given bandwidth by the arbiter. Level 8
is the highest and 1 is the lowest. Also a weight attribute defines each child’s weight at that strict level in order to determine how bandwidth is distributed to multiple children at that level when insufficient bandwidth is available to meet each child’s required bandwidth.

Fair and Unfair Bandwidth Control

Each child policer supports three leaky buckets. The PIR bucket manages the policer’s peak rate and maximum burst size, the CIR leaky bucket manages the policer’s committed rate (in-profile / out-of-profile) and committed burst size. The third leaky bucket is used by the policer control policy instance to manage the child policer’s fair rate (FIR). When multiple child policers are attached to the root arbiter at the same priority level, the policy instance uses each child’s FIR bucket rate to control how much of the traffic forwarded by the policer is fair and how much is unfair.

In the simplest case where all the child policers in the same priority level are directly attached to the root arbiter, each child’s FIR rate is set according to the child’s weight divided by the sum of the active children’s weights multiplied by the available bandwidth at the priority level. The result is that the FIR bucket will mark the appropriate amount of traffic for each child as fair based on the weighted fair output of the policy instance.

The fair/unfair forwarding control in the root parent policer is accomplished by implementing two different discard thresholds for the priority. The first threshold is discard-unfair and the second is discard-all for packet associated with the priority level. As the parent policer PIR bucket fills (due the aggregate forwarded rate being greater than the parent policers PIR decrement rate) and the bucket depth reaches the first threshold, all unfair packets within the priority are discarded. This leaves room in the bucket for the fair packets to be forwarded.

In the more complex case where one or more tiered arbiters are attached at the priority level, the policer control policy instance must consider more than just the child policer weights associated with the attached arbiter. If the arbiter is configured with an aggregate rate limit that its children cannot exceed, the policer control policy instance will switch to calculating the rate each child serviced by the arbiter should receive and enforces that rate using each child policers PIR leaky bucket.

When the child policer PIR leaky bucket is used to limit the bandwidth for the child policer and the child’s PIR bucket discard threshold is reached, packets associated with the child policer are discarded. The child policer’s discarded packets do not consume depth in the child policer’s CIR or FIR buckets. The child policers discarded packets are also prevented from impacting the parent policer and will not consume the aggregate bandwidth managed by the parent policer.

Parent Policer Priority Level Thresholds

As stated above, each child policer is attached either to the root arbiter or explicitly to one of the tier 1 or tier 2 arbiters. When attached directly to the root arbiter, its priority relative to all other child policers is indicated by the parenting level parameter. When attached through one of the tiered arbiters, the parenting hierarchy of the arbiters must be traced through to the ultimate attachment to the root arbiter. The parenting level parameter of the arbiter parented to the root arbiter defines the child policer’s priority level within the parent policer.

The priority level is important since it defines the parent policer discard thresholds that will be applied at the parent policer. The parent policer has 8 levels of strict priority and each priority level has its own discard-unfair and discard-all thresholds. Each priority’s thresholds are larger than the thresholds of the lower priority levels. This ensures that when the parent policer is discarding, it will be priority sensitive.

To visualize the behavior of the parent policer, picture that when the aggregate forwarding rate of all child policers is currently above the decrement rate of the parent PIR leaky bucket, the bucket depth will increase over time. As the bucket depth increases, it will eventually cross the lowest priority’s
discard-unfair threshold. If this amount of discard sufficiently lowers the remaining aggregate child policer rate, the parent PIR bucket will hover around this bucket depth. If however, the remaining aggregate child rate is still greater than the decrement rate, the bucket will continue to rise and eventually reach the lowest priority’s discard-all threshold which will cause all packets associated with the priority level to be discarded (fair and unfair). Again, if the remaining aggregate child rate is less than or equal to the bucket decrement rate, the parent PIR bucket will hover around this higher bucket depth. If the remaining aggregate child rate is still higher than the decrement rate, the bucket will continue to rise through the remaining priority level discards until equilibrium is achieved.

As noted above, each child’s rate feeding into the parent policer is governed by the child policer’s PIR bucket decrement rate. The amount of bandwidth the child policer offers to the parent policer will not exceed the child policer’s configured maximum rate.

Root Arbiter’s Parent Policier’s Priority Aggregate Thresholds

Each policer-control-policy root arbiter supports configurable aggregate priority thresholds which are used to control burst tolerance within each priority level. Two values are maintained per priority level; the shared-portion and the fair-portion. The shared-portion represents the amount of parent PIR bucket depth that is allowed to be consumed by both fair and unfair child packets at the priority level. The fair-portion represents the amount of parent PIR bucket depth that only the fair child policer packets may consume within the priority level. It should be noted that the fair and unfair child packets associated with a higher parent policer priority level may also consume the bucket depth set aside for this priority.

While the policy maintains a parent policer default or explicit configurable values for shared-portion and fair-portion within each priority level, it is possible that some priority levels will not be used within the parent policer. Most parent policer use cases require fewer than eight strict priority levels.

In order to derive the actual priority level discard-unfair and discard-all thresholds while only accounting for the actual in-use priority levels, the system maintains a child policer to parent policer association counter per priority level for each policer control policy instance. As a child policer is parented to either the root or a tiered arbiter, the system determines the parent policer priority level for the child policer and increments the association counter for that priority level on the parent policer instance.

The shared-portion for each priority level is affected by the parent policer global min-thresh-separation parameter that defines the minimum separation between any in-use discard thresholds. When more than one child policer is associated with a parent policer priority level, the shared-portion for that priority level will be the current value of min-thresh-separation. When only a single child policer is associated, the priority level’s shared-portion is zero since all packets from the child will be marked fair and the discard-unfair threshold is meaningless. When the association counter is zero, both the shared-portion and the fair-portion for that priority level are zero since neither discard thresholds will be used. Whenever the association counter is greater than 0, the fair-portion for that priority level will be derived from the current value of the priority’s mbs-contribution parameter and the global min-thresh-separation parameter.

Each priority level’s discard-unfair and discard-all thresholds are calculated based on an accumulation of lower priorities shared-portions and fair-portions and the priority level’s own shared-portion and fair-portion. The base threshold value for each priority level is equal to the sum of all lower priority level’s shared-portions and fair-portions. The discard-unfair threshold is the priority level’s base threshold plus the priority level’s shared-portion. The discard-all threshold for the priority level is the priority level’s base threshold plus both the shared-portion and fair-portion values of the priority. As can be seen, an in-use priority level’s thresholds are always greater than the thresholds of lower priority levels.
Policer Control Policy Application

A policer-control-policy may be applied on any Ethernet ingress or egress SAP that is associated with a port (or ports in the case of LAG).

The **no** form of the command removes a non-associated policer control policy from the system. The command will not execute when policer-name is currently associated with any SAP context.

**Default**

none

**Parameters**

- **policy-name** — Each policer-control-policy must be created with a unique policy name. The name must given as policy-name must adhere to the system policy ASCII naming requirements. If the defined policy-name already exists, the system will enter that policy’s context for editing purposes. If policy-name does not exist, the system will attempt to create a policy with the specified name. Creating a policy may require use of the create parameter when the system is configured for explicit object creation mode.

- **create** — The keyword is required when a new policy is being created and the system is configured for explicit object creation mode.

---

**policer-override**

**Syntax**

```plaintext
[n] policer-override
```

**Context**

```
config>service>epipe>sap>egress
```

**Description**

This command, within the SAP ingress or egress contexts, is used to create a CLI node for specific overrides to one or more policers created on the SAP through the sap-ingress or sap-egress QoS policies.

The **no** form of the command is used to remove any existing policer overrides.

**Default**

no policer-overrides

---

**policer**

**Syntax**

```plaintext
policer policer-id [create]
no policer policer-id
```

**Context**

```
config>service>epipe>sap>egress>policer-override
```

**Description**

This command, within the SAP ingress or egress contexts, is used to create a CLI node for specific overrides to a specific policer created on the SAP through a sap-ingress or sap-egress QoS policy.

The **no** form of the command is used to remove any existing overrides for the specified policer-id.

**Parameters**

- **policer-id** — The policer-id parameter is required when executing the policer command within the policer-overrides context. The specified policer-id must exist within the sap-ingress or sap-egress QoS policy applied to the SAP. If the policer is not currently used by any forwarding class or forwarding type mappings, the policer will not actually exist on the SAP. This does not preclude creating an override context for the policer-id.
create — The create keyword is required when a policer policer-id override node is being created and the system is configured to expect explicit confirmation that a new object is being created. When the system is not configured to expect explicit confirmation, the create keyword is not required.

cbs

Syntax  
cbs size-in-kbytes  
no cbs  

Context config>service>epipe>sap>egress>policer-override>policer  

Description This command, within the SAP ingress and egress policer-overrides contexts, is used to override the sap-ingress and sap-egress QoS policy configured CBS parameter for the specified policer-id. The no form of this command returns the CBS size to the default value.

Default no cbs  

Parameters  
size-in-kbytes — The size parameter is required when specifying mbs override and is expressed as an integer representing the required size in either bytes or kilobytes. The default is kilobytes. The optional byte and kilobyte keywords are mutually exclusive and are used to explicitly define whether size represents bytes or kilobytes.

Values  
0 – 16777216 or default

kilobytes — When kilobytes is defined, the value given for size is interpreted as the policer’s CBS value given in kilobytes.

mbs

Syntax  
mbs size [bytes | kilobytes]  
no mbs  

Context config>service>epipe>sap>egress>policer-override>policer  
config>service>epipe>sap>ingress>policer-override>policer  

Description This command, within the SAP ingress and egress policer-overrides contexts, is used to override the sap-ingress and sap-egress QoS policy configured mbs parameter for the specified policer-id. The no form of the command is used to restore the policer’s mbs setting to the policy defined value.

Default no mbs  

Parameters  
size — The size parameter is required when specifying mbs override and is expressed as an integer representing the required size in either bytes or kilobytes. The default is kilobytes. The optional byte and kilobyte keywords are mutually exclusive and are used to explicitly define whether size represents bytes or kilobytes.

Values  
0 – 16777216 or default

kilobytes — When kilobytes is defined, the value given for size is interpreted as the policer’s MBS value given in kilobytes.
packet-byte-offset

Syntax: `packet-byte-offset {add add-bytes | subtract sub-bytes}`

Context: `config>service>eipe>.sap>egress>policer-override>policer`

Description: This command, within the SAP ingress and egress policer-overrides contexts, is used to override the sap-ingress and sap-egress QoS policy configured packet-byte-offset parameter for the specified policer-id. The `no` packet-byte-offset command is used to restore the policer’s packet-byte-offset setting to the policy defined value.

Default: `no packet-byte-offset`

Parameters:
- **add add-bytes** — The add keyword is mutually exclusive to the subtract keyword. Either add or subtract must be specified. When add is defined the corresponding bytes parameter specifies the number of bytes that is added to the size each packet associated with the policer for rate metering, profiling and accounting purposes. From the policer’s perspective, the maximum packet size is increased by the amount being added to the size of each packet.
  
  Values: 1 — 32

- **subtract sub-bytes** — The subtract keyword is mutually exclusive to the add keyword. Either add or subtract must be specified. When subtract is defined the corresponding bytes parameter specifies the number of bytes that is subtracted from the size of each packet associated with the policer for rate metering, profiling and accounting purposes. From the policer’s perspective, the maximum packet size is reduced by the amount being subtracted from the size of each packet.
  
  Values: 1 — 32

percent-rate

Syntax: `percent-rate pir-percent [cir cir-percent]

Context: `config>service>eipe>.sap>egress>policer-override>policer`

Description: This command configures the percent rates (CIR and PIR) override.

Parameters:
- **pir-rate** — The pir-percent parameter is used to express the policer’s PIR as a percentage of the policers’ parent arbiter rate.
  
  Values: Percentage ranging from 0.01 to 100.00. The default is 100.00.

- **cir cir-rate** — Configures the administrative CIR specified by the user.
  
  Values: 0 — 20000000, max
Context  config>service>epipe>sap>egress>queue-override>queue

Description  The percent-rate command within the SAP ingress and egress QoS policy enables supports for a queue’s PIR and CIR rate to be configured as a percentage of the egress port’s line rate or of its parent scheduler’s rate.

When the rates are expressed as a port-limit, the actual rates used per instance of the queue will vary based on the port speed. For example, when the same QoS policy is used on a 1-Gigabit and a 10-Gigabit Ethernet port, the queue’s rates will be 10 times greater on the 10 Gigabit port due to the difference in port speeds. This enables the same QoS policy to be used on SAPs on different ports without needing to use SAP based queue overrides to modify a queue’s rate to get the same relative performance from the queue.

If the port’s speed changes after the queue is created, the queue’s PIR and CIR rates will be recalculated based on the defined percentage value.

Values  When the rates are expressed as a local-limit, the actual rates used per instance of the queue are relative to the queue’s parent scheduler rate. This enables the same QoS policy to be used on SAPs with different parent scheduler rates without needing to use SAP based queue overrides to modify a queue’s rate to get the same relative performance from the queue.

If the parent scheduler rate changes after the queue is created, the queue’s PIR and CIR rates will be recalculated based on the defined percentage value.

Queue rate overrides can only be specified in the form as configured in the QoS policy (a SAP override can only be specified as a percent-rate if the associated QoS policy was also defined as percent-rate). Likewise, a SAP override can only be specified as a rate (kbps) if the associated QoS policy was also defined as a rate. Queue overrides are relative to the limit type specified in the QoS policy.

When no percent-rate is defined within a SAP ingress or egress queue-override, the queue reverts to the defined shaping and CIR rates within the SAP ingress and egress QOS policy associated with the queue.

Parameters  percent-of-line-rate — The percent-of-line-rate parameter is used to express the queue’s shaping rate as a percentage of line rate. The line rate associated with the queue’s port may dynamically change due to configuration or auto-negotiation. The line rate may also be affected by an egress port scheduler defined max-rate.

pir-percent — The pir-percent parameter is used to express the queue’s PIR as a percentage dependant on the use of the port-limit or local-limit.

Values  Percentage ranging from 0.01 to 100.00. The default is 100.00.

pir-percent — The pir-percent parameter is used to express the queue’s PIR as a percentage dependant on the use of the port-limit or local-limit.

cir  cir-percent — The cir keyword is optional and when defined the required cir-percent CIR parameter expresses the queue’s CIR as a percentage dependant on the use of the port-limit or local-limit.

Percentage ranging from 0.00 to 100.00. The default is 100.00
rate

**Syntax**
```
rate {rate | max} [cir {max | rate}]
```

**Context**
```
config>service>epipe>sap>egress>policer-override>policer
config>service>epipe>sap>ingress>policer-override>policer
```

**Description**
This command within the SAP ingress and egress policer-overrides contexts is used to override the sap-ingress and sap-egress QoS policy configured rate parameters for the specified policer-id.

The **no rate** command is used to restore the policy defined metering and profiling rate to a policer.

**Parameters**
- `{rate | max}` — Specifying the keyword `max` or an explicit kilobits-per-second parameter directly following the rate override command is required and identifies the policer instance metering rate for the PIR leaky bucket. The kilobits-per-second value must be expressed as an integer and defines the rate in Kilobits-per-second. The integer value is multiplied by 1,000 to derive the actual rate in bits-per-second. When `max` is specified, the maximum policer rate used will be equal to the maximum capacity of the card on which the policer is configured. If the policer rate is set to a value larger than the maximum rate possible for the card, then the PIR used is equivalent to `max`.
  - **Values**
    - 1 — 2000000000, `max`

- `cir {max | rate}` — The optional cir keyword is used to override the policy derived profiling rate of the policer. Specifying the keyword `max` or an explicit kilobits-per-second parameter directly following the cir keyword is required. The kilobits-per-second value must be expressed as an integer and defines the rate in Kilobits-per-second. The integer value is multiplied by 1,000 to derive the actual rate in bits-per-second. When `max` is specified, the maximum policer rate used will be equal to the maximum capacity of the card on which the policer is configured. If the policer rate is set to a value larger than the maximum rate possible for the card, then the CIR used is equivalent to `max`.
  - **Values**
    - 0 — 2000000000, `max`

stat-mode

**Syntax**
```
stat-mode stat-mode
no stat-mode
```

**Context**
```
config>service>epipe>sap>egress>policer-override>policer
```

**Description**
The sap-egress QoS policy’s policer stat-mode command is used to configure the forwarding plane counters that allow offered, output and discard accounting to occur for the policer. An egress policer has multiple types of offered packets (soft in-profile and out-of-profile from ingress and hard in-profile and out-of-profile due to egress profile overides) and each of these offered types is interacting with the policers metering and profiling functions resulting in colored output packets (green, yellow and red). Due to the potential large number of egress policers, it is not economical to allocate counters in the forwarding plane for all possible offered packet types and output conditions. Many policers will not be configured with a CIR profiling rate and not all policers will receive explicitly re-profiled offered packets. The stat-mode command allows provisioning of the number of counters each policer requires and how the offered packet types and output conditions should be mapped to the counters.
While a no-stats mode is supported which prevents any packet accounting, the use of the policer’s parent command requires at the policer’s stat-mode to be set at least to the minimal setting so that offered stats are available for the policer’s Fair Information Rate (FIR) to be calculated. Once a policer has been made a child to a parent policer, the stat-mode cannot be changed to no-stats unless the policer parenting is first removed.

Each time the policer’s stat-mode is changed, any previous counter values are lost and any new counters are set to zero.

Each mode uses a certain number of counters per policer instance that are allocated from the forwarding plane’s policer counter resources. If insufficient counters exist to implement a mode on any policer instance, the stat-mode change will fail and the previous mode will continue unaffected for all instances of the policer.

The default stat-mode when a policer is created within the policy is no-stats.

The stat-mode setting defined for the policer in the QoS policy may be overridden on an sla-profile or SAP where the policy is applied. If insufficient policer counter resources exist to implement the override, the stat-mode override command will fail. The previous stat-mode setting active for the policer will continue to be used by the policer.

The no stat-mode command attempts to return the policer’s stat-mode setting to no-stats. The command will fail if the policer is currently configured as a child policer using the policer’s parent command. The no parent command must first be executed for the no stat-mode command to succeed.

### Parameters

**stat-mode** — Specifies the mode of statistics collected by this policer.

### Values

- **no-stats**, **minimal**, **offered-profile-no-cir**, **offered-profile-cir**, **offered-total-cir**

**no-stats** — Counter resource allocation: 0

The no-stats mode is the default stat-mode for the policer. The policer does not have any forwarding plane counters allocated and cannot provide offered, discard and forward statistics. A policer using no-stats cannot be a child to a parent policer and the policers parent command will fail.

When collect-stats is enabled, the lack of counters causes the system to generate the following statistics:

```
a. offered-in = 0
b. offered-out = 0
c. discard-in = 0
d. discard-out = 0
e. forward-in = 0
f. forward-out = 0
```

Counter 0 indicates that the accounting statistic returns a value of zero.

**minimal** — Counter resource allocation: 1

The minimal mode allocates 1 forwarding plane offered counter and one traffic manager discard counter. The forwarding counter is derived by subtracting the discard counter from the offered counter. The counters do not differentiate possible offered types (soft or hard profile) and do not count green or yellow output. This does not prevent the policer from supporting different offered packet types and does not prevent the policer from supporting a CIR rate.

This counter mode is useful when only the most basic accounting information is required.

The counters are used in the following manner:
1. offered <= soft-in-profile-out-of-profile, profile in/out
2. discarded <= Same as 1
3. forwarded <= Derived from 1 – 2

When collect-stats is enabled, the counters are used by the system to generate the following statistics:

a. offered-in = 1
b. offered-out = 0
c. discard-in = 2
d. discard-out = 0
e. forward-in = 3
f. forward-out = 0

Counter 0 indicates that the accounting statistic returns a value of zero.

**offered-profile-no-cir** — Counter resource allocation: 2

The offered-profile-no-cir mode allocates two forwarding plane offered counters and two traffic manager discard counters.

The offered-profile-no-cir mode is most useful when profile based offered, discard and forwarding stats are required from the ingress policer, but a CIR is not being used to recolor the soft in-profile and out-of-profile packets. This mode does not prevent the policer from being configured with a CIR rate.

The counters are used in the following manner:

1. offered-in <= soft-in-profile, profile in
2. offered-out <= soft-out-of-profile, profile out
3. dropped-in <= Same as 1
4. dropped-out <= Same as 2
5. forwarded-in <= Derived from 1 – 3
6. forwarded-out <= Derived from 2 – 4

When collect-stats is enabled, the counters are used by the system to generate the following statistics:

a. offered-in = 1
b. offered-out = 2
c. discard-in = 3
d. discard-out = 4
e. forward-in = 5
f. forward-out = 6

**offered-profile-cir** — Counter resource allocation: 3

The offered-profile-cir mode allocates three forwarding plane offered counters and three traffic manager discard counters.

The offered-profile-cir mode is most useful when profile based offered, discard and forwarding stats are required from the ingress policer and a CIR rate is being used to recolor the soft in-profile and out-of-profile packets.

The counters are used in the following manner:

1. offered-in-that-stayed-green-or-turned-red <= profile in
2. offered-soft-that-turned-green <= soft-in-profile-out-of-profile
3. offered-soft-or-out-that-turned-yellow-or-red <= soft-in-profile-out-of-profile, profile out
4. dropped-in-that-stayed-green-or-turned-red <= Same as 1
5. dropped-soft-that-turned-green <= Same as 2
6. dropped-soft-or-out-that-turned-yellow-or-red <= Same as 3
7. forwarded-in-that-stayed-green <= Derived from 1 – 4
8. forwarded-soft-that-turned-green <= Derived from 2 – 5
9. forwarded-soft-or-out-that-turned-yellow <= Derived from 3 – 6

When collect-stats is enabled, the counters are used by the system to generate the following statistics:

a. offered-in = 1
b. offered-out = 2 + 3
c. discard-in = 4
d. discard-out = 5 + 6
e. forward-in = 7 + 8
f. forward-out = 9

offered-total-cir — Counter resource allocation: 2

The offered-total-cir mode allocates two forwarding plane offered counters and two traffic manager discard counters.

The offered-total-cir mode is most useful when profile based offered stats are not required from the ingress policer and a CIR rate is being used to recolor the soft in-profile and out-of-profile packets.

The counters are used in the following manner:

1. offered-that-turned-green <= soft-in-profile-out-of-profile, profile in/out
2. offered-that-turned-yellow-or-red <= soft-in-profile-out-of-profile, profile in/out
3. dropped-offered-that-turned-green <= Same as 1
4. dropped-offered-that-turned-yellow-or-red <= Same as 2
5. forwarded-offered-that-turned-green <= Derived from 1 – 3
6. forwarded-offered-that-turned-yellow <= Derived from 2 – 4

When collect-stats is enabled, the counters are used by the system to generate the following statistics:

a. offered-in = 1 + 2  (Or 1 and 2 could be summed on b)
b. offered-out = 0
c. discard-in = 3
d. discard-out = 4
e. forward-in = 5
f. forward-out = 6
Counter 0 indicates that the accounting statistic returns a value of zero.

qinq-mark-top-only

Syntax
[no] qinq-mark-top-only

Context
config>service>epipe>sap>egress

Description
When enabled (the encapsulation type of the access port where this SAP is defined as qinq), the qinq-mark-top-only command specifies which P-bits/DEI bit to mark during packet egress. When disabled, both set of P-bits/DEI bit are marked. When the enabled, only the P-bits/DEI bit in the top Q-tag are marked.

Default
no qinq-mark-top-only

multi-service-site

Syntax
multi-service-site customer-site-name
no multi-service-site

Context
config>service>epipe>sap

Description
This command associates the SAP with a customer-site-name. If the specified customer-site-name does not exist in the context of the service customer ID an error occurs and the command will not execute. If customer-site-name exists, the current and future defined queues on the SAP (ingress and egress) will attempt to use the scheduler hierarchies created within customer-site-name as parent schedulers.

The no form of the command removes the SAP from any multi-service customer site the SAP belongs to. Removing the site can cause existing or future queues to enter an orphaned state.

Default
None

customer-site-name — The customer-site-name must exist in the context of the customer-id defined as the service owner. If customer-site-name exists and local scheduler policies have not been applied to the SAP, the current and future queues defined on the SAP will look for their parent schedulers within the scheduler hierarchies defined on customer-site-name.

Values
Any valid customer-site-name created within the context of the customer-id.

ring-node

Syntax
ring-node ring-node-name
no ring-node

Context
config>service>epipe>sap

Description
This command configures a multi-chassis ring-node for this SAP.

The no form of the command removes the name from the configuration.
Default none

tod-suite

Syntax tod-suite tod-suite-name

no tod-suite

Context config>service>epipe>sap

Description This command applies a time-based policy (filter or QoS policy) to the service SAP. The suite name must already exist in the config>cron context.

Default no tod-suite

Parameters tod-suite-name — Specifies collection of policies (ACLs, QoS) including time-ranges that define the full or partial behavior of a SAP. The suite can be applied to more than one SAP.

transit-policy

Syntax transit-policy prefix prefix-aasub-policy-id

no transit-policy

Context config>service>epipe>sap

Description This command assigns a transit policy id.

The no form of the command removes the transit policy ID from the spoke SDP configuration.

Default no transit-policy

Parameters prefix-aasub-policy-id — Specifies the transit policy ID.

Values 1 — 65535

accounting-policy

Syntax accounting-policy acct-policy-id

no accounting-policy

Context config>service>apipe>sap

config>service>epipe>sap

config>service>epipe>spoke-sdp

Description This command creates the accounting policy context that can be applied to a SAP.

An accounting policy must be defined before it can be associated with a SAP. If the policy-id does not exist, an error message is generated.

A maximum of one accounting policy can be associated with a SAP at one time. Accounting policies are configured in the config>log context.
The `no` form of this command removes the accounting policy association from the SAP, and the accounting policy reverts to the default.

**Default**
Default accounting policy.

**Parameters**
`acct-policy-id` — Enter the accounting `policy-id` as configured in the `config>log>accounting-policy` context.

**Values**
1 — 99

### bandwidth

**Syntax**
`bandwidth bandwidth`
`no bandwidth`

**Context**
`config>service>epipe>spoke-sdp`

**Description**
This command specifies the bandwidth to be used for VLL bandwidth accounting by the VLL CAC feature.

The service manager keeps track of the available bandwidth for each SDP. The maximum value is the sum of the bandwidths of all constituent LSPs in the SDP. The SDP available bandwidth is adjusted by the user configured booking factor.

If an LSP consists of a primary and many secondary standby LSPs, then the bandwidth used in the maximum SDP available bandwidth is that of the active path. Any change to and LSP active path bandwidth will update the maximum SDP available bandwidth. Note however that a change to any constituent LSP bandwidth due to re-signaling of the primary LSP path or the activation of a secondary path which causes overbooking of the maximum SDP available bandwidth causes a warning and a trap to be issued but no further action is taken. The activation of a bypass or detour LSP in the path of the primary LSP does not change the maximum SDP available bandwidth.

When the user binds a VLL service to this SDP, an amount of bandwidth equal to bandwidth is subtracted from the SDP available bandwidth adjusted by the booking factor. When the user deletes this VLL service binding from this SDP, an amount of bandwidth equal to bandwidth is added back into the SDP available bandwidth.

If the total SDP available bandwidth when adding this VLL service is about to overbook, a warning is issued and the binding is rejected. This means that the spoke-sdp bandwidth does not update the maximum SDP available bandwidth. In this case, the spoke-sdp is put in operational down state and a status message of “pseudowire not forwarding” is sent to the remote SR-Series PE node. A trap is also generated. The service manager will not put the spoke-sdp into operational UP state until the user performs a shutdown/no-shutdown of the spoke-sdp and the bandwidth check succeeds. Thus, the service manager will not automatically audit spoke-sdp’s subsequently to their creation to check if bandwidth is available.

If the VLL service contains an endpoint with multiple redundant spoke-sdp’s, each spoke-sdp will have its bandwidth checked against the available bandwidth of the corresponding SDP.

If the VLL service performs a pseudowire switching (VC switching) function, each spoke-sdp is separately checked for bandwidth against the corresponding SDP.

Note this feature does not alter the way service packets are sprayed over multiple RSVP LSPs, which are part of the same SDP. In other words, by default load balancing of service packets occurs over the
SDP LSP’s based on service-id, or based on a hash of the packet header if ingress SAP shared queuing is enabled. In both cases, the VLL bandwidth is not checked against the selected LSP(s) available bandwidth but on the total SDP available bandwidth. Thus, if there is a single LSP per SDP, these two match.

If class-forwarding is enabled on the SDP, VLL service packets are forwarded to the SDP LSP which the packet forwarding class maps to, or if this is down to the default LSP. However, the VLL bandwidth is not checked against the selected LSP available bandwidth but on the total SDP available bandwidth. If there is a single LSP per SDP, these two match.

If a non-zero bandwidth is specified for a VLL service and attempts to bind the service to an LDP or a GRE SDP, a warning is issued that CAC failed but the VLL is established. A trap is also generated.

The no form of the command reverts to the default value.

Values 0 — 100000000, max in units of kilobits/sec.
Default 0

**block-on-peer-fault**

**Syntax** [no] block-on-peer-fault

**Context** config>service>epipe>spoke-sdp

**Description** When enabled, this command blocks the transmit direction of a PW when any of the following PW status codes is received from the far end PE:

- 0x00000001 Pseudowire Not Forwarding
- 0x00000002 Local Attachment Circuit (ingress) Receive Fault
- 0x00000004 Local Attachment Circuit (egress) Transmit Fault
- 0x00000008 Local PSN-facing PW (ingress) Receive Fault
- 0x00000010 Local PSN-facing PW (egress) Transmit Fault

The transmit direction is unblocked when the following PW status code is received:

- 0x00000000 Pseudowire forwarding (clear all failures)

This command is mutually exclusive with no pw-status-signaling, and standby-signaling-slave. It is not applicable to spoke SDPs forming part of an MC-LAG or spoke SDPs in an endpoint.

Default no block-on-peer-fault

**cflowd**

**Syntax** [no] cflowd

**Context** config>service>epipe>sap

**Description** This command enables cflowd to collect traffic flow samples through a service interface (SAP) for analysis. When cflowd is enabled on an ethernet service SAP, the ethernet traffic can be sampled and

---

7950 SR OS Services Guide  Page 435
processed by the system’s cflowd engine and exported to IPFIX collectors with the l2-ip template enabled.

cflowd is used for network planning and traffic engineering, capacity planning, security, application and user profiling, performance monitoring, usage-based billing, and SLA measurement. When cflowd is enabled at the SAP level, all packets forwarded by the interface are subjected to analysis according to the cflowd configuration.

For L2 services, only ingress sampling is supported.

**Default**

no cflowd

---

### collect-stats

**Syntax**

[n] collect-stats

**Context**

config>service>cpipe>spoke-sdp  
cfg>service>epipe>spoke-sdp  
cfg>service>epipe>sap

**Description**

This command enables accounting and statistical data collection for either the SAP, network port, or IP interface. When applying accounting policies the data, by default, is collected in the appropriate records and written to the designated billing file.

When the **no collect-stats** command is issued the statistics are still accumulated by the cards. However, the CPU will not obtain the results and write them to the billing file. If a subsequent **collect-stats** command is issued then the counters written to the billing file include all the traffic while the **no collect-stats** command was in effect.

**Default**

no collect-stats

---

### cpu-protection

**Syntax**

cpu-protection policy-id [mac-monitoring] [eth-cfm-monitoring [aggregate][car]]  
no cpu-protection

**Context**

config>service>apipe>sap  
cfg>service>epipe>spoke-sdp  
cfg>service>epipe>sap

**Description**

This command assigns an existing CPU protection policy to the associated service SAP. The CPU protection policies are configured in the **config/sys/security/cpu-protection** context.

**Default**

cpu-protection 254 (for access interfaces)  
cpu-protection 255 (for network interfaces)

The configuration of no cpu-protection returns the interface/SAP to the default policies as shown above.
If no CPU protection policy is assigned to a service SAP then the default policy is used to limit the overall-rate.

**Parameters**

- **policy-id** — Specifies an existing CPU protection policy.
  
  **Values**
  
  1 — 255

- **mac-monitoring** — This keyword enables MAC monitoring.

- **eth-cfm-monitoring** — This keyword enables Ethernet Connectivity Fault Management monitoring.

- **aggregate** — This keyword applies the rate limit to the sum of the per peer packet rates.

- **car** — (Committed Access Rate) This keyword causes Eth-CFM packets to be ignored when enforcing the overall-rate.

### dist-cpu-protection

**Syntax**

- dist-cpu-protection *policy-name*
- no dist-cpu-protection

**Context**

- config>service>epipe>sap
- config>service>apipe>sap
- config>service>cpipe>sap
- config>service>fpipe>sap
- config>service>ipipe>sap

**Description**

This command assigns a Distributed CPU Protection (DCP) policy to the SAP. Only a valid created DCP policy can be assigned to a SAP or a network interface (note that this rule does not apply to templates such as an msap-policy)

**Default**

- no dist-cpu-protection

### ethernet

**Syntax**

- ethernet

**Context**

- config>service>epipe>sap

**Description**

Use this command to configure Ethernet properties in this SAP.

### llf

**Syntax**

- [no] llf

**Context**

- config>service>epipe>sap>ethernet

**Description**

This command enables Link Loss Forwarding (LLF) on an Ethernet port or an ATM port. This feature provides an end-to-end OAM fault notification for Ethernet VLL service. It brings down the Ethernet port (Ethernet LLF) towards the attached CE when there is a local fault on the Pseudowire or service,
or a remote fault on the SAP or pseudowire, signaled with label withdrawal or T-LDP status bits. It ceases when the fault disappears.

The Ethernet port must be configured for null encapsulation.
ETH-CFM Service Commands

eth-cfm

Syntax  eth-cfm
Context  config>service>epipe>sap
        config>service>epipe>sdp

This command enables the context to configure ETH-CFM parameters.

ais-enable

Syntax  [no] ais-enable
Context  config>service>epipe>sap>eth-cfm
        config>service>epipe>sap>eth-cfm>mep
        config>service>epipe>sap>eth-cfm>mep

Description  This command enables the generation and the reception of AIS messages.

interface-support-enable

Syntax  [no] interface-support-enable
Context  config>service>epipe>sap>eth-cfm>mep>ais
        config>service>epipe>sdp>eth-cfm>mep>ais

Description  This command enables the AIS function to consider the operational state of the entity on which it is configured. With this command, ETH-AIS on DOWN MEPS will be triggered and cleared based on the operational status of the entity on which it is configured. If CCM is also enabled then transmission of the AIS PDU will be based on either the non operational state of the entity or on ANY CCM defect condition. AIS generation will cease if BOTH operational state is UP and CCM has no defect conditions. If the MEP is not CCM enabled then the operational state of the entity is the only consideration assuming this command is present for the MEP.

Default  no interface-support-enabled (AIS will not be generated or stopped based on the state of the entity on) which the DOWN MEP is configured.

client-meg-level

Syntax  client-meg-level [/[level [level ...]]
        no client-meg-level
Context  config>service>epipe>sap>eth-cfm>mep
**VLL SAP Commands**

`config>service>epipe>spoke-sdp>eth-cfm>aid-enable`

**Description**
This command configures the client maintenance entity group (MEG) level(s) to use for AIS message generation. Up to 7 levels can be provisioned with the restriction that the client MEG level must be higher than the local MEG level.

**Parameters**
- `level` — Specifies the client MEG level.
  - **Values**
    - `1` — 7
  - **Default**
    - 1

**interval**

**Syntax**
interval `{1 | 60}
no interval`

**Context**
`config>service>epipe>spap>eth-cfm>mep
config>service>epipe>spoke-sdp>eth-cfm>aid-enable`

**Description**
This command specifies the transmission interval of AIS messages in seconds.

**Parameters**
- `1 | 60` — The transmission interval of AIS messages in seconds.
  - **Default**
    - 1

**priority**

**Syntax**
priority `priority-value`
no priority

**Context**
`config>service>epipe>spap>eth-cfm>mep
config>service>epipe>spoke-sdp>eth-cfm>aid-enable`

**Description**
This command specifies the priority of AIS messages originated by the node.

**Parameters**
- `priority-value` — Specify the priority value of the AIS messages originated by the node.
  - **Values**
    - `0` — 7
  - **Default**
    - 1

**mep**

**Syntax**
mep `mep-id domain md-index association ma-index [direction {down}]`
no mep `mep-id` `domain md-index association ma-index` [primary-valn-enable]
[vlan vlan-id]

**Context**
`config>service>epipe>spap>eth-cfm
config>service>epipe>spoke-sdp>eth-cfm`
**Description**

This command provisions the maintenance endpoint (MEP).

The **no** form of the command reverts to the default values.

**Parameters**

* `mep-id` — Specifies the maintenance association end point identifier.

  **Values**
  
  1 — 81921

* `md-index` — Specifies the maintenance domain (MD) index value.

  **Values**
  
  1 — 4294967295

* `ma-index` — Specifies the MA index value.

  **Values**
  
  1 — 4294967295

* `direction down` — Indicates the direction in which the maintenance association (MEP) faces on the bridge port. The UP direction is not supported for all Fpipe services.

  **down** — Sends ETH-CFM messages away from the MAC relay entity.

* `primary-vlan-enable` — Provides a method for linking the MIP with the primary VLAN configured under the bridge-identifier for the MA. This is only allowed if the mhf-creation method is static. MIPs can not be changed from or to primary vlan functions without first being deleted. This must be configured as part of the creation step and can only be changed by deleting the MEP and recreating it. Primary VLANs are only supported under Ethernet SAPs.

  **Vlan** — A required parameter when including primary-vlan-enable. Provides a method for associating the VLAN under the bridge-identifier under the MA with the MIP.

  **Vlan-id** — Must match the vlan-id under the bridge-identifier for the MA that is appropriate for this service.

  **Values**
  
  0 — 4094

**ccm-enable**

**Syntax**

```
[no] ccm-enable
```

**Context**

**Description**

This command enables the generation of CCM messages.

The **no** form of the command disables the generation of CCM messages.

**ccm-ltm-priority**

**Syntax**

```
ccm-ltm-priority priority
no ccm-ltm-priority
```

**Context**

**Description**

This command specifies the priority value for CCMs and LTMs transmitted by the MEP.

The **no** form of the command removes the priority value from the configuration.

**Default**

The highest priority on the bridge-port.
Parameters  

priority — Specifies the priority of CCM and LTM messages.

Values  

0 — 7

ccm-padding-size

Syntax  

ccm-padding-size  ccm-padding

no  ccm-padding-size  ccm-padding

Context  

config>service>epipe>sdp>eth-cfm>mep
config>service>epipe>spoke-sdp>eth-cfm>mep
config>service>vpls>sap>eth-cfm>mep
config>service>vpls>spoke-sdp>eth-cfm>mep
config>service>vpls>mesh-sdp>eth-cfm>mep
config>service>vpls>sap>eth-cfm>mep
config>service>vpls>spoke-sdp>eth-cfm>mep
config>service>vpls>mesh-sdp>eth-cfm>mep
config>service>ies>if>sap>eth-cfm>mep
config>service>ies>if>spoke-sdp>eth-cfm>mep
config>service>vprn>if>sap>eth-cfm>mep
config>service>vprn>if>spoke-sdp>eth-cfm>mep
config>port>ethernet>eth-cfm>mep
config>lag>eth-cfm>eth-cfm>mep
config>router>if>eth-cfm>mep

Description  

Set the byte size of the optional Data TLV to be included in the ETH-CC PDU. This will increase the size of the ETH-CC PDU by the configured value. The base size of the ETH-CC PDU, including the Interface Status TLV and Port Status TLV, is 83 bytes not including the Layer Two encapsulation. CCM padding is not supported when the CCM-Interval is less than one second.

Default  

[no] ccm-padding-size

Parameters  

ccm-padding — specifies the byte size of the Optional Data TLV

Values  

3 — 1500

csf-enable

Syntax  

[no]  csf-enable

Context  

config>service>epipe>sap>eth-cfm>mep
config>service>epipe>spoke-sdp>eth-cfm>mep

Description  

This command enables the reception and local processing of ETH-CSF frames.

multiplier

Syntax  

multiplier  multiplier-value

no  multiplier
### ccm-tlv-ignore

**Syntax**

```
ccm-tlv-ignore [interface-status][port-status]
```

**Context**

- `config>port>ethernet>eth-cfm>mep`
- `config>lag>eth-cfm>mep`
- `config>router>interface>eth-cfm>mep`

**Description**

This command allows the receiving MEP to ignore the specified TLVs in CCM PDU. Ignored TLVs will be reported as absent and will have no impact on the MEP state machine.

The `no` form of the command means the receiving MEP will process all recognized TLVs in the CCM PDU.

**Default**

`no ccm-tlv-ignore`

**Parameters**

- `interface-status` — ignores the interface status TLV on reception.
- `port-status` — ignores the port status TLV on reception.

### eth-test-enable

**Syntax**

```
[no] eth-test-enable
```

**Context**

- `config>service>epipe>sap>eth-cfm>mep`
- `config>service>epipe>spoke-sdp>eth-cfm>mep`
- `config>service>epipe>sap>mep`

**Description**

For this test to work, operators need to configure ETH-test parameters on both sender and receiver nodes. The ETH-test then can be done using the following OAM commands:

```
oam eth-cfm eth-test mac-address mep mep-id domain md-index association ma-index [priority priority] [data-length data-length]
```

A check is performed for both the provisioning and test to ensure the MEP is an Y.1731 MEP (MEP provisioned with domain format none, association format icc-based). If not, the operation fails. An error message in the CLI and SNMP indicates the problem.
bit-error-threshold

Syntax: bit-error-threshold errors
no bit-error-threshold

Context: config>service>epipe>sap>eth-cfm>mep>eth-test-enable

Description: This command is used to specify the threshold value of bit errors.

test-pattern

Syntax: test-pattern {all-zeros | all-ones} [crc-enable]
no test-pattern

Context: config>service>epipe>spoke-sdp>eth-cfm>mep>eth-test-enable
config>service>epipe>sap>mep>eth-test-enable

Description: This command configures the test pattern for eth-test frames.

The no form of the command removes the values from the configuration.

Default: all-zeros

Parameters:

all-zeros — Specifies to use all zeros in the test pattern.
all-ones — Specifies to use all ones in the test pattern.
crc-enable — Generates a CRC checksum.

fault-propagation-enable

Syntax: fault-propagation-enable {use-if-tlv | suspend-ccm}
no fault-propagation-enable

Context: config>service>epipe>sap>eth-cfm>mep
config>service>epipe>spoke-sdp>eth-cfm>mep

Description: This command configures the fault propagation for the MEP.

Parameters:

use-if-tlv — Specifies to use the interface TLV.
suspend-ccm — Specifies to suspend the continuity check messages.

low-priority-defect

Syntax: low-priority-defect {allDef | macRemErrXcon | remErrXcon | errXcon | xcon | noXcon}

Context: config>service>epipe>spoke-sdp>eth-cfm>mep
config>service>epipe>sap>eth-cfm>mep
This command specifies the lowest priority defect that is allowed to generate a fault alarm.

**Default**

macRemErrXcon

**Values**

- allDef: DefRDICCM, DefMACstatus, DefRemoteCCM, DefErrorCCM, and DefXconCCM
- macRemErrXcon: Only DefMACstatus, DefRemoteCCM, DefErrorCCM, and DefXconCCM
- remErrXcon: Only DefRemoteCCM, DefErrorCCM, and DefXconCCM
- errXcon: Only DefErrorCCM and DefXconCCM
- xcon: Only DefXconCCM; or
- noXcon: No defects DefXcon or lower are to be reported

**mac-address**

**Syntax**

mac-address *mac-address*

no mac-address

**Context**

```
config>service>epipe>spoke-sdp>eth-cfm>mep
config>service>epipe>sap>eth-cfm>mep
```

**Description**

This command specifies the MAC address of the MEP.

The **no** form of this command reverts the MAC address of the MEP back to that of the port (if the MEP is on a SAP) or the bridge (if the MEP is on a spoke SDP).

**Parameters**

- *mac-address* — Specifies the MAC address of the MEP.
  
  **Values**
  
  6-byte unicast mac-address (xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx) of the MEP. Using the all zeros address is equivalent to the no form of this command.

**one-way-delay-threshold**

**Syntax**

one-way-delay-threshold *seconds*

**Context**

```
config>service>vpls>sap>eth-cfm>mep
```

**Description**

This command enables/disables eth-test functionality on MEP.

**Parameters**

- *seconds* — Specifies the one way delay threshold in seconds.
  
  **Values**
  
  0-600

  **Default**
  
  3
mip

Syntax

mip [mac mac-address] primary-vlan-enable [vlan vlan-id]
mip default-mac
no mip

Context
config>service>epipe>sap>eth-cfm

Description
This command allows Maintenance Intermediate Points (MIPs). The creation rules of the MIP are dependant on the mhf-creation configuration for the MA. This MIP option is only available for default and static mhf-creation methods.

Parameters

mac — provides a method for manually configuring the MIP MAC.

mac-address — Specifies the MAC address of the MIP.

Values
6-byte mac-address in the form of xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx of the MIP. The MAC must be unicast. Using the all zeros address is equivalent to the no form of this command.

default-mac — Using the no command deletes the MIP. If the operator wants to change the mac back to the default mac without having to delete the MIP and reconfiguring this command is useful.

primary-vlan-enable — Provides a method for linking the MIP with the primary VLAN configured under the bridge-identifier for the MA. This is only allowed if the mhf-creation method is static. MIPs can not be changed from or to primary vlan functions without first being deleted. This must be configured as part of the creation step and can only be changed by deleting the MEP and recreating it. Primary VLANs are only supported under Ethernet SAPs.

vlan — A required parameter when including primary-vlan-enable. Provides a method for associating the VLAN under the bridge-identifier under the MA with the MIP.

vlan-id — Must match the vlan-id under the bridge-identifier for the MA that is appropriate for this service.

Values
0 — 4094

Default
no mip

squelch-ingress-levels

Syntax

[no] squelch-ingress-levels [md-level [md-level...]]

Context
config>service>epipe>sap>eth-cfm
config>service>epipe>spoke-sdp>eth-cfm
config>service>vpls>sap>eth-cfm
config>service>vpls>spoke-sdp>eth-cfm
config>service>vpls>mesh-sdp>eth-cfm
config>service>ies>interface>sap>eth-cfm
config>service>ies>interface>spoke-sdp>eth-cfm
config>service>ies>subscriber-interface>group-interface>sap>eth-cfm
config>service>vprn>interface>sap>eth-cfm
config>service>vprn>interface>spoke-sdp>eth-cfm
Description
This command defines the levels of the ETH-CFM PDUs that will silently be discarded on ingress into the SAP or SDP Binding from the wire. All ETH-CFM PDUs inbound to the SAP or SDP binding will be dropped that match the configured levels without regard for any other ETH-CFM criteria. No statistical information or drop count will be available for any ETH-PDU that is silently discarded by this option. The operator must configure a complete contiguous list of md-levels up to the highest level that will be dropped. The command must be retyped in complete form to modify a previous configuration, if the operator does not want to delete it first.

The no form of the command removes the silent discarding of previously matching ETH-CFM PDUs.

Default
[no] squelch-ingress-levels

Parameters
md-level — Identifies the level.

Values
[0..7]

tunnel-fault

Syntax
tunnel-fault {accept | ignore}

Context
config>service>epipe>eth-cfm
config>service>epipe>sap>eth-cfm

Description
Allows the individual service SAPs to react to changes in the tunnel MEP state. When tunnel-fault accept is configured at the service level, the SAP will react according to the service type, Epipe will set the operational flag and VPLS, IES and VPRN SAP operational state will become down on failure or up on clear. This command triggers the OAM mapping functions to mate SAPs and bindings in an Epipe service as well as setting the operational flag. If AIS generation is the requirement for the Epipe services this command is not required. See the ais-enable command under config>service>epipe>sap>eth-cfm>ais-enable context for more details. This works in conjunction with the tunnel-fault accept on the individual SAPs. Both must be set to accept to react to the tunnel MEP state. By default the service level command is “ignore” and the sap level command is “accept”. This means simply changing the service level command to “accept” will enable the feature for all SAPs. This is not required for Epipe services that only wish to generate AIS on failure.

Parameters
accept — Share fate with the facility tunnel MEP
ignore — Do not share fate with the facility tunnel MEP

Default
ignore (Service Level)
accept (SAP Level for Epipe and VPLS)
Service Filter and QoS Policy Commands

egress

Syntax: `egress`

Context:
- `config>service>epipe>spoke-sdp`
- `config>service>epipe.sap`

Description: This command enables the context to configure egress SAP parameters.

force-vlan-vc-forwarding

Syntax: `[no] force-vlan-vc-forwarding`

Context:
- `config>service>epipe>spoke-sdp`
- `config>service>vpls>mesh-sdp`
- `config>service>vpls>spoke-sdp`

Description: This command forces vc-vlan-type forwarding in the data path for spoke and mesh SDPs which have either vc-type. This command is not allowed on vlan-vc-type SDPs.

The `no` version of this command sets default behavior.

Default: Per default this feature is disabled

ingress

Syntax: `ingress`

Context:
- `config>service>epipe>spoke-sdp`
- `config>service>epipe.sap`
- `config>service>epipe.sap`

Description: This command enables the context to configure ingress SAP Quality of Service (QoS) policies.

If no sap-ingress QoS policy is defined, the system default sap-ingress QoS policy is used for ingress processing.

cookie

Syntax: `cookie cookie`

Context: `config>service>epipe>spoke-sdp>egress>l2tpv3`
config>service>epipe*spoke-sdp>ingress>l2tpv3

**Description**
This command configures the RX/TX cookie for L2TPv3 spoke-SDPs for EPipe services. The RX cookie must match the configured TX cookie on a far-end node, while the TX cookie must match the configured RX cookie on a far-end node.

The purpose of the cookie is to provide validation against misconfiguration of service endpoints, and to ensure that the right service egress is being used.

A cookie is not mandatory.

**Default**
no cookie

**Parameters**
cookie — Specify a 64-bit colon separated hex value.

**filter**

**Syntax**
filter [ip ip-filter-id]
filter [mac mac-filter-id]
no filter [ip ip-filter-id]
no filter [mac mac-filter-id]

**Context**
config>service>epipe>sap>egress
config>service>epipe>sap>ingress

**Description**
This command associates an IP filter policy with an ingress or egress Service Access Point (SAP) or IP interface.

Filter policies control the forwarding and dropping of packets based on IP matching criteria. Only one filter can be applied to a SAP at a time.

The filter command is used to associate a filter policy with a specified filter-id with an ingress or egress SAP. The filter-id must already be defined before the filter command is executed. If the filter policy does not exist, the operation will fail and an error message returned.

IP filters apply only to RFC 2427-routed IP packets. Frames that do not contain IP packets will not be subject to the filter and will always be passed, even if the filter's default action is to drop.

The no form of this command removes any configured filter ID association with the SAP or IP interface. The filter ID itself is not removed from the system.

**Special Cases**
**Epipe** — Both MAC and IP filters are supported on an Epipe service SAP.

**Parameters**
ip ip-filter-id — Specifies IP filter policy. The filter ID must already exist within the created IP filters.

Values 1 — 65535

mac mac-filter-id — Specifies the MAC filter policy. The specified filter ID must already exist within the created MAC filters. The filter policy must already exist within the created MAC filters.

Values 1 — 65535

Values
VLL SAP Commands

qos

Syntax

```
qos policy-id [shared-queuing] [fp-redirect-group queue-group-name instance instance-id]
```

```
no qos
```

Context

```
cfg>service>apipe>sap>ingress
cfg>service>fpipe>sap>ingress
cfg>service>ipipe>sap>ingress
cfg>service>epipe>sap>ingress
```

Description

This command associates a Quality of Service (QoS) policy with an ingress Service Access Point (SAP).

QoS ingress and egress policies are important for the enforcement of SLA agreements. The policy ID must be defined prior to associating the policy with a SAP. If the policy-id does not exist, an error will be returned.

The `qos` command, when used under the ingress context, is used to associate ingress QoS policies. The `qos` command only allows ingress policies to be associated on SAP ingress and egress policies on SAP egress. Attempts to associate a QoS policy of the wrong type returns an error.

Only one ingress and one egress QoS policy can be associated with a SAP at one time. Attempts to associate a second QoS policy of a given type will return an error.

By default, if no specific QoS policy is associated with the SAP for ingress or egress, so the default QoS policy is used.

The `no` form of this command removes the QoS policy association from the SAP, and the QoS policy reverts to the default.

Default

`none`

Parameters

```
policy-id — The ingress policy ID to associate with SAP or IP interface on ingress. The policy ID must already exist.
```

Values

```
1 — 65535
```

```
shared-queuing — This keyword can only be specified on SAP ingress. The shared-queueing keyword specifies the shared queue policy will be used by this SAP. When the value of this object is null, the SAP will use individual ingress QoS queues, instead of the shared ones.
```

```
multipoint-shared — This keyword specifies that this queue-id is for multipoint forwarded traffic only. This queue-id can only be explicitly mapped to the forwarding class multicast, broadcast, or unknown unicast ingress traffic. Attempting to map forwarding class unicast traffic to a multipoint queue generates an error; no changes are made to the current unicast traffic queue mapping.
```

A queue must be created as multipoint. The `multipoint` designator cannot be defined after the queue is created. If an attempt is made to modify the command to include the `multipoint` keyword, an error is generated and the command will not execute.

The `multipoint` keyword can be entered in the command line on a pre-existing multipoint queue to edit queue-id parameters.

```
Default Present (the queue is created as non-multipoint).
```

```
Values Multipoint or not present.
```
**fp-redirect-group** — This keyword can only be used on SAP ingress and associates a SAP ingress with an instance of a named queue group template on the ingress forwarding plane of a given IOM/IMM/XMA. The queue-group-name and instance instance-id are mandatory parameters when executing the command.

**queue-group-name** — Specifies the name of the queue group to be instance on the forwarding plane of the IOM/IMM/XMA, up to 32 characters in length. The queue-group-name must correspond to a valid ingress forwarding plane queue group, created under `config>card>fp>ingress>access`.

**instance instance-id** — Specifies the instance of the named queue group on the IOM/IMM/XMA ingress forwarding plane.

---

**QOS**

**Syntax**

```
qos policy-id [port-redirect-group queue-group-name instance instance-id]
no qos
```

**Context**

```
config>service>apipe>sap>egress
cfg>service>cpipe>sap>egress
cfg>service>fpipe>sap>egress
cfg>service>ipipe>sap>egress
cfg>service>epipe>sap>egress
```

**Description**

This command associates a Quality of Service (QoS) policy with an egress Service Access Point (SAP).

QoS ingress and egress policies are important for the enforcement of SLA agreements. The policy ID must be defined prior to associating the policy with a SAP. If the policy-id does not exist, an error will be returned.

The `qos` command, when used under the egress context, is used to associate egress QoS policies.

The `qos` command only allows ingress policies to be associated on SAP ingress and egress policies on SAP egress. Attempts to associate a QoS policy of the wrong type returns an error.

Only one ingress and one egress QoS policy can be associated with a SAP at one time. Attempts to associate a second QoS policy of a given type will return an error.

By default, if no specific QoS policy is associated with the SAP for ingress or egress, so the default QoS policy is used.

The `no` form of this command removes the QoS policy association from the SAP, and the QoS policy reverts to the default.

**Default**

```
none
```

**Parameters**

- `policy-id` — The egress policy ID to associate with SAP on egress. The policy ID must already exist.
  - **Values**
    - `1 — 65535`

- `port-redirect-group` — This keyword associates a SAP egress with an instance of a named queue group template on the egress port of a given IOM/IMM/XMA. The queue-group-name and instance instance-id are mandatory parameters when executing the command.
queue-group-name — Specifies the name of the egress port queue group of the IOM/IMM/XMA, up to 32 characters in length. The queue-group-name must correspond to a valid egress queue group, created under config>port>ethernet>access>egress.

instance instance-id — Specifies the instance of the named egress port queue group on the IOM/IMM/XMA.

Values

| 1 — 40960 |

Default 1

queue-override

Syntax [no] queue-override

Context config>service>apipe>sap>egress
config>service>apipe>sap>ingress
config>service>cpipe>sap>egress
config>service>cpipe>sap>ingress
config>service>fpipe>sap>egress
config>service>fpipe>sap>ingress
config>service>ipipe>sap>egress
config>service>ipipe>sap>ingress
config>service>epipe>sap>egress
config>service>epipe>sap>ingress

Description This command enables the context to configure override values for the specified SAP egress or ingress QoS queue. These values override the corresponding ones specified in the associated SAP egress or ingress QoS policy. If the policy was created as a template policy, this command overrides the parameter and its description and queue parameters in the policy.

queue

Syntax queue queue-id [create]
no queue queue-id

Context config>service>apipe>sap>egress>queue-override
config>service>apipe>sap>ingress>queue-override
config>service>cpipe>sap>egress>queue-override
config>service>cpipe>sap>ingress>queue-override
config>service>fpipe>sap>egress>queue-override
config>service>fpipe>sap>ingress>queue-override
config>service>ipipe>sap>egress>queue-override
config>service>ipipe>sap>ingress>queue-override
config>service>epipe>sap>egress>queue-override
config>service>epipe>sap>ingress>queue-override

Description This command specifies the ID of the queue whose parameters are to be overridden.

Parameters queue-id — The queue ID whose parameters are to be overridden.
adaptation-rule

Syntax  adaptation-rule [pir adaptation-rule]] [cir adaptation-rule]]
no adaptation-rule

Context  config>service>epipe>sap>egress>queue-override>queue
config>service>epipe>sap>ingress>queue-override>queue

Description  This command can be used to override specific attributes of the specified queue’s adaptation rule parameters. The adaptation rule controls the method used by the system to derive the operational CIR and PIR settings when the queue is provisioned in hardware. For the CIR and PIR parameters individually, the system attempts to find the best operational rate depending on the defined constraint. The no form of the command removes any explicitly defined constraints used to derive the operational CIR and PIR created by the application of the policy. When a specific adaptation-rule is removed, the default constraints for rate and cir apply.

Default  no adaptation-rule

Parameters  
pir — The pir parameter defines the constraints enforced when adapting the PIR rate defined within the queue queue-id rate command. The pir parameter requires a qualifier that defines the constraint used when deriving the operational PIR for the queue. When the rate command is not specified, the default applies.

cir — The cir parameter defines the constraints enforced when adapting the CIR rate defined within the queue queue-id rate command. The cir parameter requires a qualifier that defines the constraint used when deriving the operational CIR for the queue. When the cir parameter is not specified, the default constraint applies.

adaptation-rule — Specifies the criteria to use to compute the operational CIR and PIR values for this queue, while maintaining a minimum offset.

Values  
max — The max (maximum) keyword is mutually exclusive with the min and closest options. When max is defined, the operational PIR for the queue will be equal to or less than the administrative rate specified using the rate command.

min — The min (minimum) keyword is mutually exclusive with the max and closest options. When min is defined, the operational PIR for the queue will be equal to or greater than the administrative rate specified using the rate command.

closest — The closest parameter is mutually exclusive with the min and max parameter. When closest is defined, the operational PIR for the queue will be the rate closest to the rate specified using the rate command.

avg-frame-overhead

Syntax  avg-frame-overhead percent
no avg-frame-overhead

Context  config>service>epipe>sap>egress>queue-override>queue
Description

This command configures the average frame overhead to define the average percentage that the offered load to a queue will expand during the frame encapsulation process before sending traffic on-the-wire. While the avg-frame-overhead value may be defined on any queue, it is only used by the system for queues that egress a Sonet or SDH port or channel. Queues operating on egress Ethernet ports automatically calculate the frame encapsulation overhead based on a 20 byte per packet rule (8 bytes for preamble and 12 bytes for Inter-Frame Gap).

When calculating the frame encapsulation overhead for port scheduling purposes, the system determines the following values:

- **Offered-load** — The offered-load of a queue is calculated by starting with the queue depth in octets, adding the received octets at the queue and subtracting queue discard octets. The result is the number of octets the queue has available to transmit. This is the packet based offered-load.

- **Frame encapsulation overhead** — Using the avg-frame-overhead parameter, the frame encapsulation overhead is simply the queue’s current offered-load (how much has been received by the queue) multiplied by the avg-frame-overhead. If a queue had an offered load of 10000 octets and the avg-frame-overhead equals 10%, the frame encapsulation overhead would be 10000 x 0.1 or 1000 octets.

For egress Ethernet queues, the frame encapsulation overhead is calculated by multiplying the number of offered-packets for the queue by 20 bytes. If a queue was offered 50 packets then the frame encapsulation overhead would be 50 x 20 or 1000 octets.

- **Frame based offered-load** — The frame based offered-load is calculated by adding the offered-load to the frame encapsulation overhead. If the offered-load is 10000 octets and the encapsulation overhead was 1000 octets, the frame based offered-load would equal 11000 octets.

- **Packet to frame factor** — The packet to frame factor is calculated by dividing the frame encapsulation overhead by the queue’s offered-load (packet based). If the frame encapsulation overhead is 1000 octets and the offered-load is 10000 octets then the packet to frame factor would be 1000 / 10000 or 0.1. When in use, the avg-frame-overhead will be the same as the packet to frame factor making this calculation unnecessary.

- **Frame based CIR** — The frame based CIR is calculated by multiplying the packet to frame factor with the queue’s configured CIR and then adding that result to that CIR. If the queue CIR is set at 500 octets and the packet to frame factor equals 0.1, the frame based CIR would be 500 x 1.1 or 550 octets.

- **Frame based within-cir offered-load** — The frame based within-cir offered-load is the portion of the frame based offered-load considered to be within the frame-based CIR. The frame based within-cir offered-load is the lesser of the frame based offered-load and the frame based CIR. If the frame based offered-load equaled 11000 octets and the frame based CIR equaled 550 octets, the frame based within-cir offered-load would be limited to 550 octets. If the frame based offered-load equaled 450 octets and the frame based CIR equaled 550 octets, the frame based within-cir offered-load would equal 450 octets (or the entire frame based offered-load).

As a special case, when a queue or associated intermediate scheduler is configured with a CIR-weight equal to 0, the system automatically sets the queue’s frame based within-cir offered-load to 0, preventing it from receiving bandwidth during the port scheduler’s within-cir pass.

- **Frame based PIR** — The frame based PIR is calculated by multiplying the packet to frame factor with the queue’s configured PIR and then adding the result to that PIR. If the queue PIR is set to 7500 octets and the packet to frame factor equals 0.1, the frame based PIR would be 7500 x 1.1 or 8250 octets.
Virtual Leased Line Services

- Frame based within-pir offered-load — The frame based within-pir offered-load is the portion of the frame based offered-load considered to be within the frame based PIR. The frame based within-pir offered-load is the lesser of the frame based offered-load and the frame based PIR. If the frame based offered-load equaled 11000 octets and the frame based PIR equaled 8250 octets, the frame based within-pir offered-load would be limited to 8250 octets. If the frame based offered-load equaled 7000 octets and the frame based PIR equaled 8250 octets, the frame based within-pir offered load would equal 7000 octets.

Port scheduler operation using frame transformed rates — The port scheduler uses the frame based rates to figure the maximum rates that each queue may receive during the within-cir and above-cir bandwidth allocation passes. During the within-cir pass, a queue may receive up to its frame based within-cir offered-load. The maximum it may receive during the above-cir pass is the difference between the frame based within-pir offered load and the amount of actual bandwidth allocated during the within-cir pass.

The no form of this command restores the average frame overhead parameter for the queue to the default value of 0 percent. When set to 0, the system uses the packet based queue statistics for calculating port scheduler priority bandwidth allocation. If the no avg-frame-overhead command is executed in a queue-override queue id context, the avg-frame-overhead setting for the queue within the sap-egress QoS policy takes effect.

Default 0

Parameters

percent — This parameter sets the average amount of packet-to-frame encapsulation overhead expected for the queue. This value is not used by the system for egress Ethernet queues.

Values 0.00 — 100.00

burst-limit

Syntax burst-limit (default | size [byte | kilobyte])
no burst-limit

Context config>service>epipe>sap>egress>queue-override>queue
config>service>epipe>sap>ingress>queue-override>queue

Description The queue burst-limit command is used to define an explicit shaping burst size for a queue. The configured size defines the shaping leaky bucket threshold level that indicates the maximum burst over the queue’s shaping rate.

The burst-limit command is supported under the sap-ingress and sap-egress QoS policy queues. The command is also supported under the ingress and egress queue-group-templates queues.

The no form of this command is used to restore the default burst limit to the specified queue. This is equivalent to specifying burst-limit default within the QoS policies or queue group templates. When specified within a queue-override queue context, any current burst limit override for the queue will be removed and the queue’s burst limit will be controlled by its defining policy or template.

Parameters

default — The default parameter is mutually exclusive to specifying an explicit size value. When burst-limit default is executed, the queue is returned to the system default value.

size — When a numeric value is specified (size), the system interprets the value as an explicit burst limit size. The value is expressed as an integer and by default is interpreted as the burst limit in
Kilobytes. If the value is intended to be interpreted in bytes, the byte qualifier must be added following size.

**Values**
1 to 14,000 (14,000 or 14,000,000 depending on bytes or kilobytes)

**Default**
No default for size, use the default keyword to specify default burst limit

**byte** — The bytes qualifier is used to specify that the value given for size must be interpreted as the burst limit in bytes. The byte qualifier is optional and mutually exclusive with the kilobytes qualifier.

**kilobyte** — The kilobyte qualifier is used to specify that the value given for size must be interpreted as the burst limit in Kilobytes. The kilobyte qualifier is optional and mutually exclusive with the bytes qualifier. If neither bytes nor kilobytes is specified, the default qualifier is kilobytes.

### cbs

**Syntax**
```text
cbs size-in-kbytes
no cbs
```

**Context**
```text
config>service>epipe>sap>egress>queue-override>queue
config>service>epipe>sap>ingress>queue-override>queue
```

**Description**
This command can be used to override specific attributes of the specified queue’s CBS parameters. It is permissible, and possibly desirable, to oversubscribe the total CBS reserved buffers for a given access port egress buffer pool. Oversubscription may be desirable due to the potential large number of service queues and the economy of statistical multiplexing the individual queue’s CBS setting into the defined reserved total.

When oversubscribing the reserved total, it is possible for a queue depth to be lower than its CBS setting and still not receive a buffer from the buffer pool for an ingress frame. As more queues are using their CBS buffers and the total in use exceeds the defined reserved total, essentially the buffers are being removed from the shared portion of the pool without the shared in use average and total counts being decremented. This can affect the operation of the high and low priority RED slopes on the pool, causing them to miscalculate when to start randomly to drop packets. If the CBS value is larger than the MBS value, an error will occur, preventing the CBS change.

The **no** form of this command returns the CBS size to the default value.

**Default**
no cbs

**Parameters**
```text
size-in-kbytes — The size parameter is an integer expression of the number of kilobytes reserved for the queue. If a value of 10KBytes is desired, enter the value 10. A value of 0 specifies that no reserved buffers are required by the queue (a minimal reserved size can still be applied for scheduling purposes).
```

**Values**
0 — 131072, default

### high-prio-only

**Syntax**
```text
high-prio-only percent
no high-prio-only
```
Virtual Leased Line Services

**Context**
```
config>service>epipe>sap<gress>queue-override>queue
config>service>epipe>sap<gress>queue-override>queue
```

**Description**
This command can be used to override specific attributes of the specified queue’s high-prio-only parameters. The high-prio-only command configures the percentage of buffer space for the queue, used exclusively by high priority packets.

The priority of a packet can only be set in the SAP ingress QoS policy and is only applicable on the ingress queues for a SAP. The high-prio-only parameter is used to override the default value derived from the network-queue command.

The defined high-prio-only value cannot be greater than the MBS size of the queue. Attempting to change the MBS to a value smaller than the high priority reserve will generate an error and fail execution. Attempting to set the high-prio-only value larger than the current MBS size will also result in an error and fail execution.

The no form of this command restores the default high priority reserved size.

**Parameters**
```percent — The percent parameter is the percentage reserved for high priority traffic on the queue. If a value of 10KBytes is desired, enter the value 10. A value of 0 specifies that none of the MBS of the queue will be reserved for high priority traffic. This does not affect RED slope operation for packets attempting to be queued.
```

**Values**
```0 — 100, default
```

---

**mbs**

**Syntax**
```mbs size [bytes|kilobytes]
no mbs
```

**Context**
```
config>service>epipe>sap<gress>hsmda-queue-override>queue
config>service>epipe>sap<gress>queue-override>queue
```

**Description**
This command can be used to override specific attributes of the specified queue’s MBS parameters. The MBS value is used by a queue to determine whether it has exhausted all of its buffers while enqueuing packets. Once the queue has exceeded the amount of buffers allowed by MBS, all packets are discarded until packets have been drained from the queue.

The sum of the MBS for all queues on an ingress access port can oversubscribe the total amount of buffering available. When congestion occurs and buffers become scarce, access to buffers is controlled by the RED slope a packet is associated with. A queue that has not exceeded its MBS size is not guaranteed that a buffer will be available when needed or that the packet’s RED slope will not force the discard of the packet. Setting proper CBS parameters and controlling CBS oversubscription is one major safeguard to queue starvation (when a queue does not receive its fair share of buffers). Another is properly setting the RED slope parameters for the needs of services on this port or channel. If the CBS value is larger than the MBS value, an error will occur, preventing the MBS change.

The defined high-prio-only value cannot be greater than the MBS size of the queue. Attempting to change the MBS to a value smaller than the high priority reserve will generate an error and fail execution. Attempting to set the high-prio-only value larger than the current MBS size will also result in an error and fail execution.

The no form of this command returns the MBS size assigned to the queue to the default value.

**Default**
```default
```
**Parameters**

- `size-in-kbytes` — The size parameter is an integer expression of the maximum number of kilobytes of buffering allowed for the queue. For a value of 100 kbps, enter the value 100. A value of 0 causes the queue to discard all packets.

**Values**

- `0 — 131072 or default`

**parent**

**Syntax**

```
parent [weight weight] [cir-weight cir-weight]
```

**no parent**

**Context**

```
config>service>epipe>sap>egress>queue-override>queue
config>service>epipe>sap>ingress>queue-override>queue
```

**Description**

This command defines an optional parent scheduler that further governs the available bandwidth given the queue aside from the queue’s PIR setting. When multiple schedulers and/or queues share a child status with the parent scheduler, the `weight` or `level` parameters define how this queue contends with the other children for the parent’s bandwidth.

Checks are not performed to see if a `scheduler-name` exists when the parent command is defined on the queue. Scheduler names are configured in the `config>qos>scheduler-policy>tier level` context. Multiple schedulers can exist with the `scheduler-name` and the association pertains to a scheduler that should exist on the egress SAP as the policy is applied and the queue created. When the queue is created on the egress SAP, the existence of the `scheduler-name` is dependent on a scheduler policy containing the `scheduler-name` being directly or indirectly applied (through a multi-service customer site) to the egress SAP. If the `scheduler-name` does not exist, the queue is placed in the orphaned operational state. The queue will accept packets but will not be bandwidth limited by a virtual scheduler or the scheduler hierarchy applied to the SAP. The orphaned state must generate a log entry and a trap message. The SAP which the queue belongs to must also depict an orphan queue status. The orphaned state of the queue is automatically cleared when the `scheduler-name` becomes available on the egress SAP.

The parent scheduler can be made unavailable due to the removal of a scheduler policy or scheduler. When an existing parent scheduler is removed or inoperative, the queue enters the orphaned state mentioned above and automatically return to normal operation when the parent scheduler is available again.

When a parent scheduler is defined without specifying weight or strict parameters, the default bandwidth access method is weight with a value of 1.

The `no` form of the command removes a child association with a parent scheduler. If a parent association does not currently exist, the command has no effect and returns without an error. Once a parent association has been removed, the former child queue attempts to operate based on its configured rate parameter. Removing the parent association on the queue within the policy takes effect immediately on all queues using the SAP egress QoS policy.

**Parameters**

- `weight weight` — These optional keywords are mutually exclusive to the keyword `level`. `weight` defines the relative weight of this queue in comparison to other child schedulers and queues while vying for bandwidth on the parent `scheduler-name`. Any queues or schedulers defined as weighted receive no parental bandwidth until all strict queues and schedulers on the parent have reached their maximum bandwidth or are idle. In this manner, weighted children are considered to be the lowest priority.
All **weight** values from all weighted active queues and schedulers with a common parent scheduler are added together. Then, each individual active weight is divided by the total, deriving the percentage of remaining bandwidth provided to the queue or scheduler after the strict children are serviced. A weight is considered to be active when the pertaining queue or scheduler has not reached its maximum rate and still has packets to transmit. All child queues and schedulers with a weight of 0 are considered to have the lowest priority level and are not serviced until all strict and non-zero weighted queues and schedulers are operating at the maximum bandwidth or are idle.

**Values** 0 — 100

**Default** 1

cir-weight *cir-weight* — Defines the weight the queue or scheduler will use at the within-cir port priority level (defined by the cir-level parameter). The weight is specified as an integer value from 0 to 100 with 100 being the highest weight. When the cir-weight parameter is set to a value of 0 (the default value), the queue or scheduler does not receive bandwidth during the port schedulers within-cir pass and the cir-level parameter is ignored. If the cir-weight parameter is 1 or greater, the cir-level parameter comes into play.

**Values** 0 — 100

**percent-rate**

**Syntax**

percent-rate *pir-percent* [cir *cir-percent*]

**Context**

config>service>epipe>sap>egress>queue-override>queue

**Description**

The **percent-rate** command supports a queue’s shaping rate and CIR rate as a percentage of the egress port’s line rate. When the rates are expressed as a percentage within the template, the actual rate used per instance of the queue group queue-id will vary based on the port speed. For example, when the same template is used to create a queue group on a 1-Gigabit and a 10-Gigabit Ethernet port, the queue’s rates will be 10 times greater on the 10 Gigabit port due to the difference in port speeds. This enables the same template to be used on multiple ports without needing to use port based queue overrides to modify a queue’s rate to get the same relative performance from the queue.

If the port’s speed changes after the queue is created, the queue’s shaping and CIR rates will be recalculated based on the defined percentage value.

The rate and percent-rate commands override one another. If the current rate for a queue is defined using the percent-rate command and the rate command is executed, the percent-rate values are deleted. In a similar fashion, the percent-rate command causes any rate command values to be deleted. A queue’s rate may dynamically be changed back and forth from a percentage to an explicit rate at anytime.

An egress port queue group queue rate override may be expressed as either a percentage or an explicit rate independent on how the queue's template rate is expressed.

The **no** form of this command returns the queue to its default shaping rate and cir rate. When **no percent-rate** is defined within a port egress queue group queue override, the queue reverts to the defined shaping and CIR rates within the egress queue group template associated with the queue.
Parameters  

pir-percent — The percent-of-line-rate parameter is used to express the queue’s shaping rate as a percentage of line rate. The line rate associated with the queue’s port may dynamically change due to configuration or auto-negotiation. The line rate may also be affected by an egress port scheduler defined max-rate.

Values  Percentage ranging from 0.01 to 100.00. The default is 100.00.

cir cir-percent — The cir keyword is optional and when defined the required percent-of-line-rate CIR parameter expresses the queue’s committed scheduling rate as a percentage of line rate. The line rate associated with the queue’s port may dynamically change due to configuration or auto-negotiation. The line rate may also be affected by an egress port scheduler defined max-rate.

rate

Syntax  

rate pir-rate [cir cir-rate]
no rate

Context  

config>service>epipe>sap>egress>queue-override>queue
config>service>epipe>sap>ingress>queue-override>queue

Description  

This command can be used to override specific attributes of the specified queue’s Peak Information Rate (PIR) and the Committed Information Rate (CIR) parameters.

The PIR defines the maximum rate that the queue can transmit packets out an egress interface (for SAP egress queues). Defining a PIR does not necessarily guarantee that the queue can transmit at the intended rate. The actual rate sustained by the queue can be limited by oversubscription factors or available egress bandwidth.

The CIR defines the rate at which the system prioritizes the queue over other queues competing for the same bandwidth. In-profile packets are preferentially queued by the system at egress and at subsequent next hop nodes where the packet can traverse. To be properly handled as in- or out-of-profile throughout the network, the packets must be marked accordingly for profiling at each hop.

The CIR can be used by the queue’s parent commands cir-level and cir-weight parameters to define the amount of bandwidth considered to be committed for the child queue during bandwidth allocation by the parent scheduler.

The rate command can be executed at any time, altering the PIR and CIR rates for all queues created through the association of the SAP egress QoS policy with the queue-id.

The no form of the command returns all queues created with the queue-id by association with the QoS policy to the default PIR and CIR parameters (max, 0).

Default  

rate max cir 0 — The max default specifies the amount of bandwidth in kilobits per second (thousand bits per second). The max value is mutually exclusive to the pir-rate value.

Parameters  

pir-rate — Defines the administrative PIR rate, in kilobits, for the queue. When the rate command is executed, a valid PIR setting must be explicitly defined. When the rate command has not been executed, the default PIR of max is assumed.

Fractional values are not allowed and must be given as a positive integer.
The actual PIR rate is dependent on the queue’s adaptation-rule parameters and the actual hardware where the queue is provisioned.

**Values**  
1 — 100000000  
**Default**  
max

**cir-rate** — The cir parameter overrides the default administrative CIR used by the queue. When the rate command is executed, a CIR setting is optional. When the rate command has not been executed or the cir parameter is not explicitly specified, the default CIR (0) is assumed. Fractional values are not allowed and must be given as a positive integer. The sum keyword specifies that the CIR be used as the summed CIR values of the children schedulers or queues.

**Values**  
0 — 100000000, max, sum  
**Default**  
0

### scheduler-override

**Syntax**  
[no] scheduler-override

**Context**  
config>service>epipe>sap>egress  
config>service>epipe>sap>ingress

**Description**  
This command specifies the set of attributes whose values have been overridden by management on this virtual scheduler. Clearing a given flag will return the corresponding overridden attribute to the value defined on the SAP’s ingress scheduler policy.

### scheduler

**Syntax**  
[no] scheduler scheduler-name

**Context**  
config>service>epipe>sap>egress>sched-override  
config>service>epipe>sap>ingress>sched-override

**Description**  
This command can be used to override specific attributes of the specified scheduler name. A scheduler defines bandwidth controls that limit each child (other schedulers and queues) associated with the scheduler. Scheduler objects are created within the hierarchical tiers of the policy. It is assumed that each scheduler created will have queues or other schedulers defined as child associations. The scheduler can be a child (take bandwidth from a scheduler in a higher tier, except for schedulers created in tier 1). A total of 32 schedulers can be created within a single scheduler policy with no restriction on the distribution between the tiers.

Each scheduler must have a unique name within the context of the scheduler policy; however the same name can be reused in multiple scheduler policies. If scheduler-name already exists within the policy tier level (regardless of the inclusion of the keyword create), the context changes to that scheduler name for the purpose of editing the scheduler parameters. Modifications made to an existing scheduler are executed on all instantiated schedulers created through association with the policy of the edited scheduler. This can cause queues or schedulers to become orphaned (invalid parent association) and adversely affect the ability of the system to enforce service level agreements (SLAs).
If the `scheduler-name` exists within the policy on a different tier (regardless of the inclusion of the keyword `create`), an error occurs and the current CLI context will not change.

If the `scheduler-name` does not exist in this or another tier within the scheduler policy, it is assumed that an attempt is being made to create a scheduler of that name. The success of the command execution is dependent on the following:

1. The maximum number of schedulers has not been configured.
2. The provided `scheduler-name` is valid.
3. The `create` keyword is entered with the command if the system is configured to require it (enabled in the `environment create` command).

When the maximum number of schedulers has been exceeded on the policy, a configuration error occurs and the command will not execute, nor will the CLI context change.

If the provided scheduler-name is invalid according to the criteria below, a name syntax error will occur, the command will not execute, and the CLI context will not change.

**Parameters**

- `scheduler-name` — The name of the scheduler.

**Values**

Valid names consist of any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

**Default**

None. Each scheduler must be explicitly created.

`create` — This optional keyword explicitly specifies that it is acceptable to create a scheduler with the given `scheduler-name`. If the `create` keyword is omitted, `scheduler-name` is not created when the system environment variable `create` is set to true. This safeguard is meant to avoid accidental creation of system objects (such as schedulers) while attempting to edit an object with a mistyped name or ID. The keyword has no effect when the object already exists.

**Context**

- `config>service>epipe>sap>egress>sched-override>scheduler`
- `config>service>epipe>sap>ingress>sched-override>scheduler`

**Description**

This command can be used to override specific attributes of the specified scheduler rate. The `rate` command defines the maximum bandwidth that the scheduler can offer its child queues or schedulers. The maximum rate is limited to the amount of bandwidth the scheduler can receive from its parent scheduler. If the scheduler has no parent, the maximum rate is assumed to be the amount available to the scheduler. When a parent is associated with the scheduler, the CIR parameter provides the amount of bandwidth to be considered during the parent scheduler’s ‘within CIR’ distribution phase.

The actual operating rate of the scheduler is limited by bandwidth constraints other than its maximum rate. The scheduler’s parent scheduler may not have the available bandwidth to meet the scheduler’s needs or the bandwidth available to the parent scheduler could be allocated to other child schedulers or child queues on the parent based on higher priority. The children of the scheduler may not need the maximum rate available to the scheduler due to insufficient offered load or limits to their own maximum rates.

When a scheduler is defined without specifying a rate, the default rate is `max`. If the scheduler is a root scheduler (no parent defined), the default maximum rate must be changed to an explicit value. Without this explicit value, the scheduler will assume that an infinite amount of bandwidth is available and allow all child queues and schedulers to operate at their maximum rates.

The `no` form of this command returns all queues created with this `queue-id` by association with the QoS policy to the default PIR and CIR parameters.
Parameters  

pir-rate — The pir parameter accepts a step multiplier value that specifies the multiplier used to determine the PIR rate at which the queue will operate. A value of 0 to 100000000 or the keyword max or sum is accepted. Any other value will result in an error without modifying the current PIR rate.

To calculate the actual PIR rate, the rate described by the queue’s rate is multiplied by the pir-rate.

The SAP ingress context for PIR is independent of the defined forwarding class (fc) for the queue. The default pir and definable range is identical for each class. The PIR in effect for a queue defines the maximum rate at which the queue will be allowed to forward packets in a given second, thus shaping the queue’s output.

The PIR parameter for SAP ingress queues do not have a negate (no) function. To return the queues PIR rate to the default value, that value must be specified as the PIR value.

Values  

1 — 100000000, max

Default  

max

cir cir-rate — The cir parameter accepts a step-multiplier value that specifies the multiplier used to determine the CIR rate at which the queue will operate. A value of 0 to 250 or the keyword max is accepted. Any other value will result in an error without modifying the current CIR rate.

To calculate the actual CIR rate, the rate described by the rate pir pir-rate is multiplied by the cir cir-rate. If the cir is set to max, then the CIR rate is set to infinity.

The SAP ingress context for CIR is dependent on the defined forwarding class (fc) for the queue. The default CIR and definable range is different for each class. The CIR in effect for a queue defines both its profile (in or out) marking level as well as the relative importance compared to other queues for scheduling purposes during congestion periods.

Values  

0 — 10000000, max, sum

Default  

sum

scheduler-policy

Syntax  

scheduler-policy scheduler-policy-name

no scheduler-policy

Context  

config>service>epipe>sap>ingress
config>service>epipe>sap>egress

Description  

This command applies an existing scheduler policy to an ingress or egress scheduler used by SAP queues associated with this multi-service customer site. The schedulers defined in the scheduler policy can only be created once the customer site has been appropriately assigned to a chassis port, channel or slot. Scheduler policies are defined in the config>qos>scheduler-policy scheduler-policy-name context.

The no form of this command removes the configured ingress or egress scheduler policy from the multi-service customer site. When the policy is removed, the schedulers created due to the policy are removed also making them unavailable for the ingress SAP queues associated with the customer site. Queues that lose their parent scheduler association are deemed to be orphaned and are no longer subject to a virtual scheduler. The SAPs that have ingress queues reliant on the removed schedulers
enter into an operational state depicting the orphaned status of one or more queues. When the **no scheduler-policy** command is executed, the customer site ingress or egress node will not contain an applied scheduler policy.

`scheduler-policy-name` — The `scheduler-policy-name` parameter applies an existing scheduler policy that was created in the `config>qos>scheduler-policy scheduler-policy-name` context to create the hierarchy of ingress or egress virtual schedulers. The scheduler names defined within the policy are created and made available to any ingress or egress queues created on associated SAPs.

### vlan-translation

**Syntax**

```
vlan-translation {vlan-id | copy-outer}
```

**no vlan-translation**

**Context**

`config>service>epipe>sap>ingress`

**Description**

This command configures ingress VLAN translation. If enabled with an explicit VLAN value, the preserved vlan-id will be overwritten with this value. This setting is applicable to dot1q encapsulated ports. If enabled with “copy-outer” keyword, the outer vlan-id will be copied to inner position on QinQ encapsulated ports. The feature is not supported on default-dot1q saps (1/1/1:* and 1/1/1:0), nor on TopQ saps.

The **no** version of the command sets the default value and no action will be taken.

**Default**

Per default, the preserved VLAN values will not be overwritten.

**Parameters**

- `vlan-id` — Specifies that the preserved vlan-id will be overwritten with this value.

  **Values**

  0 — 4094

- `outer-copy` — Keyword specifies to use the outer VLAN ID.

### match-qinq-dot1p

**Syntax**

```
match-qinq-dot1p {top | bottom}
```

**no match-qinq-dot1p de**

**Context**

`config>service>epipe>sap>ingress`

**Description**

This command specifies which Dot1Q tag position Dot1P bits in a QinQ encapsulated packet should be used to evaluate Dot1P QoS classification.

The `match-qinq-dot1p` command allows the top or bottom PBits to be used when evaluating the applied sap-ingress QoS policy’s Dot1P entries. The **top** and **bottom** keywords specify which position should be evaluated for QinQ encapsulated packets.

The setting also applies to classification based on the DE indicator bit.

The **no** form of this command reverts the dot1p and de bits matching to the default tag.

By default, the bottom most service delineating Dot1Q tags Dot1P bits are used. Table 6 defines the default behavior for Dot1P evaluation.
### Parameters

- **top** — The top parameter is mutually exclusive to the bottom parameter. When the top parameter is specified, the top most PBits are used (if existing) to match any dot1p dot1p-value entries. The following table defines the dot1p evaluation behavior when the top parameter is specified.

#### Table 6: Default QinQ and TopQ SAP Dot1P Evaluation

<table>
<thead>
<tr>
<th>Port / SAP Type</th>
<th>Existing Packet Tags</th>
<th>PBits Used for Match</th>
</tr>
</thead>
<tbody>
<tr>
<td>Null</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>Null</td>
<td>Dot1P (VLAN-ID 0)</td>
<td>Dot1P PBits</td>
</tr>
<tr>
<td>Null</td>
<td>Dot1Q</td>
<td>Dot1Q PBits</td>
</tr>
<tr>
<td>Null</td>
<td>TopQ BottomQ</td>
<td>TopQ PBits</td>
</tr>
<tr>
<td>Null</td>
<td>TopQ (No BottomQ)</td>
<td>TopQ PBits</td>
</tr>
<tr>
<td>Dot1Q</td>
<td>None (Default SAP)</td>
<td>None</td>
</tr>
<tr>
<td>Dot1Q</td>
<td>Dot1P (Default SAP VLAN-ID 0)</td>
<td>Dot1P PBits</td>
</tr>
<tr>
<td>Dot1Q</td>
<td>Dot1Q</td>
<td>Dot1Q PBits</td>
</tr>
<tr>
<td>QinQ / TopQ</td>
<td>TopQ</td>
<td>TopQ PBits</td>
</tr>
<tr>
<td>QinQ / TopQ</td>
<td>TopQ BottomQ</td>
<td>TopQ PBits</td>
</tr>
<tr>
<td>QinQ / QinQ</td>
<td>TopQ BottomQ</td>
<td>BottomQ PBits</td>
</tr>
</tbody>
</table>

no match-qinq-dot1p (no filtering based on p-bits)

(top or bottom must be specified to override the default QinQ dot1p behavior)
**bottom** — The bottom parameter is mutually exclusive to the top parameter. When the bottom parameter is specified, the bottom most PBits are used (if existing) to match any dot1p dot1p-value entries. The following table defines the dot1p evaluation behavior when the bottom parameter is specified.

**Table 7: Bottom Position QinQ and TopQ SAP Dot1P Evaluation**

<table>
<thead>
<tr>
<th>Port / SAP Type</th>
<th>Existing Packet Tags</th>
<th>PBits Used for Match</th>
</tr>
</thead>
<tbody>
<tr>
<td>Null</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>Null</td>
<td>Dot1P (VLAN-ID 0)</td>
<td>Dot1P PBits</td>
</tr>
<tr>
<td>Null</td>
<td>Dot1Q</td>
<td>Dot1Q PBits</td>
</tr>
<tr>
<td>Null</td>
<td>TopQ BottomQ</td>
<td>TopQ PBits</td>
</tr>
<tr>
<td>Null</td>
<td>TopQ (No BottomQ)</td>
<td>TopQ PBits</td>
</tr>
<tr>
<td>Dot1Q</td>
<td>None (Default SAP)</td>
<td>None</td>
</tr>
<tr>
<td>Dot1Q</td>
<td>Dot1P (Default SAP VLAN-ID 0)</td>
<td>Dot1P PBits</td>
</tr>
<tr>
<td>Dot1Q</td>
<td>Dot1Q</td>
<td>Dot1Q PBits</td>
</tr>
<tr>
<td>QinQ / TopQ</td>
<td>TopQ</td>
<td>TopQ PBits</td>
</tr>
<tr>
<td>QinQ / TopQ</td>
<td>TopQ BottomQ</td>
<td>TopQ PBits</td>
</tr>
<tr>
<td>QinQ / QinQ</td>
<td>TopQ BottomQ</td>
<td>BottomQ PBits</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Egress SAP Type</th>
<th>Ingress Packet Preserved Dot1P State</th>
<th>Marked (or Remarked) PBits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Null</td>
<td>No preserved Dot1P bits</td>
<td>None</td>
</tr>
<tr>
<td>Null</td>
<td>Preserved Dot1P bits</td>
<td>Preserved tag PBits remarked using dot1p-value</td>
</tr>
<tr>
<td>Dot1Q</td>
<td>No preserved Dot1P bits</td>
<td>New PBits marked using dot1p-value</td>
</tr>
<tr>
<td>Dot1Q</td>
<td>Preserved Dot1P bits</td>
<td>Preserved tag PBits remarked using dot1p-value</td>
</tr>
<tr>
<td>TopQ</td>
<td>No preserved Dot1P bits</td>
<td>TopQ PBits marked using dot1p-value</td>
</tr>
<tr>
<td>TopQ</td>
<td>Preserved Dot1P bits (used as TopQ and BottomQ PBits)</td>
<td>TopQ PBits marked using dot1p-value, BottomQ PBits preserved</td>
</tr>
<tr>
<td>QinQ</td>
<td>No preserved Dot1P bits</td>
<td>TopQ PBits and BottomQ PBits marked using dot1p-value</td>
</tr>
<tr>
<td>QinQ</td>
<td>Preserved Dot1P bits (used as TopQ and BottomQ PBits)</td>
<td>TopQ PBits and BottomQ PBits marked using dot1p-value</td>
</tr>
</tbody>
</table>
The QinQ and TopQ SAP PBit/DEI bit marking follows the default behavior defined in the table above when `qinq-mark-top-only` is not specified.

The `dot1p dot1p-value` command must be configured without the `qinq-mark-top-only` parameter to remove the TopQ PBits only marking restriction.

Note that a QinQ-encapsulated Ethernet port can have two different sap types:

- For a TopQ SAP type, only the outer (top) tag is explicitly specified. For example, `sap 1/1/1:10.*`
- For QinQ SAP type, both inner (bottom) and outer (top) tags are explicitly specified. For example, `sap 1/1/1:10.100`. 
VLL SDP Commands

spoke-sdp

Syntax

```plaintext
spoke-sdp  sdp-id[:vc-id]  [vc-type {ether | vlan}]  [no-endpoint]
spoke-sdp  sdp-id[:vc-id]  [vc-type {ether | vlan}]  endpoint  endpoint-name  [icb]
no spoke-sdp  sdp-id[:vc-id]
```

Context

```plaintext
config>service>cpipe
cfgig>service>epipe
```

Description

This command binds a service to an existing Service Distribution Point (SDP). A spoke SDP is treated like the equivalent of a traditional bridge “port” where flooded traffic received on the spoke SDP is replicated on all other “ports” (other spoke and mesh SDPs or SAPs) and not transmitted on the port it was received.

The SDP has an operational state which determines the operational state of the SDP within the service. For example, if the SDP is administratively or operationally down, the SDP for the service will be down.

The SDP must already be defined in the `config>service>sdp` context in order to associate an SDP with an Epipe, VPLS, VPRN, VPRN service. If the `sdp sdp-id` is not already configured, an error message is generated. If the `sdp-id` does exist, a binding between that `sdp-id` and the service is created. SDPs must be explicitly associated and bound to a service. If an SDP is not bound to a service, no far-end devices can participate in the service.

The `no` form of this command removes the SDP binding from the service. The SDP configuration is not affected; only the binding of the SDP to a service. Once removed, no packets are forwarded to the far-end router.

Default

No `sdp-id` is bound to a service.

Special Cases

`Epipe` — At most, only one `sdp-id` can be bound to an Epipe service. Since an Epipe is a point-to-point service, it can have, at most, two end points. The two end points can be one SAP and one SDP or two SAPs. Vc-switching VLLs are an exception. If the VLL is a “vc-switching” VLL, then the two endpoints must both be SDPs.

L2TPv3 SDP types are only supported on EPipe services and not other xPipe services.

Parameters

- `sdp-id` — The SDP identifier. Allowed values are integers in the range of 1 to 17407 for existing SDPs.

- `vc-id` — The virtual circuit identifier. The VC-ID is not used with L2TPv3 SDPs, however it must be configured.

- `vc-type` — This command overrides the default VC type signaled for the spoke or mesh binding to the far end of the SDP. The VC type is a 15 bit-quantity containing a value which represents the type of VC. The actual signaling of the VC type depends on the signaling parameter defined for the SDP. If signaling is disabled, the `vc-type` command can still be used to define the dot1q value expected by the far-end provider equipment. A change of the bindings VC type causes the...
Virtual Leased Line Services

binding to signal the new VC type to the far end when signaling is enabled. VC types are derived according to IETF draft-martini-l2circuit-trans-mpls.

- The VC type value for Ethernet is 0x0005.
- The VC type value for an Ethernet VLAN is 0x0004.
- The VC type value for a VPLS service is defined as 0x000B.

Values

ether — Defines the VC type as Ethernet. The ethernet and vlan keywords are mutually exclusive. When the VC type is not defined then the default is Ethernet for spoke SDP bindings. Defining Ethernet is the same as executing no vc-type and restores the default VC type for the spoke SDP binding.

vlan — Defines the VC type as VLAN. The ethernet and vlan keywords are mutually exclusive. When the VC type is not defined then the default is Ethernet for spoke SDP bindings. The VLAN VC-type requires at least one dot1Q tag within each encapsulated Ethernet packet transmitted to the far end.

no endpoint — Removes the association of a spoke SDP with an explicit endpoint name.

endpoint endpoint-name — Specifies the name of the service endpoint.

icb — Configures the spoke SDP as an inter-chassis backup SDP binding.

spoke-sdp

Syntax

spoke-sdp sdp-id[:vc-id] [no-endpoint]
spoke-sdp sdp-id[:vc-id] endpoint endpoint-name [icb]
no spoke-sdp sdp-id[:vc-id]

Context config>service>cpipe

Description

This command binds a service to an existing Service Distribution Point (SDP). A spoke SDP is treated like the equivalent of a traditional bridge “port” where flooded traffic received on the spoke SDP is replicated on all other “ports” (other spoke and mesh SDPs or SAPs) and not transmitted on the port it was received.

The SDP has an operational state which determines the operational state of the SDP within the service. For example, if the SDP is administratively or operationally down, the SDP for the service will be down.

The SDP must already be defined in the config>service>sdp context in order to associate an SDP with a service. If the sdp sdp-id is not already configured, an error message is generated. If the sdp-id does exist, a binding between that sdp-id and the service is created.

SDPs must be explicitly associated and bound to a service. If an SDP is not bound to a service, no far-end SR/ESS devices can participate in the service.

The no form of this command removes the SDP binding from the service. The SDP configuration is not affected; only the binding of the SDP to a service. Once removed, no packets are forwarded to the far-end router.

Default No sdp-id is bound to a service.
**Parameters**

- **sdp-id** — The SDP identifier. Allowed values are integers in the range of 1 to 17407 for existing SDPs.

- **vc-id** — The virtual circuit identifier.

  **Values**

  - 1 — 4294967295

- **no endpoint** — Adds or removes a spoke SDP association.

- **endpoint endpoint-name** — Specifies the name of the service endpoint.

- **ich** — Configures the spoke SDP as an inter-chassis backup SDP binding.

**hash-label**

**Syntax**

```
hash-label [signal-capability]
no hash-label
```

**Context**

- `config>service>epipe>spoke-sdp`
- `config>service>pw-template`
- `config>service>vprn`
- `config>service>vprn>interface>spoke-sdp`
- `config>service>ies>interface>spoke-sdp`

**Description**

This command enables the use of the hash label on a VLL or VPLS service bound to LDP or RSVP SDP. This feature is not supported on a service bound to a GRE SDP. This feature is also not supported on multicast packets forwarded using RSVP P2MP LPS or mLDP LSP in both the base router instance and in the multicast VPN (mVPN) instance. It is, however, supported when forwarding multicast packets using an IES spoke-interface.

When this feature is enabled, the ingress data path is modified such that the result of the hash on the packet header is communicated to the egress data path for use as the value of the label field of the hash label. The egress data path appends the hash label at the bottom of the stack (BoS) and sets the S-bit to one (1).

In order to allow applications where the egress LER infers the presence of the hash label implicitly from the value of the label, the Most Significant Bit (MSB) of the result of the hash is set before copying into the Hash Label. This means that the value of the hash label will always be in the range \([524,288 - 1,048,575]\) and will not overlap with the signaled/static LSP and signaled/static service label ranges. This also guarantees that the hash label will not match a value in the reserved label range.

The (unmodified) result of the hash continues to be used for the purpose of ECMP and LAG spraying of packets locally on the ingress LER. Note, however, that for VLL services, the result of the hash is overwritten and the ECMP and LAG spraying will be based on service-id when ingress SAP shared queuing is not enabled. However, the hash label will still reflect the result of the hash such that an LSR can use it to perform fine grained load balancing of VLL PW packets.

Packets generated in CPM and that are forwarded labeled within the context of a service (for example, OAM packets) must also include a Hash Label at the BoS and set the S-bit accordingly.

The TTL of the hash label is set to a value of 0.

The user enables the signaling of the hash-label capability under a VLL spoke-sdp, a VPLS spoke-sdp or mesh-sdp, or an IES/VPRN spoke interface by adding the `signal-capability` option. In this case, the decision whether to insert the hash label on the user and control plane packets by the local PE is
solely determined by the outcome of the signaling process and can override the local PE configuration. The following are the procedures:

- The local PE will insert the flow label interface parameters sub-TLV with F=1 in the PW ID FEC element in the label mapping message for that spoke-sdp or mesh-sdp.
- If the remote PE includes this sub-TLV with F=1 or F=0, then local PE must insert the hash label in the user and control plane packets.
- If remote PE does not include this sub-TLV (for example, it does not support it, or it is supported but the user did not enable the hash-label option or the signal-capability option), then the local PE establishes the PW but must not insert the hash label in the user and control packets over that spoke-sdp or mesh-sdp. If the remote PE does not support the signal-capability option, then there are a couple of possible outcomes:
  - If the hash-label option was enabled on the local configuration of the spoke-sdp or mesh-sdp at the remote PE, the PW packets received by the local PE will have the hash label included. These packets must be dropped. The only way to solve this is to disable the signaling capability option on the local node which will result in the insertion of the hash label by both PE nodes.
  - If the hash-label option is not supported or was not enabled on the local configuration of the spoke-sdp or mesh-sdp at the remote PE, the PW received by the local PE will not have the hash label included.

- The user can enable or disable the signal-capability option in CLI as needed. When doing so, the must withdraw the label it sent to its peer and send a new label mapping message with the new value of the F bit in the flow label interface parameters sub-TLV of the PW ID FEC element.

The no form of this command disables the use of the hash label.

**Default**

```plaintext
no hash-label
```

**Parameters**

```plaintext
signal-capability — Enables the signaling and negotiation of the use of the hash label between the local and remote PE nodes. The signal-capability option is not supported on a VPRN spoke-sdp.
```

---

**control-word**

**Syntax**

```plaintext
[no] control-word
cfg>service>spoke-sdp
cfg>service>epipe>spoke-sdp
```

**Description**

The control word command provides the option to add a control word as part of the packet encapsulation for pseudowire types for which the control word is optional. These are Ethernet pseudowires (Epipe).

The configuration for the two directions of the pseudowire must match because the control word negotiation procedures described in Section 6.2 of RFC 4447 are not supported. The C-bit in the pseudowire FEC sent in the label mapping message is set to 1 when the control word is enabled. Otherwise, it is set to 0.

The service will only come up if the same C-bit value is signaled in both directions. If a spoke-sdp is configured to use the control word but the node receives a label mapping message with a C-bit clear, the node releases the label with the an “Illegal C-bit” status code as per Section 6.1 of RFC 4447. As soon as the user also enabled the control the remote peer, the remote peer will withdraw its original label and will send a label mapping with the C-bit set to 1 and the VLL service will be up in both
nodes. The control word must be enabled to allow MPLS-TP OAM to be used on a static spoke-sdp in a apipe, epipe and cpipe service.

when used with IES and VPRN services:

**hash-label**

**Syntax**

```
hash-label [signal-capability]
no hash label
```

**Context**

```
config>service>epipe>spoke-sdp
```

**Description**

This command enables the use of the hash label on a VLL, VPLS, or VPRN service bound to LDP or RSVP SDP as well as to a VPRN service using the autobind mode with the with the ldp, rsvp-te, or mpls options. This feature is not supported on a service bound to a GRE SDP or for a VPRN service using the autobind mode with the gre option.

When this feature is enabled, the ingress data path is modified such that the result of the hash on the packet header is communicated to the egress data path for use as the value of the label field of the hash label. The egress data path appends the hash label at the bottom of the stack (BoS) and sets the S-bit to 1 to indicate that.

In order to allow for applications whereby the egress LER infers the presence of the Hash Label implicitly from the value of the label, the Most Significant Bit (MSB) of the result of the hash is set before copying into the Hash Label. This means that the value of the hash label will always be in the range [524,288 - 1,048,575] and will not overlap with the signaled/static LSP and signaled/static service label ranges. This also guarantees that the hash label will not match a value in the reserved label range.

The (unmodified) result of the hash continues to be used for the purpose of ECMP and LAG spraying of packets locally on the ingress LER. Note however that for VLL services, the result of the hash is overwritten and the ECMP and LAG spraying will be based on service-id when ingress SAP shared queuing is not enabled. However, the hash label will still reflect the result of the hash such that an LSR can use it to perform fine grained load balancing of VLL pseudowire packets.

Packets that are generated in CPM and forwarded labeled within the context of a service (for example, OAM packets) must also include a Hash Label at the BoS and set the S-bit accordingly.

The TTL of the Hash Label is set to a value of 0.

The **no** form of this command disables the use of the hash label.

The user enables the signaling of the hash-label capability under a VLL spoke-sdp, a VPLS spoke-sdp or mesh-sdp, or an IES/VPRN spoke interface by adding the **signal-capability** option. In this case, the decision whether to insert the hash label on the user and control plane packets by the local PE is solely determined by the outcome of the signaling process and can override the local PE configuration. The following are the procedures:

- The local PE will insert the flow label interface parameters sub-TLV with F=1 in the PW ID FEC element in the label mapping message for that spoke-sdp or mesh-sdp.
- If the remote PE includes this sub-TLV with F=1 or F=0, then local PE must insert the hash label in the user and control plane packets.
- If remote PE does not include this sub-TLV (for example, it does not support it, or it is supported but the user did not enable the **hash-label** option or the **signal-capability** option), then the local PE establishes the PW but must not insert the hash label in the user and control packets over that
spoke-sdp or mesh-sdp. If the remote PE does not support the **signal-capability** option, then there are a couple of possible outcomes:

- If the **hash-label** option was enabled on the local configuration of the spoke-sdp or mesh-sdp at the remote PE, the PW packets received by the local PE will have the hash label included. These packets must be dropped. The only way to solve this is to disable the signaling capability option on the local node which will result in the insertion of the hash label by both PE nodes.

- If the **hash-label** option is not supported or was not enabled on the local configuration of the spoke-sdp or mesh-sdp at the remote PE, the PW received by the local PE will not have the hash label included.

  - The user can enable or disable the signal-capability option in CLI as needed. When doing so, the must withdraw the label it sent to its peer and send a new label mapping message with the new value of the F bit in the flow label interface parameters sub-TLV of the PW ID FEC element.

The **no** form of this command disables the use of the hash label.

**Default**

no hash-label

**Parameters**

`signal-capability` — Enables the signaling and negotiation of the use of the hash label between the local and remote PE nodes. The **signal-capability** option is not supported on a VPRN spoke-sdp.

generate-ignore-oper-down

**Syntax**

ignore-oper-down

[no] ignore-oper-down

**Context**

config>service>epipe>sap>

**Description**

ePipe service will not transition to Oper State: Down when a SAP fails and when this optional command configured under that specific SAP. Only a single SAP in an ePipe may have this optional command included.

**Default**

no ignore-oper-down

qos

**Syntax**

qos network-policy-id port-redirect-group queue-group-name [instance instance-id]

no qos

**Context**

config>service>apipe>spoke-sdp>egress
config>service>cpipe>spoke-sdp>egress
config>service>epipe>spoke-sdp>egress
config>service>fpipe>spoke-sdp>egress
config>service>ipipe>spoke-sdp>egress
config>service>vpipe>spoke-sdp>egress
config>service>vpls>spoke-sdp>egress
config>service>vpls>mesh-sdp>egress
config>service>pw-template>egress
config>service>vprn>interface>spoke-sdp>egress
config>service>ies>interface>spoke-sdp>egress
**Description**

This command is used to redirect PW packets to an egress port queue-group for the purpose of shaping.

The egress PW shaping provisioning model allows the mapping of one or more PWs to the same instance of queues, or policers and queues, that are defined in the queue-group template.

Operationally, the provisioning model consists of the following steps:

1. Create an egress queue-group template and configure queues only, or policers and queues for each FC that needs to be redirected.
2. Apply the queue-group template to the network egress context of all ports where there exists a network IP interface that the PW packets can be forwarded on. This creates one instance of the template on the egress of the port. One or more instances of the same template can be created.
3. Configure FC-to-policer or FC-to-queue mappings together with the redirect to a queue-group in the egress context of a network QoS policy. No queue-group name is specified in this step, which means the same network QoS policy can redirect different PWs to different queue-group templates.
4. Apply this network QoS policy to the egress context of a spoke-sdp inside a service, or to the egress context of a PW template and specify the redirect queue-group name.

One or more spoke-sdps can have their FCs redirected to use queues only, or queues and policers in the same queue-group instance.

The following are the constraints and rules of this provisioning model:

1. When a PW FC is redirected to use a queue or a policer and a queue in a queue-group and the queue-group name does not exist, the association is failed at the time the user associates the egress context of a spoke-sdp to the named queue-group. In such a case, the PW packet will be fed directly to the corresponding egress queue for that FC used by the IP network interface the PW packet is forwarded on. This queue can be a queue-group queue or the egress shared queue for that FC defined in the network-queue policy applied to the egress of this port. This is the existing implementation and default behavior for a PW packet.
2. When a PW FC is redirected to use a queue or a policer and a queue in a queue-group and the queue-group name exists but the policer-id and/or the queue-id is not defined in the queue-group template, the association is failed at the time the user associates the egress context of a spoke-sdp to the named queue-group. In such a case, the PW packet will be fed directly to the corresponding egress queue for that FC used by the IP network interface the PW packet is forwarded on.
3. When a PW FC is redirected to use a queue or a policer and a queue in a queue-group and the queue-group name exists and the policer-id or policer-id plus queue-id exist, it is not required to check that an instance of that queue-group exists in all egress network ports that have network IP interfaces. The handling of this is dealt with in the data path as follows:
   - When a PW packet for that FC is forwarded and an instance of the referenced queue-group name exists on that egress port, the packet is processed by the queue-group policer and will then be fed to the queue-group queue.
   - When a PW packet for that FC is forwarded and an instance of the referenced queue-group name does not exist on that egress port, the PW packet will be fed directly to the corresponding egress shared queue for that FC defined in the network-queue policy applied to the egress of this port.
4. If a network QoS policy is applied to the egress context of a PW, any PW FC that is not explicitly redirected in the network QoS policy will have the corresponding packets feed directly the
corresponding the egress shared queue for that FC defined in the network-queue policy applied to the egress of this port.

When the queue-group name the PW is redirected to exists and the redirection succeeds, the marking of the packet’s DEI/dot1.p/DSCP and the tunnel’s DEI/dot1.p/DSCP/EXP is performed according to the relevant mappings of the {FC, profile} in the egress context of the network QoS policy applied to the PW. This is true regardless if an instance of the queue-group exists or not on the egress port the PW packet is forwarded to. If the packet’s profile value changed due to egress child policer CIR profiling, the new profile value is used to mark the packet’s DEI/dot1.p and the tunnel’s DEI/dot1.p/EXP, but the DSCP is not modified by the policer’s operation.

When the queue-group name the PW is redirected does not exist, the redirection command is failed. In this case, the marking of the packet’s DEI/dot1.p/DSCP and the tunnel’s DEI/dot1.p/DSCP/EXP fields is performed according to the relevant commands in the egress context of the network QoS policy applied to the network IP interface the PW packet is forwarded to.

The no version of this command removes the redirection of the PW to the queue-group.

Parameters

network-policy-id — Specifies the network policy identification. The value uniquely identifies the policy on the system.

Values 1—65535

port-redirect-group queue-group-name — Specifies the name of the queue group template up to 32 characters in length.

instance instance-id — Specifies the optional identification of a specific instance of the queue-group.

Values 1—40960

QoS

Syntax qos network-policy-id fp-redirect-group queue-group-name instance instance-id

no qos

Context config>service>apipe>spoke-sdp>ingress
config>service>cpipe>spoke-sdp>ingress
config>service>epipe>spoke-sdp>ingress
config>service>fpipe>spoke-sdp>ingress
config>service>ipipe>spoke-sdp>ingress
config>service>vplspoke-sdp>ingress
config>service>vplsmesh-sdp>ingress
config>service>pw-template>ingress
config>service>vprn>interface>spoke-sdp>ingress
config>service>ies>interface>spoke-sdp>ingress

Description This command is used to redirect PW packets to an ingress forwarding plane queue-group for the purpose of rate-limiting.

The ingress PW rate-limiting feature uses a policer in queue-group provisioning model. This model allows the mapping of one or more PWs to the same instance of policers that are defined in a queue-group template.

Operationally, the provisioning model in the case of the ingress PW shaping feature consists of the following steps:
1. Create an ingress queue-group template and configure policers for each FC that needs to be redirected and optionally for each traffic type (unicast or multicast).

2. Apply the queue-group template to the network ingress forwarding plane where there exists a network IP interface that the PW packets can be received on. This creates one instance of the template on the ingress of the FP. One or more instances of the same template can be created.

3. Configure FC-to-policer mappings together with the policer redirect to a queue-group in the ingress context of a network QoS policy. No queue-group name is specified in this step which means the same network QoS policy can redirect different PWs to different queue-group templates.

4. Apply this network QoS policy to the ingress context of a spoke-sdp inside a service, or to the ingress context of a PW template and specify the redirect queue-group name.

One or more spoke-sdps can have their FCs redirected to use policers in the same policer queue-group instance.

The following are the constraints and rules of this provisioning model when used in the ingress PW rate-limiting feature:

1. When a PW FC is redirected to use a policer in a named policer queue-group and the queue-group name does not exist, the association is failed at the time the user associates the ingress context of a spoke-sdp to the named queue-group. In such a case, the PW packet will feed directly the ingress network shared queue for that FC defined in the network-queue policy applied to the ingress of the MDA/FP.

2. When a PW FC is redirected to use a policer in a named policer queue-group and the queue-group name exists but the policer-id is not defined in the queue-group template, the association is failed at the time the user associates the ingress context of a spoke-sdp to the named queue-group. In such a case, the PW packet will feed directly the ingress network shared queue for that FC defined in the network-queue policy applied to the ingress of the MDA/FP.

3. When a PW FC is redirected to use a policer in a named policer queue-group and the queue-group name exists and the policer-id is defined in the queue-group template, it is not required to check that an instance of that queue-group exists in all ingress FPs that have network IP interfaces. The handling of this is dealt within the data path as follows:
   - When a PW packet for that FC is received and an instance of the referenced queue-group name exists on that FP, the packet is processed by the policer and will then feed the per-FP ingress shared queues referred to as “policer-output-queues”.
   - When a PW packet for that FC is received and an instance of the referenced queue-group name does not exist on that FP, the PW packets will be fed directly into the corresponding ingress network shared queue for that FC defined in the network-queue policy applied to the ingress of the MDA/FP.

4. If a network QoS policy is applied to the ingress context of a PW, any PW FC that is not explicitly redirected in the network QoS policy will have the corresponding packets feed directly into the ingress network shared queue for that FC defined in the network-queue policy applied to the ingress of the MDA/FP.

5. If no network QoS policy is applied to the ingress context of the PW, then all packets of the PW will feed:
   - the ingress network shared queue for the packet’s FC defined in the network-queue policy applied to the ingress of the MDA/FP. This is the default behavior.
a queue-group policer followed by the per-FP ingress shared queues, referred to as “policer-output-queues”, if the ingress context of the network IP interface from which the packet is received is redirected to a queue-group [csc-policing]. The only exceptions to this behavior are for packets received from an IES/VPRN spoke interface and from an R-VPLS spoke-sdp that is forwarded to the R-VPLS IP interface. In these two cases, the ingress network shared queue for the packet’s FC defined in the network-queue policy applied to the ingress of the MDA/FP is used.

When a PW is redirected to use a policer queue-group, the classification of the packet for the purpose of FC and profile determination is performed according to the default classification rule or the QoS filters defined in the ingress context of the network QoS policy applied to the PW. This is true regardless if an instance of the named policer queue-group exists on the ingress FP the PW packet is received on. The user can apply a QoS filter matching the dot1.p in the VLAN tag corresponding to the Ethernet port encapsulation, the EXP in the outer label when the tunnel is an LSP, the DSCP in the IP header if the tunnel encapsulation is GRE, and the DSCP in the payload’s IP header if the user enabled the ler-use-dscp option and the PW terminates in IES or VPRN service (spoke-interface).

When the policer queue-group name the PW is redirected does not exist, the redirection command is failed. In this case, the packet classification is performed according to the default classification rule or the QoS filters defined in the ingress context of the network QoS policy applied to the network IP interface the PW packet is received on.

The no version of this command removes the redirection of the PW to the queue-group.

Parameters

- network-policy-id — Specifies the network policy identification. The value uniquely identifies the policy on the system.
  - Values: 1—65535

- fp-redirect-group queue-group-name — Specifies the name of the queue group template up to 32 characters in length.

- instance instance-id — Specifies the identification of a specific instance of the queue-group.
  - Values: 1—16384

monitor-oper-group

Syntax

- monitor-oper-group group-name

- no monitor-oper-group

Context

- config>service>epipe>spoke-sdp
- config>service>epipe>sap

Description

This command specifies the operational group to be monitored by the object under which it is configured. The oper-group name must be already configured under the config>service context before its name is referenced in this command.

The no form of the command removes the association.

Default

- none

Parameters

- group-name — Specifies an oper group name.
**oper-group**

**Syntax**

```
oper-group group-name
no oper-group
```

**Context**

`config>service>epipe>sap`

**Description**

This command configures the operational group identifier.

The no form of the command removes the group name from the configuration.

**Default**

`none`

**Parameters**

`group-name` — Specifies the Operational-Group identifier up to 32 characters in length.

**precedence**

**Syntax**

```
precedence [precedence-value | primary]
no precedence
```

**Context**

`config>service>cpipe>spoke-sdp`
`config>service>epipe>spoke-sdp`

**Description**

This command specifies the precedence of the SDP binding when there are multiple SDP bindings attached to one service endpoint. The value of zero can only be assigned to one SDP bind making it the primary SDP bind. When an SDP binding goes down, the next highest precedence SDP binding will begin to forward traffic.

The no form of the command returns the precedence value to the default.

**Default**

`4`

**Parameters**

`precedence-value` — Specifies the spoke SDP precedence.

**Values**

`1 — 4`

`primary` — Specifies to make this the primary spoke SDP.

**pw-status-signaling**

**Syntax**

```
[no] pw-status-signaling
```

**Context**

`config>service>epipe>spoke-sdp`

**Description**

This command enables pseudowire status signaling for this spoke SDP binding.

The no form of the command disables the status signaling.

**Default**

`pw-status-signaling`
use-sdp-bmac

Syntax  

use-sdp-bmac
no use-sdp-bmac

Context  config>service>epipe>spoke-sdp

Description  This command indicates that this spoke-SDP is expected to be part of a redundant pseudowire connected to a PBB EPIPE service. Enabling this parameter will cause traffic forwarded from this spoke-SDP into the B-VPLS domain to use a virtual backbone MAC as its source MAC address when both this, and the control pseudowire, are in the active state on this BEB. This virtual backbone MAC is derived from the SDP source-bmac-lsb configuration.

This command will fail when configuring it under a spoke-SDP within a PBB-Epipe that is connected to a B-VPLS with mac-notification enabled.

Default  no use-sdp-bmac

vc-label

Syntax  

[no] vc-label vc-label

Context  config>service>cpipe>spoke-sdp>egress
config>service>epipe>spoke-sdp>egress

Description  This command configures the egress VC label.

Parameters  

vc-label — A VC egress value that indicates a specific connection.

Values  

16 — 1048575

vc-label

Syntax  

[no] vc-label vc-label

Context  config>service>cpipe>spoke-sdp>ingress
config>service>epipe>spoke-sdp>ingress

Description  This command configures the ingress VC label.

Parameters  

vc-label — A VC ingress value that indicates a specific connection.

Values  

2048 — 18431

vlan-vc-tag

Syntax  

vlan-vc-tag 0..4094
no vlan-vc-tag [0..4094]

Context  config>service>epipe>spoke-sdp
Description
This command specifies an explicit dot1q value used when encapsulating to the SDP far end. When
signaling is enabled between the near and far end, the configured dot1q tag can be overridden by a
received TLV specifying the dot1q value expected by the far end. This signaled value must be stored
as the remote signaled dot1q value for the binding. The provisioned local dot1q tag must be stored as
the administrative dot1q value for the binding.
When the dot1q tag is not defined, the default value of zero is stored as the administrative dot1q
value. Setting the value to zero is equivalent to not specifying the value.

The no form of this command disables the command.

Default
no vlan-vc-tag

Parameters
0..4094 — Specifies a valid VLAN identifier to bind an 802.1Q VLAN tag ID.

spoke-sdp-fec

Syntax
spoke-sdp-fec
spoke-sdp-fec spoke-sdp-fec-id [fec fec-type] [a11-type a11-type] [create]
spoke-sdp-fec spoke-sdp-fec-id no-endpoint
spoke-sdp-fec spoke-sdp-fec-id [fec fec-type] [a11-type a11-type] [create] endpoint name
[icb]

Context
config>service>epipe

Description
This command binds a service to an existing Service Distribution Point (SDP), using a dynamic MS-
PW.

A spoke SDP is treated like the equivalent of a traditional bridge “port” where flooded traffic received
on the spoke SDP is replicated on all other “ports” (other spoke and mesh SDPs or SAPs) and not
transmitted on the port it was received.

The SDP has an operational state which determines the operational state of the SDP within the
service. For example, if the SDP is administratively or operationally down, the SDP for the service
will be down.

When using dynamic MS-PWs, the particular SDP to bind-to is automatically selected based on the
Target Attachment Individual Identifier (TAII) and the path to use, specified under spoke-SDP FEC.
The selected SDP will terminate on the first hop S-PE of the MS-PW. Therefore, an SDP must already
be defined in the config>service>sdp context that reaches the first hop 7x50 of the MS-PW. The 7x50
will in order to associate an SDP with a service. If an SDP to that is not already configured, an error
message is generated. If the spd-id does exist, a binding between that spd-id and the service is created.

It differs from the spoke-sdp command in that the spoke-sdp command creates a spoke SDP binding
that uses a PW with the PW ID FEC. However, the spoke-sdp-fec command enables PWs with other
FEC types to be used. In Release 9.0, only the Generalised ID FEC (FEC129) may be specified using
this command.

The no form of this command removes the SDP binding from the service. The SDP configuration is
not affected; only the binding of the SDP to a service. Once removed, no packets are forwarded to the
far-end router.

Default
none

Parameters
spoke-sdp-fec-id — An unsigned integer value identifying the spoke-SDP.
Values 1 — 4294967295

**fec** fec-type — An unsigned integer value for the type of the FEC used by the MS-PW.

**Values** 129 — 130

**aii-type** ai-type — An unsigned integer value for the Attachment Individual Identifier (AII) type used to identify the MS-PW endpoints.

**Values** 1 — 2

**endpoint** endpoint-name — Specifies the name of the service endpoint

**no endpoint** — Adds or removes a spoke SDP association.

**icb** — Configures the spoke-SDP as an inter-chassis backup SDP binding.

### auto-config

**Syntax** [no] auto-config

**Context** config>service>epipe>spoke-sdp-fec

**Description**

This command enables single sided automatic endpoint configuration of the spoke-SDP. The 7x50 acts as the passive T-PE for signaling this MS-PW.

Automatic Endpoint Configuration allows the configuration of a spoke-SDP endpoint without specifying the TAI associated with that spoke-SDP. It allows a single-sided provisioning model where an incoming label mapping message with a TAI that matches the SAII of that spoke-SDP to be automatically bound to that endpoint. In this mode, the far end T-PE actively initiates MS-PW signaling and will send the initial label mapping message using T-LDP, while the 7x50 T-PE for which auto-config is specified will act as the passive T-PE.

The **auto-config** command is blocked in CLI if signaling active has been enabled for this spoke-SDP. It is only applicable to spoke SDPs configured under the Epipe, IES and VPRN interface context.

The **no** form of the command means that the 7x50 T-PE either acts as the active T-PE (if signaling active is configured) or automatically determines which 7x50 will initiate MS-PW signaling based on the prefix values configured in the SAII and TAI of the spoke-SDP. If the SAII has the greater prefix value, then the 7x50 will initiate MS-PW signaling without waiting for a label mapping message from the far end. However, if the TAI has the greater value prefix, then the 7x50 will assume that the far end T-PE will initiate MS-PW signaling and will wait for that label mapping message before responding with a T-LDP label mapping message for the MS-PW in the reverse direction.

**Default** no auto-config

### path

**Syntax** path name

**no path**

**Context** config>service>epipe>spoke-sdp-fec
**VLL SDP Commands**

**Description**  This command specifies the explicit path, containing a list of S-PE hops, that should be used for this spoke SDP. The path-name should correspond to the name of an explicit path configured in the `config>service>pw-routing` context.

If no path is configured, then each next-hop of the MS-PW used by the spoke-SDP will be chosen locally at each T-PE and S-PE.

**Default**  no path

**Parameters**

- `path-name` — The name of the explicit path to be used, as configured under `config>service>pw-routing`.

**precedence**

**Syntax**  

- `precedence prec-value`
- `precedence primary`
- `no precedence`

**Context**  

`config>service>epipe>spoke-sdp-fec`

**Description**  This command specifies the precedence of the SDP binding when there are multiple SDP bindings attached to one service endpoint. The value of zero can only be assigned to one SDP bind making it the primary SDP bind. When an SDP binding goes down, the next highest precedence SDP binding will begin to forward traffic.

The `no` form of the command returns the precedence value to the default.

**Default**  42

**Parameters**

- `precedence-value` — Specifies the spoke SDP precedence.

  - **Values**
    - `primary` — Specifies to make this the primary spoke SDP.

**pw-template-bind**

**Syntax**  

- `pw-template-bind policy-id`
- `no pw-template-bind`

**Context**  

`config>service>epipe>spoke-sdp-fec`

**Description**  This command binds includes the parameters included in a specific PW Template to a spoke SDP. The `no` form of the command removes the values from the configuration.

**Default**  none

**Parameters**

- `policy-id` — Specifies the existing policy ID

  - **Values**
    - `1 — 2147483647`
retry-count

Syntax  
retry-count retry-count
no retry-count

Context  config>service>epipe>spoke-sdp-fec

Description  
This optional command specifies the number of attempts software should make to re-establish the spoke-SDP after it has failed. After each successful attempt, the counter is reset to zero.

When the specified number is reached, no more attempts are made and the spoke-sdp is put into the shutdown state.

Use the no shutdown command to bring up the path after the retry limit is exceeded.

The no form of this command reverts the parameter to the default value.

Default 30

Parameters  
retry-count — The maximum number of retries before putting the spoke-sdp into the shutdown state.

Values  10 — 10000

retry-timer

Syntax  
retry-timer retry-timer
no retry-timer

Context  config>service>epipe>spoke-sdp-fec

Description  
This command specifies a retry-timer for the spoke-SDP. This is a configurable exponential back-off timer that determines the interval between retries to re-establish a spoke-SDP if it fails and a label withdraw message is received with the status code “AII unreachable”.

The no form of this command reverts the timer to its default value.

Default 30

Parameters  
retry-timer — The initial retry-timer value in seconds.

Values  10 — 480

saii-type2

Syntax  
saii-type2 global-id:prefix:ac-id
no saiii-type2

Description  
This command configures the source attachment individual identifier for the spoke-sdp. This is only applicable to FEC129 AII type 2.

Parameters  
global-id — A Global ID of this 7x50 T-PE. This value must correspond to one of the global_id values configured for a local-prefix under config>service>pw-routing>local-prefix context.

Values  1 — 4294967295
VLL SDP Commands

pref **ix** — The prefix on this 7x50 T-PE that the spoke-sdp SDP is associated with. This value must correspond to one of the prefixes configured under `config>service>pw-routing>local-prefix` context.

**Values**  
an IPv4-formatted address a.b.c.d or 1 — 4294967295

ac-**i**d — An unsigned integer representing a locally unique identifier for the spoke-SDP.

**Values**  
1 — 4294967295

signaling

**Syntax**  
`signaling signaling`

**Context**  
`config>service>epipe>spoke-sdp-fec`

**Description**  
This command enables a user to configure this 7x50 as the active or passive T-PE for signaling this MS-PW, or to automatically select whether this T-PE is active or passive based on the prefix. In an active role, this endpoint initiates MS-PW signaling without waiting for a T-LDP label mapping message to arrive from the far end T-PE. In a passive role, it will wait for the initial label mapping message from the far end before sending a label mapping for this end of the PW. In auto mode, if the SAII has the greater prefix value, then the 7x50 will initiate MS-PW signaling without waiting for a label mapping message from the far end. However, if the TAII has the greater value prefix, then the 7x50 will assume that the far end T-PE will initiate MS-PW signaling and will wait for that label mapping message before responding with a T-LDP label mapping message for the MS-PW in the reverse direction.

The `no` form of the command means that the 7x50 T-PE automatically selects which 7x50 will initiate MS-PW signaling based on the prefix values configured in the SAII and TAII of the spoke-SDP, as described above.

**Default**  
`auto`

**Parameters**  
`signaling` — Configures this 7x50 as the active T-PE for signaling this MS-PW.

**Values**  
`auto, master`

standby-signaling-slave

**Syntax**  
`[no] standby-signaling-slave`

**Context**  
`config>service>epipe>spoke-sdp-fec`

taii-type2

**Syntax**  
`taii-type2 global-id:prefix:ac-id`

**Context**  
`config>service>epipe>spoke-sdp-fec`

`no taii-type2`
Description  taii-type2 configures the target attachment individual identifier for the spoke-sdp. This is only applicable to FEC129 AII type 2.
This command is blocked in CLI if this end of the spoke-SDP is configured for single-sided auto configuration (using the auto-config command).

Parameters  

- **global-id** — A Global ID of this 7x50 T-PE. This value must correspond to one of the global_id values configured for a local-prefix under config>service>pw-routing>local-prefix context.
  - **Values**  
    - 1 — 4294967295

- **prefix** — The prefix on this 7x50 T-PE that the spoke-sdp SDP is associated with. This value must correspond to one of the prefixes configured under config>service>pw-routing>local-prefix context.
  - **Values**  
    - an IPv4-formatted address a.b.c.d or 1 — 4294967295

- **ac-id** — An unsigned integer representing a locally unique identifier for the spoke-SDP.
  - **Values**  
    - 1 — 4294967295
**ATM Commands**

**atm**

**Syntax**

```
Syntax atm
```

**Context**

<table>
<thead>
<tr>
<th>Context</th>
</tr>
</thead>
<tbody>
<tr>
<td>config&gt;service&gt;epipe&gt;sap</td>
</tr>
<tr>
<td>config&gt;service&gt;apipe&gt;sap</td>
</tr>
<tr>
<td>config&gt;service&gt;ipipe&gt;sap</td>
</tr>
<tr>
<td>config&gt;service&gt;epipe&gt;sap</td>
</tr>
</tbody>
</table>

**Description**

This command enables access to the context to configure ATM-related attributes. This command can only be used when a given context (for example, a channel or SAP) supports ATM functionality such as:

- Configuring ATM port or ATM port-related functionality on MDAs supporting ATM functionality
- Configuring ATM-related configuration for ATM-based SAPs that exist on MDAs supporting ATM functionality.

If ATM functionality is not supported for a given context, the command returns an error.

**egress**

**Syntax**

```
Syntax egress
```

**Context**

<table>
<thead>
<tr>
<th>Context</th>
</tr>
</thead>
<tbody>
<tr>
<td>config&gt;service&gt;epipe&gt;sap</td>
</tr>
<tr>
<td>config&gt;service&gt;epipe&gt;sap&gt;atm</td>
</tr>
<tr>
<td>config&gt;service&gt;apipe&gt;sap&gt;atm</td>
</tr>
<tr>
<td>config&gt;service&gt;pipe&gt;sap</td>
</tr>
</tbody>
</table>

This command configures egress ATM attributes for the SAP.

**ingress**

**Syntax**

```
Syntax ingress
```

**Context**

<table>
<thead>
<tr>
<th>Context</th>
</tr>
</thead>
<tbody>
<tr>
<td>config&gt;service&gt;epipe&gt;sap</td>
</tr>
<tr>
<td>config&gt;service&gt;epipe&gt;sap&gt;atm</td>
</tr>
<tr>
<td>config&gt;service&gt;epipe&gt;sap</td>
</tr>
<tr>
<td>config&gt;service&gt;apipe&gt;sap&gt;atm</td>
</tr>
</tbody>
</table>

**Description**

This command configures ingress ATM attributes for the SAP.
encapsulation

Syntax  
```
encapsulation atm-encap-type
```

Context  
```
config>service>epipe>sap>atm
config>service>ipipe>sap>atm
```

Description  
This command specifies the data encapsulation for an ATM PVCC delimited SAP. The definition references RFC 2684, *Multiprotocol Encapsulation over ATM AAL5*, and to the ATM Forum LAN Emulation specification. Ingress traffic that does not match the configured encapsulation will be dropped.

Default  
The encapsulation is driven by the services for which the SAP is configured. For IES and VPRN service SAPs, the default is *aal5snap-routed*.

Parameters  
```
atm-encap-type — Specify the encapsulation type.
```

Values  
```
 * aal5snap-routed — Routed encapsulation for LLC encapsulated circuit (LLC/SNAP precedes protocol datagram) as defined in RFC 2684.
 * aal5mux-ip — Routed IP encapsulation for VC multiplexed circuit as defined in RFC 2684
```

traffic-desc

Syntax  
```
traffic-desc traffic-desc-profile-id
no traffic-desc
```

Context  
```
config>service>epipe>sap
config>service>apipe>sap>atm>egress
config>service>apipe>sap>atm>ingress
config>service>epipe>sap>atm>egress
config>service>epipe>sap>atm>ingress
```

Description  
This command assigns an ATM traffic descriptor profile to a given context (for example, a SAP). When configured under the ingress context, the specified traffic descriptor profile defines the traffic contract in the forward direction. When configured under the egress context, the specified traffic descriptor profile defines the traffic contract in the backward direction.

The `no` form of the command reverts the traffic descriptor to the default traffic descriptor profile.

Default  
The default traffic descriptor (trafficDescProfileId. = 1) is associated with newly created PVCC-delimited SAPs.

Parameters  
```
traffic-desc-profile-id — Specify a defined traffic descriptor profile (see the QoS atm-td-profile command).
```
OAM Commands

oam

Syntax  
oam

Context  
config>service>epipe>sap
config>service>apipe>sap>atm

Description  
This command enables the context to configure OAM functionality for a PVCC delimiting a SAP.

- The ATM-capable MDAs support end-to-end and segment OAM functionality (AIS, RDI, Loop-back) over both F5 (VC) and end-to-end F4 (VP) OAM:
- ITU-T Recommendation I.610 - B-ISDN Operation and Maintenance version 11/95
- GR-1248-CORE - Generic Requirements for Operations of ATM N3 June 1996

alarm-cells

Syntax  
[no] alarm-cells

Context  
config>service>epipe>sap>oam
config>service>epipe>sap>oam
config>service>apipe>sap>atm>oam

Description  
This command configures AIS/RDI fault management on a PVCC. Fault management allows PVCC terminations to monitor and report the status of their connection by propagating fault information through the network and by driving PVCC’s operational status.

When alarm-cells functionality is enabled, a PVCC’s operational status is affected when a PVCC goes into an AIS or RDI state because of an AIS/RDI processing (assuming nothing else affects PVCC’s operational status, for example, if the PVCC goes DOWN, or enters a fault state and comes back UP, or exits that fault state). RDI cells are generated when PVCC is operationally DOWN. No OAM-specific SNMP trap is raised whenever an endpoint enters/exits an AIS or RDI state, however, if as result of an OAM state change, the PVCC changes operational status, then a trap is expected from an entity the PVCC is associated with (for example a SAP).

The no command disables alarm-cells functionality for a PVCC. When alarm-cells functionality is disabled, a PVCC’s operational status is no longer affected by a PVCC’s OAM state changes due to AIS/RDI processing (Note that when alarm-cells is disabled, a PVCC will change operational status to UP due to alarm-cell processing) and RDI cells are not generated as result of the PVCC going into AIS or RDI state. The PVCC’s OAM status, however, will record OAM faults as described above.

Default  
Enabled for PVCCs delimiting IES SAPs
**terminate**

**Syntax**

[no] terminate

**Context**

config>service>apipe>sap>atm>oam

**Description**

This command specifies whether this SAP will act as an OAM termination point. ATM SAPs can be configured to tunnel or terminate OAM cells.

When configured to not terminate (the default is no terminate), the SAP will pass OAM cells through the VLL without inspecting them. The SAP will respond to OAM loopback requests that are directed to the local node by transmitting a loopback reply. Other loopback requests are transparently tunneled through the pseudowire. In this mode, it is possible to launch a loopback request towards the directly-attached ATM equipment and see the results of the reply.

When configured to terminate, the SAP will respond to AIS by transmitting RDI and will signal the change of operational status to the other endpoint (for example, through LDP status notifications). The SAP will respond to OAM loopback requests by transmitting a loopback reply. In this mode, it is possible to launch a loopback request towards the directly-attached ATM equipment and see the results of the reply.

For Apipe services, the user has the option of enabling or disabling this option for VC types atm-vcc and atm-sdu since these service types maintain the ATM layer and/or the AAL5 layer across the VLL. It is not supported on atm-vpc and atm-cell Apipe vc types since the VLL must pass the VC level (F5) OAM cells.

The terminate option for OAM is the only and default mode of operation supported for an ATM SAP which is part of Epipe, Ipipe, VPLS, and IES/VPRN. This is because the ATM and AAL5 layers are terminated.

For Apipe services, the user has the option of enabling or disabling this option for vc types atm-vcc and atm-sdu since these service types maintain the ATM layer and/or the AAL5 layer across the VLL. It is not supported on atm-vpc and atm-cell Apipe vc types since the VLL must pass the VC level (F5).

The terminate option for OAM is the only and default mode of operation supported for an ATM SAP which is part of Epipe, Ipipe, VPLS, and IES/VPRN. This is because the ATM and AAL5 layers are terminated.

**Default**

no terminate

**service-name**

**Syntax**

service-name service-name

no service-name

**Context**

config>service>epipe

**Description**

This command configures an optional service name, up to 64 characters in length, which adds a name identifier to a given service to then use that service name in configuration references as well as display and use service names in show commands throughout the system. This helps the service provider/administrator to identify and manage services within the router platforms.
All services are required to assign a service ID to initially create a service. However, either the service ID or the service name can be used to identify and reference a given service once it is initially created.

**Parameters**  
*service-name* — Specifies a unique service name to identify the service. Service names may not begin with an integer (0-9).

### site

**Syntax**
```
site name [create]  
no site name
```

**Context**
```
config>service>epipe
```

**Description**
This command configures an Epipe site.

The *no* form of the command removes the name from the configuration.

**Parameters**
*name* — Specifies a site name up to 32 characters in length.
*create* — This keyword is mandatory while creating a service.
Virtual Leased Line Services

CPipe SDP Commands

spoke-sdp

Syntax

spoke-sdp sdp-id[:vc-id] [no-endpoint] [create]
spoke-sdp sdp-id:vc-id [create] endpoint endpoint-name [icb]
no spoke-sdp sdp-id[:vc-id]

Context

config>service>cpipe

Description

This command binds a service to an existing Service Distribution Point (SDP). A spoke SDP is treated like the equivalent of a traditional bridge “port” where flooded traffic received on the spoke SDP is replicated on all other “ports” (other spoke and mesh SDPs or SAPs) and not transmitted on the port it was received.

The SDP has an operational state which determines the operational state of the SDP within the service. For example, if the SDP is administratively or operationally down, the SDP for the service will be down.

The SDP must already be defined in the config>service>sdp context. If the sdp sdp-id is not already configured, an error message is generated. If the sdp-id does exist, a binding between that sdp-id and the service is created.

SDPs must be explicitly associated and bound to a service. If an SDP is not bound to a service, no far-end devices can participate in the service.

The no form of this command removes the SDP binding from the service. The SDP configuration is not affected; only the binding of the SDP to a service. Once removed, no packets are forwarded to the far-end router.

Default

No sdp-id is bound to a service.

Parameters

sdp-id — The SDP identifier. Allowed values are integers in the range of 1 to 17407 for existing SDPs.

vc-id — The virtual circuit identifier.

Values

1 — 4294967295

vc-type — This command overrides the default VC type signaled for the spoke or mesh binding to the far end of the SDP. The VC type is a 15 bit-quantity containing a value which represents the type of VC. The actual signaling of the VC type depends on the signaling parameter defined for the SDP. If signaling is disabled, the vc-type command can still be used to define the dot1q value expected by the far-end provider equipment. A change of the bindings VC type causes the binding to signal the new VC type to the far end when signaling is enabled.

VC types are derived according to IETF draft-martini-l2circuit-trans-mpls.

- The VC type value for Ethernet is 0x0005.
- The VC type value for an Ethernet VLAN is 0x0004.
- The VC type value for a VPLS service is defined as 0x000B.

Values

ethernet

no endpoint — removes the association of a spoke SDP with an explicit endpoint name.
VLL SDP Commands

endpoint endpoint-name — Specifies the name of the service endpoint.
ich — Configures the spoke SDP as an inter-chassis backup SDP binding.

egress
Syntax  egress
Context  config>service>cpipe>spoke-sdp
Description  This command enables the context to configure egress spoke-SDP context.

ingress
Syntax  ingress
Context  config>service>cpipe>spoke-sdp
Description  This command enables the context to configure ingress spoke-SDP context.

vc-label
Syntax  vc-label  egress-vc-label
no vc-label  [egress-vc-label]
Context  config>service>cpipe>spoke-sdp>egress
Description  This command configures the spoke-SDP egress VC label.
Parameters  egress-vc-label — A VC egress value that indicates a specific connection.
  Values  16 — 1048575

vc-label
Syntax  vc-label  ingress-vc-label
no vc-label  [ingress-vc-label]
Context  config>service>cpipe>spoke-sdp>ingress
Description  This command configures the spoke-SDP ingress VC label.
Parameters  ingress-vc-label — A VC ingress value that indicates a specific connection.
  Values  2048 — 18431
precedence

Syntax  `precedence [precedence-value| primary]`
        `no precedence`

Context  `config>service>cpipe>spoke-sdp`

Description  This command specifies the precedence of the SDP binding when there are multiple SDP bindings attached to one service endpoint. The value of zero can only be assigned to one SDP bind making it the primary SDP bind. When an SDP binding goes down, the next highest precedence SDP binding will begin to forward traffic.

The `no` form of the command returns the precedence value to the default.

Default  4

Parameters  `precedence-value` — Specifies the spoke SDP precedence.

    Values  1 — 4

`primary` — Specifies to make this the primary spoke SDP.
In This Chapter

This chapter provides information about Ethernet Virtual Private Networks (EVPN), process overview, and implementation notes.

Topics in this chapter include:

- Overview on page 496
- EVPN for VXLAN Tunnels in a Layer-2 DC GW on page 497
Overview

EVPN is an IETF technology (draft-ietf-l2vpn-evpn) that uses a new BGP address family and allows VPLS services to be operated as IP-VPNs, where the MAC addresses and the information to setup the flooding trees are distributed by BGP.

EVPN is defined to fill the gaps of other L2VPN technologies like VPLS. EVPN’s main objective is to build ELAN services in a similar way to RFC4364 IP-VPNs, while supporting MAC learning within the control plane (distributed by MP-BGP), efficient multi-destination traffic delivery and active-active multi-homing.

EVPN can be used as the control plane for different data plane encapsulations. Alcatel-Lucent’s implementation supports EVPN for VXLAN overlay tunnels, being the Data Center Gateway (DC GW) function the main application for this feature. In such application VXLAN is expected within the Data Center and VPLS sdp-bindings or SAPs are expected for the connectivity to the WAN. R-VPLS and VPRN connectivity to the WAN is also supported.

The 7x50 SR/ESS/XRS EVPN for VXLAN implementation is perfectly integrated in the Nuage Data Center architecture, where the 7x50 plays the role of the Data Center Gateway (DC GW).

Refer to the Nuage Networks Virtualized Service Platform Guide for more information about the Nuage Networks architecture and products. The following sections describe the applications supported by EVPN in the 7x50 implementation.
EVPN for VXLAN Tunnels in a Layer-2 DC GW

Figure 72 depicts the use of EVPN for VXLAN overlay tunnels on the 7x50 SR/ESS/XRS when it is used as a layer-2 DC GW.

DC providers require a DC GW solution that can extend tenant subnets to the WAN. Due to the shortcomings explained in the previous section, customers will be deploying NVO3-based solutions in the DC, where EVPN is the standard control plane and VXLAN is the data plane encapsulation becoming predominant. The Alcatel-Lucent DC architecture, a.k.a Nuage, uses EVPN and VXLAN as the control and data plane solutions for layer-2 connectivity within the DC and so does the 7x50 SR OS.

While EVPN with VXLAN will be used within the DC, most of the Service Providers use VPLS and H-VPLS as the solution to extend layer-2 VPN connectivity. Figure 72 above illustrates the layer-2 DC GW function on the 7x50, providing VXLAN connectivity to the DC and regular VPLS connectivity to the WAN.
The WAN connectivity will be based on VPLS where SAPs (null, dot1q and qinq), spoke-SDPs (FEC type 128 and 129) and mesh-SDPs are supported.

The DC GWs can provide multi-homing resiliency through the use of BGP Multi-homing.
EVPN for VXLAN Tunnels in a Layer-2 DC with Integrated Routing Bridging Connectivity on the DC GW

Figure 73 depicts use of EVPN for VXLAN overlay tunnels on the 7x50 SR/ESS/XRS, when the DC provides layer-2 connectivity and the DC GW can route the traffic to the WAN through an R-VPLS and linked VPRN.

In some cases, the DC GW must provide a Layer 3 ‘default gateway’ function to all the hosts in a given tenant subnet. In this case, the VXLAN data plane will be terminated in an R-VPLS on the DC GW, and connectivity to the WAN will be accomplished through regular VPRN connectivity.
The 7x50 SROS and Nuage solution for DC supports VXLAN (Virtual eXtensible Local Area Network) overlay tunnels as per draft-mahalingam-dutt-dcops-vxlan.

VXLAN addresses the data plane needs for overlay networks within virtualized data centers accommodating multiple tenants. The main attributes of the VXLAN encapsulation are:

- VXLAN is an overlay network encapsulation used to carry MAC traffic between VMs over a logical Layer 3 tunnel.
- Avoids the Layer 2 MAC explosion, since VM MACs are only learnt at the edge of the network. Core nodes simply route the traffic based on the destination IP (which is the system IP address of the remote PE or VTEP – VXLAN Tunnel End Point).
- Supports multi-path scalability through ECMP (to a remote VTEP address, based on source UDP port entropy) while preserving the Layer 2 connectivity between VMs. xSTP is no longer needed in the network.
- Supports multiple tenants, each with its own isolated Layer 2 domain. The tenant identifier is encoded in the VNI field (VXLAN Network Identifier) and allows up to 16M values, as opposed to the 4k values provided by the 802.1q VLAN space.

Figure 74 outlines the VXLAN encapsulation supported by the Alcatel-Lucent’s implementation.
Figure 74: VXLAN Frame Format

As shown in Figure 74, VXLAN encapsulates the inner Ethernet frames into a VXLAN + UDP/IP packets. The main pieces of information encoded in this encapsulation are:

- **Outer Dest MAC**
- **Outer Src MAC** (System MAC)
- **Etype**
- **VLAN tag info**
- **Etype 0x0800**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source and Destination VTEPs</td>
<td>VTEPs reside on Hypervisors or TOR nodes or VXLAN gateways (MAC can also be intermediate or node interfaces)</td>
</tr>
<tr>
<td>Source UDP Port</td>
<td>- Hash of the inner MAC/IPs to enable entropy for ECMP load balancing</td>
</tr>
<tr>
<td>Destination UDP Port</td>
<td>- Well-known port = 4799 (IANA assigned)</td>
</tr>
<tr>
<td>Checksum</td>
<td>- should be 0 (non-0 must be accepted if correct)</td>
</tr>
</tbody>
</table>
| VXLAN Header (8 bytes) | - Flags (8 bits)
  - I = 1 for a valid VNI
  - R = 0 (reserved bits)
  - VXLAN VNI - 24 bit: to designate the individual VXLAN overlay network. VMs in different VNI cannot communicate
  - Reserved fields (24 bits and 8 bits) MUST be set to zero |

VXLAN encapsulates the inner Ethernet frames into a VXLAN + UDP/IP packets. The main pieces of information encoded in this encapsulation are:
• VXLAN header (8 bytes)
  → Flags (8 bits) where the I flag is set to 1 to indicate that the VNI is present and valid.
    The rest of the flags (“Reserved” bits) are set to 0.
  → Includes the VNI field (24-bit value) or VXLAN network identifier. It identifies an
    isolated layer-2 domain within the DC network.
  → The rest of the fields are reserved for future use.
• UDP header (8 bytes)
  → Where the destination port is a well-known UDP port assigned by IANA (4789).
  → The source port is derived from a hashing of the inner source and destination MAC/IP
    addresses that the 7x50 does at ingress. This will create an “entropy” value that can be
    used by the core DC nodes for load balancing on ECMP paths.
  → The checksum will be set to zero.
• Outer IP and Ethernet headers (34 or 28 bytes)
  → The source IP and source MAC will identify the source VTEP. In other words, these
    fields will be populated with the PE’s system IP and chassis MAC address. Note that
    the source MAC address will be changed on all the IP hops along the path, as usually
    is in regular IP routing.
  → The destination IP will identify the remote VTEP (remote system IP) and will be the
    result of the destination MAC lookup in the service FDB. Note that all the remote
    MACs will be learnt by EVPN BGP and associated to a remote VTEP address and
    VNI.

Some considerations related to the support of VXLAN on the 7x50 are listed below:

• VXLAN is only supported on network or hybrid ports with null or dot1q encapsulation.
• VXLAN is supported on Ethernet/LAG and POS/APS.
• Only IPv4 unicast addresses are supported as VTEPs.
• Only System IP addresses are supported, as VTEPs, for originating and terminating
  VXLAN tunnels.
VXLAN ECMP and LAG

The DC GW supports ECMP load balancing to reach the destination VTEP. Also, any intermediate core node in the Data Center should be able to provide further load balancing across ECMP paths since the source UDP port of each tunneled packet is derived from a hash of the customer inner packet. The following considerations must be taken into account:

- ECMP for VXLAN is supported on VPLS services, but not for BUM traffic. Unicast spraying will be based on the packet contents.
- ECMP for VXLAN is not supported on RVPLS services.
- In both cases where ECMP is not supported, each VXLAN binding is tied to a single (different) ECMP path, so in a normal deployment with a reasonable number of remote VTEPs, there should be a fair distribution of the traffic across the paths.
- LAG spraying based on the packet hash is supported in all the cases (VPLS unicast, VPLS BUM and R-VPLS).

VXLAN VPLS Tag Handling

The following describes the behavior on the 7x50 with respect to VLAN tag handling for VXLAN VPLS services:

- Dot1q, QinQ, and null SAPs as well as regular VLAN handling procedures at the WAN side are supported on VXLAN VPLS services.
- No “vc-type vlan” like VXLAN VNI bindings are supported. Therefore, at the egress of the VXLAN network port, the 7x50 will not add any inner VLAN tag on top of the VXLAN encapsulation, and at the ingress network port, the 7x50 will ignore any VLAN tag received and will consider it as part of the payload.

VXLAN MTU Considerations

For VXLAN VPLS services, the network port MTU MUST be at least 50B (54B if dot1q) greater than the Service-MTU to allow enough room for the VXLAN encapsulation.

The Service-MTU is only enforced on SAPs (any sap ingress packet with MTU greater than the service-mtu will be discarded) and not on VXLAN termination (any VXLAN ingress packet will make it to the egress SAP regardless of the configured service-mtu).

Note: The 7x50 will never fragment or reassemble VXLAN packets. In addition, the 7x50 always sets the DF (Do not Fragment) flag in the VXLAN outer IP header.
VXLAN QoS

VXLAN is a network port encapsulation, therefore, the QoS settings for VXLAN are controlled from the network QoS policies:

- The ingress network qos policy is used to classify the VXLAN packets based on the outer dot1p (if present) and then the DSCP to yield a FC/profile.

- On egress, since VXLAN adds a new IPv4 header, and the DSCP will be always marked based on the egress network qos policy. There is no need to specify “remarking” in the policy to mark the DSCP.
BGP-EVPN Control Plane for VXLAN Overlay Tunnels

The draft-sd-l2vpn-evpn-overlay describes EVPN as the control plane for overlay based networks. The 7x50 supports a subset of the routes and features described in draft-ietf-l2vpn-evpn that are required for the DC GW function. In particular, EVPN-specific multi-homing capabilities are not supported. Multi-homing can be supported though by using regular BGP-Multi-homing based on the L2VPN BGP address family.

Figure 75 shows the EVPN MP-BGP NLRI, required attributes and extended communities, and two route-types supported for the DC GW application:

- route type 3 – Inclusive Multicast Ethernet Tag route
- route type 2 – MAC Advertisement route
EVPN Route Type 3 – Inclusive Multicast Ethernet Tag Route

Route type 3 is used for setting up the flooding tree (BUM flooding) for a given VPLS service within the data center. The received inclusive multicast routes will add entries to the VPLS flood list in the 7x50. Only ingress replication is supported over VXLAN.

A route type 3 is generated from the 7x50 per VPLS service as soon as the service is UP and uses the following fields and values:

- Route Distinguisher: Taken from the RD configured in the VPLS service within the BGP context.
- Ethernet Tag ID: Carries the VNI configured in the VPLS service. Only one VNI can be configured per VPLS service.
- IP address length: always 32.
- Originating router’s IP address: Carries the system address (ipv4 only).
- PMSI attribute:
  - Tunnel type = Ingress replication (6)
  - Flags = Leaf no required
  - MPLS label = 0
  - Tunnel end-point = equal to the originating IP address

EVPN Route Type 2 – MAC Advertisement Route

The 7x50 will generate this route type for advertising MAC addresses. The 7x50 will generate MAC advertisement routes for the following:

- Learned macs on SAPs or sdp-bindings – if mac-advertisement is enabled.
- Conditional static macs – if mac-advertisement is enabled.
- unknown-mac-routes – if unknown-mac-route is enabled, there is no bgp-mh site in the service or there is a (single) DF site.

The route type 2 generated by a 7x50 uses the following fields and values:

- Route Distinguisher: Taken from the RD configured in the VPLS service within the BGP context.
- Ethernet Segment Identifier (ESI): Value = 0:0:0:0:0:0:0:0:0:0:0
- Ethernet Tag ID: Carries the VNI configured in the VPLS service. Only one VNI can be configured per VPLS.
- MAC address length: Always 48.
• MAC Address:
  → It will be 00:00:00:00:00:00 for the Unknown MAC route address.
  → It will be different from 00:…:00 for the rest if the advertised MACs.

• IP address and IP address length:
  → It will be the IP address associated to the MAC being advertised with a length of 32.
  → If the MAC address is the Unknown MAC route then the IP address length is zero and the IP is omitted.
  → In general, any MAC route without IP will have IPL=0 (IP length) and the IP will be omitted.
  → At reception, any IPL value different from zero or 32 will make discard the route.

• MPLS Label = 0.

• The MAC Mobility extended community: used for signaling the sequence number in case of mac moves and the sticky bit in case of advertising conditional static macs. If a MAC route is received with a MAC mobility ext-community, the sequence number and the ‘sticky’ bit are taken into account for the route selection.
The EVPN-VXLAN service is modeled around the current VPLS objects and the additional VXLAN construct.

Figure 72 depicts a DC with a layer-2 service that carries the traffic for a tenant who wants to extend a subnet beyond the DC. The DC PE function is carried out by the 7x50 where a VPLS instance exists for that particular tenant. Within the DC, the tenant will have VPLS instances in all the Network Virtualization Edge (NVE) devices where it requires connectivity (such VPLS instances can be instantiated in TORs, Nuage VRS, VSG, etc.). The VPLS instances in the redundant DC GW and the DC NVEs will be connected by VXLAN bindings. BGP-EVPN will provide the required control plane for such VXLAN connectivity.

The DC GW 7x50s will be configured with a VPLS per tenant that will provide the VXLAN connectivity to the Nuage VPLS instances. On the 7x50 each tenant VPLS instance will be configured with:

- The WAN-related parameters (saps, spoke-sdps, mesh-sdps, bgp-ad, etc).
- The BGP-EVPN and VXLAN (VNI) parameters. The following CLI output shows an example for an EVPN-VXLAN VPLS service.

```
*A:DGW1>config>service>vpls# info
---------------------------------------------------------------------
description "vxlan-service"
vxlan vni 1 create
exit
bgp
    route-distinguisher 65001:1
    route-target export target:65000:1 import target:65000:1
exit
bgp-evpn
    unknown-mac-route
    mac-advertisement
    vxlan
    no shutdown
    exit
sap 1/1/1:1 create
exit
no shutdown
---------------------------------------------------------------------
```

The bgp-evpn context specifies the encapsulation type (only vxlan is supported) to be used by EVPN and other parameters like the unknown-mac-route and mac-advertisement commands. These commands are typically configured in three different ways:

- **no unknown-mac-route** and **mac-advertisement** (default option) — The 7x50 will advertise new learnt macs (on the SAPs or sdp-bindings) or new conditional static macs.
• **unknown-mac-route and no mac-advertisement** — The 7x50 will only advertise an unknown-mac-route as long as the service is operationally UP (if no BGP-MH site is configured in the service) or the 7x50 is the DF (if BGP-MH is configured in the service).

• **unknown-mac-route and mac-advertisement** — The 7x50 will advertise new learnt macs, conditional static macs and the unknown-mac-route. The unknown-mac-route will only be advertised under the conditions described above.

Other parameters related to EVPN or VXLAN are:

• Mac duplication parameters

• *vxlan vni*: defines the VNI that the 7x50 will use in the EVPN routes generated for the VPLS service.

Once the VPLS is properly configured and operationally UP, the 7x50 will send/receive Inclusive Multicast Ethernet Tag routes, and a full-mesh of VXLAN connections will be automatically created. These VXLAN “auto-bindings” can be characterized as follows:

• The VXLAN auto-bindings are modeled following an IP-VPN-like model, where no SDPs or SDP-binding objects are created or visible by the user. The VXLAN auto-binds are composed of remote VTEPs and egress VNIs, and can be displayed with the following command:

```
*A:DGW# show service id 1 vxlan
```

```
VPLS VXLAN, Ingress VXLAN Network Id: 1

Egress VTEP, VNI

<table>
<thead>
<tr>
<th>VTEP Address</th>
<th>Egress VNI</th>
<th>Num. MACs</th>
<th>In Mcast List?</th>
<th>Oper State</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.0.0.71</td>
<td>1</td>
<td>1</td>
<td>Yes</td>
<td>Up</td>
</tr>
<tr>
<td>192.0.0.72</td>
<td>1</td>
<td>1</td>
<td>Yes</td>
<td>Up</td>
</tr>
</tbody>
</table>

Number of Egress VTEP, VNI : 2
```

• The VXLAN bindings observe the VPLS split-horizon rule. This is done automatically without the need of any split-horizon configuration.

Once the flooding domain is setup, the 7x50s and DC NVEs start advertising MAC addresses, and the 7x50s can learn MACs and install them in the FDB. Some considerations are the following:

• All the MAC addresses associated to remote VTEP/VNIs are always learned in the control plane by EVPN. Data plane learning on VXLAN auto-bindings is not supported.

• When **unknown-mac-route** is configured, it will be generated when: a) no (BGP-MH) site is configured, or b) a site is configured AND the site is DF in the PE. Note that the
unknown-mac-route will not be installed in the FDB (hence will not show up in the show service id x fdb detail command).

- Note that, although the 7x50 can be configured with only one VNI (and signals a single VNI per VPLS), it can accept any VNI in the received EVPN routes as long as the route-target is properly imported. The VTEPs and VNIs will show up in the FDB associated to MAC addresses:

A:PE65# show service id 1000 fdb detail

<table>
<thead>
<tr>
<th>ServId</th>
<th>MAC</th>
<th>Source-Identifier</th>
<th>Type</th>
<th>Last Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>1000</td>
<td>00:00:00:00:00:00</td>
<td>vxlan:</td>
<td>Evpn</td>
<td>10/05/13 23:25:57</td>
</tr>
<tr>
<td></td>
<td>00:00:00:00:00:65</td>
<td>sap:1/1/1:1000</td>
<td>L/30</td>
<td>10/05/13 23:25:57</td>
</tr>
<tr>
<td>1000</td>
<td>00:ca:ca:ca:ca:00</td>
<td>vxlan:</td>
<td>EvpnS</td>
<td>10/04/13 17:35:43</td>
</tr>
</tbody>
</table>

No. of MAC Entries: 3

Legend:  L=Learned  O=Oam  P=Protected-MAC

---

**Resiliency and BGP Multi-Homing**

The DC overlay infrastructure relies on IP tunneling, that is, VXLAN; the underlay IP layer sorts out, therefore, failure in the DC core. The IGP should be optimized to get the fastest convergence.

From a service perspective, resilient connectivity to the WAN is provided by BGP-Multi-homing.

---

**Use of bgp-evpn, bgp-ad, and Sites in the Same VPLS Service**

bgp-evpn (control plane for a VXLAN DC), bgp-ad (control plane for MPLS-based spoke-sdps connected to the WAN) and ONE site for BGP multi-homing (control plane for the multi-homed connection to the WAN) can be all configured in one service in a given system. If that is the case, the following considerations apply:

- The configured bgp route-distinguisher and route-target are used by BGP for the two families, that is, evpn and l2vpn. If different import/export route targets are to be used per family, vsi-import/export policies must be used.

- The pw-template-binding command under bgp, does not have any effect on evpn or bgp-mh. It is only used for the instantiation of the bgp-ad spoke-sdps.
• If the same import/export route-targets are used in the two redundant DC GWs, VXLAN binding as well as a fec129 spoke-sdp binding will be established between the two DGWs, creating a loop. To avoid creating a loop, the 7x50 will allow the establishment of an EVPN VXLAN binding and an sdp-binding to the same far-end, but the sdp-binding will be kept operationally down. Only the VXLAN binding will be operationally up.
Use of the unknown-mac-route

This section describes the behavior of the EVPN-VXLAN service in the 7x50 when the unknown-mac-route and BGP-MH are configured at the same time.

The use of E-VPN, as the control plane of NVO networks in the DC, brings a significant number of benefits as described in draft-sd-l2vpn-evpn-overlay. There is however a potential issue that SHOULD be addressed when a VPLS DCI is used for an NVO3-based DC: all the MAC addresses learned from the WAN side of the VPLS must be advertised by BGP E-VPN updates. Even if optimized BGP techniques like RT-constraint are used, the amount of MAC addresses to advertise or withdraw (in case of failure) from the DC GWs can be difficult to control and overwhelming for the DC network, especially when the NVEs reside in the hypervisors.

The 7x50 solution to this issue is based on the use of an unknown-mac-route address that is advertised by the DC PEs. By using this unknown-mac-route advertisement, the DC tenant may decide to optionally turn off the advertisement of WAN MAC addresses in the DC GW, hence reducing the control plane overhead and the size of the FDB tables in the NVEs.

The use of the unknown-mac-route is optional and helps to reduce the amount of unknown-unicast traffic within the data center. All the receiving NVEs supporting this concept will send any unknown-unicast packet to the owner of the unknown-mac-route, as opposed to flooding the unknown-unicast traffic to all other NVEs part of the same VPLS.

Note: Although the 7x50 can be configured to generate and advertise the unknown-mac-route, the 7x50 will never honor the unknown-mac-route and will flood to the TLS-flood list when an unknown-unicast packet arrives to an ingress sap/sdp-binding.

The use of the unknown-mac-route assumes the following:

1. a fully virtualized DC where all the MACs are control-plane learned, and learned previously to any communication (no legacy TORs or VLAN connected servers).
2. The only exception is MACs learned over the SAPs/SDP-bindings that are part of the BGP-MH WAN site-id. Only one site-id is supported in this case.
3. No other SAPs/SDP-bindings out of the WAN site-id are supported, unless ONLY static macs are used on those SAPs/SDP-bindings.

Therefore, when unknown-mac-route is configured, it will ONLY be generated when:

• no site is configured and the service is operationally UP or
• a BGP-MH site is configured AND the DC GW is Designated Forwarder (DF) for the site. In case of BGP-MH failover, the unknown-mac-route will be withdrawn by the former DF and advertised by the new DF.
Proxy-ARP Table

A proxy-ARP table per VPLS service is created and populated by the MAC-IP pairs received from bgp-evpn advertisements. The entries do not age out and can only be flushed by the corresponding bgp-evpn route withdraw. When a new ARP-request arrives at a sap/sdp-binding, a lookup is done on the proxy-arp table:

• If there is no match, the ARP-request is flooded.
• If there is a match, an ARP-reply is issued to the requester as long as its MAC address is in the FDB.

If a VPLS is bound to a VPRN service, then MAC-IP pairs received from bgp-evpn advertisements are used to populate the VPRN ARP table.

BGP-EVPN MAC-Mobility

EVPN defines a mechanism to allow the smooth mobility of MAC addresses from an NVE to another NVE. The 7x50 supports this procedure as well as the MAC-mobility extended community in MAC advertisement routes as in the following:

• The 7x50 honors and generates the SEQ (Sequence) number in the mac mobility extended community for mac moves.
• When a MAC is EVPN-learned and it is attempted to be learned locally, a bgp update is sent with SEQ number changed to “previous SEQ”+1 (exception: mac duplication num-moves value is reached).
• SEQ number = zero or no mac mobility ext comm are interpreted as sequence zero.
• In case of mobility, the following MAC selection procedure is followed:
  → If a PE has two or more active remote EVPN routes for the same MAC (VNI can be the same or different), the highest SEQ number is selected. The tie-breaker is the lowest IP (BGP NH IP).
  → If a PE has two or more active EVPN routes and it is the originator of one of them, the highest SEQ number is selected. The tie-breaker is the lowest IP (BGP NH IP of the remote route is compared to the local system address).

BGP-EVPN MAC-duplication

EVPN defines a mechanism to protect the EVPN service from control plane churn as a result of loops or accidental duplicated MAC addresses. The 7x50 supports an enhanced version of this procedure as described in this section.
A situation may arise where the same MAC address is learned by different PEs in the same VPLS because of two (or more hosts) being mis-configured with the same (duplicate) MAC address. In such situation, the traffic originating from these hosts would trigger continuous MAC moves among the PEs attached to these hosts. It is important to recognize such situation and avoid incrementing the sequence number (in the MAC Mobility attribute) to infinity.

To remedy such situation, a 7x50 that detects a MAC mobility event by way of local learning starts a window <in-minutes> timer (default value of window = 3) and if it detects num-moves <num> before the timer expires (default value of num-moves = 5), it concludes that a duplicate MAC situation has occurred. The 7x50 then alerts the operator with a trap message. The offending MAC address can be shown using the show service id x bgp-evpn command:

```
10 2014/01/14 01:00:22.91 UTC MINOR: SVCMGR #2331 Base
"VPLS Service 1 has MAC(s) detected as duplicates by EVPN mac-duplication detection."
# show service id 1 bgp-evpn
```

```
BGP EVPN Table

MAC Advertisement : Enabled            Unknown MAC Route  : Disabled
VXLAN Admin Status  : Enabled            Creation Origin    : manual
MAC Dup Detn Moves : 5                  MAC Dup Detn Window: 3
MAC Dup Detn Retry : 9                  Number ofDupMACs : 1

Detected Duplicate MAC Addresses             Time Detected
-----------------------------------------------
00:00:00:00:00:12                            01/14/2014 01:00:23

After detecting the duplicate, the 7x50 stops sending and processing any BGP MAC advertisement routes for that MAC address till:

- The MAC is flushed due to a local event (sap/sdp-binding associated to the MAC fails) or the reception of a remote update with better SEQ number (due to a mac flush at the remote 7x50) or
- The retry in_minutes timer expires, which will flush the MAC and restart the process.

Note: The other 7x50s in the VPLS instance will forward the traffic for the duplicate MAC address to the 7x50 advertising the best route for the MAC.

The values of num-moves and window are configurable to allow for the required flexibility in different environments. In scenarios where bgp rapid-update evpn is configured, the operator might want to configure a shorter window timer than in scenarios where BGP updates are sent every (default) min-route-advertisement interval.

mac-duplication is always enabled in EVPN-VXLAN VPLS services, and the mac duplication parameters described above can be configured per VPLS service under the bgp-evpn mac-duplication context:
Conditional Static MAC and Protection

The draft-sd-l2vpn-evpn-overlay defines the use of the sticky bit in the mac-mobility extended community to signal static mac addresses. These addresses must be protected in case there is an attempt to dynamically learn them in a different place in the EVPN-VXLAN VPLS service.

In the 7x50, any conditional static mac defined in an EVPN-VXLAN VPLS service will be advertised by BGP-EVPN as static address, that is, with the sticky bit set. An example of the configuration of a conditional static mac is shown below:

```bash
*A:PE63>config>service>vpls# info
----------------------------------------------
description "vxlan-service"
...
sap 1/1/1:1000 create
exit
static-mac
    mac 00:ca:ca:ca:ca:00 create sap 1/1/1:1000 monitor fwd-status
exit
no shutdown
*A:PE64#
```

```bash
show router bgp routes evpn mac hunt mac-address 00:ca:ca:ca:ca:00
```

BGP EVPN Mac Routes

<table>
<thead>
<tr>
<th>Network</th>
<th>0.0.0.0/0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nexthop</td>
<td>192.0.2.63</td>
</tr>
<tr>
<td>From</td>
<td>192.0.2.63</td>
</tr>
<tr>
<td>Res. Nexthop</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>Local Pref.</td>
<td>100</td>
</tr>
<tr>
<td>Aggregator AS</td>
<td>None</td>
</tr>
<tr>
<td>Atomic Aggr.</td>
<td>Not Atomic</td>
</tr>
<tr>
<td>AIGP Metric</td>
<td>None</td>
</tr>
<tr>
<td>Connector</td>
<td>None</td>
</tr>
<tr>
<td>Community</td>
<td>target:65000:1000</td>
</tr>
<tr>
<td>Cluster</td>
<td>No Cluster Members</td>
</tr>
<tr>
<td>Originator Id</td>
<td>None</td>
</tr>
<tr>
<td>Peer Router Id</td>
<td>192.0.2.63</td>
</tr>
<tr>
<td>Flags</td>
<td>Used Valid Best IGP</td>
</tr>
<tr>
<td>Route Source</td>
<td>Internal</td>
</tr>
<tr>
<td>AS-Path</td>
<td>No As-Path</td>
</tr>
<tr>
<td>EVPN type</td>
<td>MAC</td>
</tr>
</tbody>
</table>
Local static MACs or remote MACs with sticky bit are considered as ‘protected’. A packet entering a SAP / SDP-binding will be discarded if its source MAC addresses matches one of these ‘protected’ MACs.
EVPN for VXLAN in R-VPLS Services

Figure 73 depicts a DC with a layer-2 service that carries the traffic for a tenant who extends a subnet within the DC, while the DC GW is the default gateway for all the hosts in the subnet. The DC GW function is carried out by the 7x50 where an R-VPLS instance exists for that particular tenant. Within the DC, the tenant will have VPLS instances in all the NVE devices where it requires connectivity (such VPLS instances can be instantiated in TORs, Nuage VRS, VSG, etc.). The WAN connectivity will be based on existing IP-VPN features.

In this model, the DC GW 7x50s will be configured with a R-VPLS (bound to the VPRN that provides the WAN connectivity) per tenant that will provide the VXLAN connectivity to the Nuage VPLS instances. This model provides inter-subnet forwarding for L2-only TORs and other L2 DC NVEs.

On the 7x50:

- The VPRN will be configured with an interface bound to the backhaul R-VPLS. That interface will be a regular IP interface (IP address configured).
- The VPRN can support other numbered interfaces to the WAN or even to the DC.
- The R-VPLS will be configured with the BGP, BGP-EVPN and VXLAN (VNI) parameters.

On the Nuage VSGs and NVEs:

- Regular VPLS service model with BGP EVPN and VXLAN parameters.

Other considerations:

- Route-type 2 routes with MACs and IPs will be advertised. Some considerations about MAC+IP and ARP entries are listed below:
  - The 7750 will advertise its IRB MAC+IP in a route type 2 route and possibly the VRRP vMAC+vIP if it runs VRRP and it is the master. In both cases, the MACs will be advertised as conditional static MACs, hence protected by the receiving PEs.
  - If the 7750 VPRN interface is configured with one or more additional secondary IP addresses, they will all be advertised in routes type 2, as conditional static MACs.
  - The 7750 will process route-type 2 routes as usual, populating the FDB with the received MACs and the VPRN ARP table with the MAC and IPs respectively. The ARP entries coming from EVPN will be tagged as “EVPN”:

```
A:PE73# show router 2 arp
------------------------------------------------------------------------------------
ARP Table (Service: 2)
------------------------------------------------------------------------------------
IP Address      MAC Address       Expiry    Type   Interface
------------------------------------------------------------------------------------
10.10.10.70     d8:46:ff:ff:ff:3e 00h00m00s Evp[I] local
```

A:PE73# show router 2 arp
------------------------------------------------------------------------------------
ARP Table (Service: 2)
------------------------------------------------------------------------------------
IP Address      MAC Address       Expiry    Type   Interface
------------------------------------------------------------------------------------
10.10.10.70     d8:46:ff:ff:ff:3e 00h00m00s Evp[I] local
When a VPLS containing proxy-ARP entries is bound to a VPRN (allow-ip-int-binding) all the proxy-ARP entries are moved to the VPRN ARP table. ARP entries will be also moved to proxy-ARP entries if the VPLS is unbound.

EVPN will not program EVPN-received ARP entries if the receiving VPRN has no IP addresses for the same subnet. It will retry to add the ARP entry periodically until an IP address for the same subnet is added.

Note that static ARP entries have precedence over dynamic and EVPN ARP entries.

- VPRN interface binding to VPLS service will bring down the VPRN interface operational status, if the VPRN interface mac or the VRRP mac matches a static-mac or OAM mac configured in the associated VPLS service. If that is the case, a trap will be generated.
- Redundancy will be handled by VRRP. The 7750 master will advertise vMAC and vIP, as discussed, including the mac mobility extended community and the sticky bit.
Interaction of EVPN and VXLAN with Existing VPLS Features

When trying to enable existing VPLS features in an EVPN-VXLAN enabled service, the following must be taken into consideration:

- I-VPLS/B-VPLS services are not supported. `bgp-evpn` or VXLAN cannot be enabled on those services.
- In general, no 7x50-generated control packets will be sent to the VXLAN auto-bindings, except for ARP, VRRP, ping, and BFD.
- `eth-cfm` (meps, vmeps, mips): This command can be configured and used in an EVPN-VXLAN VPLS service objects (service, saps and sdp-bindings). Although `vmeps` can be configured and used for tests to the WAN, `eth-cfm` tests will not work through VXLAN. This behavior is expected since no `eth-cfm` is supported in the DC and `eth-cfm` flooding to the DC NVEs is definitively not desired.
- xSTP and M-VPLS services:
  - xSTP can be configured in `bgp-evpn` services. BPDUs will not be sent over the VXLAN bindings.
  - `bgp-evpn` is blocked in m-vpls services, however, a different m-vpls service can manage a `sap/spoke-sdp` in a `bgp-evpn` enabled service.
- `mac-move`: in `bgp-evpn` enabled VPLS services, `mac-move` can be used in `saps/sdp-bindings`, however the macs being learned through BGP-EVPN will not be considered.
  
  **Note:** The mac duplication already provides a protection against `mac-moves` between EVPN and `saps/sdp-bindings`.
- `disable-learning` and other fdb-related tools: they will only work for data plane learnted mac addresses.
- `mac-protect`: `mac-protect` cannot be used in conjunction with EVPN and VXLAN.
  
  **Note:** EVPN provides its own protection mechanism for static mac addresses.
- `provider-tunnel`: p2mp RSVP/mLDP LSPs are not supported in the `bgp-evpn` service. The configuration of the `provider-tunnel` is blocked.
- MAC OAM: any MAC OAM tool is blocked for `bgp-evpn` services, that is: `mac-ping`, `mac-trace`, `mac-populate`, and `mac-purge`.
- `igmp-snooping`: no igmp report is considered to build a flood list for a given multicast group when received from the VXLAN side. No igmp message is sent to the VXLAN bindings.
Interaction of EVPN and VXLAN with Existing VPLS Features
Configuring a EVPN Service with CLI

This section provides information to configure VPLS using the command line interface.

Topics in this section include:

• EVPN Configuration Examples on page 522
EVPN Configuration Examples

This section shows a configuration example for three 7x50 PEs in a Data Center, given the following assumptions:

- PE-1 is a Data Center Network Virtualization Edge device (NVE) where service VPLS 2000 is configured.
- PE-2 and PE-3 are redundant Data Center Gateways providing layer-2 connectivity to the WAN for service VPLS 2000

DC PE-1 configuration for service VPLS 2000

```
service vpls 2000 customer 1 create
vxlans vni 2000 create
  bgp
    route-target 65000:2000
    route-distinguisher 65010:2000
  bgp-evpn
    no shutdown
  vxlan
    no shutdown
```

DC PE-2 and PE-3 configuration with SAPs at the WAN side (advertisement of all macs and unknown-mac-route):

```
service vpls 2000 customer 1 create
vxlans vni 2000 create
  bgp
    route-target 65000:2000
    route-distinguisher 65001:2000
  bgp-evpn
    mac-advertisement
    unknown-mac-route
  vxlan
    no shutdown
  site site-1 create
    sap 1/1/1:1
    no shutdown
  site-id 1
  sap 1/1/1:1 create
```

DC PE-2 and PE-3 configuration with BGP-AD spoke-sdps at the WAN side (mac-advertisement disable, only unknown-mac-route advertised):

```
service vpls 2000 customer 1 create
vxlans vni 2000 create
  bgp
    pw-template-binding 1 split-horizon-group “to-WAN” import-rt target:65000:2500
    vsls-export “export-policy-1” #policy exporting the WAN and DC RTs
    vsls-import “import-policy-1” #policy importing the WAN and DC RTs
    route-distinguisher 65001:2000
  bgp-ad
    no shutdown
```
vpls-id 65000:2000
bgp-evpn
  mac-advertisement disable
  unknown-mac-route
  vxlan
  no shutdown
site site-1 create
  split-horizon-group “to-WAN”
  no shutdown
  site-id 1
EVPN Command Reference

Command Hierarchies

```
config
  — service
    — vpls service-id [customer customer-id] [vpn vpn-id] [m-vpls] [b-vpls] [i-vpls] [create]
    — no vpls service-id
  — bgp
    — route-distinguisher [ip-addr:comm-val | as-number:ext-comm-val]
    — no route-distinguisher
    — route-target [ext-community | [{export ext-community} [import ext-community]]]
    — no route-target
    — vlsi-export policy-name [policy-name...(up to 5 max)]
    — no vlsi-export
    — vlsi-import policy-name [policy-name...(up to 5 max)]
    — no vlsi-import
  — bgp-evpn
    — [no] mac-advertisement
    — mac-duplication
      — detect num-moves num-moves window minutes
      — [no] retry minutes
    — [no] unknown-mac-route
    — vxlan
    — [no] shutdown
  — static-mac
    — mac ieee-address [create] sap sap-id [monitor fwd-status]
    — mac ieee-address [create] spoke-sdp sdp-id:vc-id [monitor fwd-status]
    — no mac ieee-address
  — vxlans vni vni-id create
  — no vxlan vni
```
EVPN Command Reference

Show Commands

  show
    — service
      — id service-id
        — bgp-evpn
        — proxy-arp
        — vxlan
      — vxlan [vtep]

Debug Commands

  tools
    — dump
      — service
        — id service-id
          — vxlan [clear]
        — vxlan [vtep]
          — usage
          — dup-vtep-evpn [clear]
EVPN Commands

vpls

Syntax

```plaintext
vpls service-id customer customer-id vpn vpn-id [m-vpls] [bvpls | i-vpls] [create]
no vpls service-id
```

Context

```
config>service
```

Description

This command creates or edits a Virtual Private LAN Services (VPLS) instance. The `vpls` command is used to create or maintain a VPLS service. If the `service-id` does not exist, a context for the service is created. If the `service-id` exists, the context for editing the service is entered.

A VPLS service connects multiple customer sites together acting like a zero-hop, Layer 2 switched domain. A VPLS is always a logical full mesh.

When a service is created, the `create` keyword must be specified if the `create` command is enabled in the environment context. When a service is created, the `customer` keyword and customer-id must be specified and associates the service with a customer. The `customer-id` must already exist having been created using the `customer` command in the service context. Once a service has been created with a customer association, it is not possible to edit the customer association. The service must be deleted and recreated with a new customer association.

Once a service is created, the use of the `customer` `customer-id` is optional for navigating into the service configuration context. Attempting to edit a service with the incorrect `customer-id` specified will result in an error.

More than one VPLS service may be created for a single customer ID.

By default, no VPLS instances exist until they are explicitly created.

The `no` form of this command deletes the VPLS service instance with the specified `service-id`. The service cannot be deleted until all SAPs and SDPs defined within the service ID have been shutdown and deleted, and the service has been shutdown.

Parameters

- `service-id` — The unique service identification number or string identifying the service in the service domain. This ID must be unique to this service and may not be used for any other service of any type. The `service-id` must be the same number used for every router on which this service is defined.
  
  **Values**
  
  - `service-id`: 1 — 2147483648
  
  - `svc-name`: 64 characters maximum

- `customer customer-id` — Specifies the customer ID number to be associated with the service. This parameter is required on service creation and optional for service editing or deleting.
  
  **Values**
  
  - 1 — 2147483647

- `vpn vpn-id` — Specifies the VPN ID number which allows you to identify virtual private networks (VPNs) by a VPN identification number.
  
  **Values**
  
  - 1 — 2147483647

  **Default**

  `null (0)`
EVPN Commands

**m-vpls** — Specifies a management VPLS.

**b-vpls | i-vpls** — Creates a backbone-vpls or ISID-vpls.

**bgp**

**Syntax**

```plaintext
bgp
```

**Context**

```plaintext
config>service>vpls
```

**Description**

This command enables the context to configure the BGP related parameters for BGP AD, BGP VPLS and EVPN.

**route-target**

**Syntax**

```plaintext
route-target {ext-community[export ext-community][import ext-community]}
```

**no route-target**

**Context**

```plaintext
config>service>vpls>bgp-ad
config>service>vpls>bgp
```

**Description**

This command configures the route target (RT) component that will be signaled in the related MP-BGP attribute to be used for BGP auto-discovery, BGP VPLS, BGP Multi-Homing and EVPN if these features are configured in this VPLS service.

If this command is not used, the RT is built automatically using the VPLS ID. The ext-comm can have the same two formats as the VPLS ID, a two-octet AS-specific extended community, IPv4 specific extended community.

**Parameters**

- **export ext-community** — Specify communities allowed to be sent to remote PE neighbors.
- **import ext-community** — Specify communities allowed to be accepted from remote PE neighbors.

**vsi-export**

**Syntax**

```plaintext
vsi-export policy-name [policy-name...(up to 5 max)]
```

**no vsi-export**

**Context**

```plaintext
config>service>vpls>bgp-ad
config>service>vpls>bgp
```

**Description**

This command specifies the name of the VSI export policies to be used for BGP auto-discovery, BGP VPLS and BGP Multi-Homing if these features are configured in this VPLS service. If multiple policy names are configured, the policies are evaluated in the order they are specified. The first policy that matches is applied.

The policy name list is handled by the SNMP agent as a single entity.
vsi-import

Syntax

vsi-import policy-name [policy-name...(up to 5 max)]

no vsi-import

Context

config>service>vpls>bgp-ad>vsi-id
config>service>vpls>bgp

Description

This command specifies the name of the VSI import policies to be used for BGP auto-discovery, BGP VPLS and BGP Multi-Homing if these features are configured in this VPLS service. If multiple policy names are configured, the policies are evaluated in the order they are specified. The first policy that matches is applied.

The policy name list is handled by the SNMP agent as a single entity.

route-distinguisher

Syntax

route-distinguisher [ip-addr:comm-val | as-number:ext-comm-val]

no route-distinguisher

Context

config>service>vpls>bgp-ad>vsi-id
config>service>vpls>bgp

Description

This command configures the Route Distinguisher (RD) component that will be signaled in the MP-BGP NLRI for L2VPN AFI. This value will be used for BGP-AD, BGP VPLS and BGP Multi-Homing NLRI if these features are configured.

If this command is not configured, the RD is automatically built using the BGP-AD VPLS ID. The following rules apply:

- if BGP AD VPLS-id is configured & no RD is configured under BGP node - RD = VPLS-ID
- if BGP AD VPLS-id is not configured then an RD value must be configured under BGP node (this is the case when only BGP VPLS is configured)
- if BGP AD VPLS-id is configured and an RD value is also configured under BGP node, the configured RD value prevails

Values and format (6 bytes, other 2 bytes of type will be automatically generated)

Parameters

ip-addr:comm-val — Specifies the IP address.

Values

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-addr</td>
<td>a.b.c.d</td>
</tr>
<tr>
<td>comm-val</td>
<td>0 — 65535</td>
</tr>
</tbody>
</table>

as-number:ext-comm-val — Specifies the AS number and the

Values

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>as-number</td>
<td>1 — 65535</td>
</tr>
<tr>
<td>ext-comm-val</td>
<td>0 — 4294967295</td>
</tr>
</tbody>
</table>
EVPN Commands

vsi-import

Syntax  
```plaintext
vsi-import  policy-name  [policy-name...(up to 5 max)]

no vsi-import
```

Context  
```
config>service>vpls>bgp-ad>vsi-id
config>service>vpls:bgp
```

Description  
This command specifies the name of the VSI import policies to be used for BGP auto-discovery, BGP VPLS and BGP Multi-Homing if these features are configured in this VPLS service. If multiple policy names are configured, the policies are evaluated in the order they are specified. The first policy that matches is applied.

The policy name list is handled by the SNMP agent as a single entity.

Syntax  
```plaintext
bgp-evpn

[no] bgp-evpn
```

Context  
```
config>service>vpls
```

Description  
This command enables the context to configure the BGP EVPN parameters.

bgp-evpn

Syntax  
```plaintext
[no] bgp-evpn
```

Context  
```
config>service>vpls
```

Description  
This command enables the context to configure the BGP EVPN parameters.

mac-advertisement

Syntax  
```plaintext
[no] mac-advertisement
```

Context  
```
config>service>vpls:bgp-evpn
```

Description  
The mac-advertisement command enables the advertisement in BGP of the learnt macs on SAPs and SDP bindings. When the mac-advertisement is disabled, the local macs will be withdrawn in BGP.

Default  
mac-advertisement

mac-duplication

Syntax  
```plaintext
mac-duplication
```

Context  
```
config>service>vpls:bgp-evpn
```

Description  
This command enables the context to configure the BGP EVPN mac duplication parameters.
detect

Syntax  
detect num-moves num-moves window minutes

Context  
config>service>vpls>bgp-evpn>mac-duplication

Description  
The mac-duplication feature is always enabled by default. This command modifies the default behavior. mac-duplication monitors the number of moves of a MAC address for a period of time (window).

Default  
num-moves 5 window 3

Parameters  
num-moves — Identifies the number of MAC moves in a VPLS service. The counter is incremented when a given MAC is locally relearned in the FDB or flushed from the FDB due to the reception of a better remote EVPN route for that MAC.

Values  
3..10 minutes

Default  
3 minutes

retry

Syntax  
retry minutes
no retry

Context  
config>service>vpls>bgp-evpn>mac-duplication

Description  
Specifies the timer after which the MAC in hold-down state is automatically flushed and the mac-duplication process starts again. This value is expected to be equal to two times or more than that of window.

If no retry is configured, this implies that, once mac-duplication is detected, mac updates for that mac will be held down till the user intervenes or a network event (that flushes the mac) occurs.

Default  
9 minutes

Parameters  
minutes — Specifies the BGP EVPN MAC duplication retry in minutes.

Values  
2 — 60 minutes

unknown-mac-route

Syntax  
[no] unknown-mac-route

Context  
config>service>vpls>bgp-evpn

Description  
This command enables the advertisement of the unknown-mac-route in BGP. This will be coded in an EVPN mac route where the mac address is zero and the mac address length 48. By using this unknown-mac-route advertisement, the user may decide to optionally turn off the advertisement of MAC addresses learnt from saps and sdp-bindings, hence reducing the control plane overhead and the size of the FDB tables in the data center. All the receiving NVEs supporting this concept will send any unknown-unicast packet to the owner of the unknown-mac-route, as opposed to flooding the
unknown-unicast traffic to all other nodes part of the same VPLS. Note that, although the 7x50 can be configured to generate and advertise the unknown-mac-route, the 7x50 will never honor the unknown-mac-route and will flood to the vpls flood list when an unknown-unicast packet arrives to an ingress sap/sdp-binding.

**Default**
no unknown-mac-route

### vxlan

**Syntax**
- `vxlan vni vni-id create`
- `no vxlan vni`

**Context**
config>service>vpls

**Description**
This command enables the use of vxlan in the VPLS service.

**Parameters**
- `vni vni-id` — Specifies the VXLAN network identifier configured in the VPLS service. All the EVPN advertisements (MAC routes and inclusive multicast routes) for this services will encode the configured vni in the Ethernet Tag field of the NLRI.

**Values**
1 — 16777215

Note that the VPLS service will be operationally UP once the `vxlan vni vni-id` is successfully created. However, **bgp-evpn** must be enabled so that VXLAN bindings can be established and MAC learning and flooding can happen on them.

### vxlan

**Syntax**
- `vxlan`

**Context**
config>service>vpls>bgp-evpn

**Description**
This command enables the context to configure the VXLAN parameters when BGP EVPN is used as the control plane.

### shutdown

**Syntax**
- `[no] shutdown`

**Context**
config>service>vpls>bgp-evpn.vxlan

**Description**
This command enables/disables the automatic creation of VXLAN auto-bindings by BGP-EVPN.

**Default**
shutdown
static-mac

**Syntax**

```
static-mac
```

**Context**

```
config>service>vpls
```

**Description**

A set of conditional static MAC addresses can be created within a VPLS supporting bgp-evpn. Conditional static macs are also supported in B-VPLS with SPBM. Conditional Static MACs are dependent on the SAP/SDP state.

This command allows assignment of a set of conditional static MAC addresses to a SAP/ spoke-SDP. In the FDB, the static MAC is then associated with the active SAP or spoke SDP.

Static MACs are used for PBB Epipe and I-VPLS services that may terminate external to SPBM. If this is configured under a Control B-VPLS the interface referenced will not use IS-IS for this neighbor. This may also be configured under a User B-VPLS where the corresponding interface is not supported under the Control B-VPLS.

Static MACs configured in a bgp-evpn service are advertised as protected (EVPN will signal the mac as protected).

---

**mac**

**Syntax**

```
mac ieee-address [create] sap sap-id [monitor fwd-status]  
mac ieee-address [create] spoke-sdp sdp-id:vc-id [monitor fwd-status]  
no mac ieee-address
```

**Context**

```
config>service>vpls>static-mac
```

**Description**

This command assigns a conditional static MAC address entry to an SPBM B-VPLS SAP/spoke-SDP allowing external MACs for single and multi-homed operation.

Static MACs are used for PBB Epipe and I-VPLS services that may terminate external to SPBM. If this is configured under a Control B-VPLS the interface referenced will not use IS-IS for this neighbor. This may also be configured under a User B-VPLS where the corresponding interface is not supported under the Control B-VPLS.

**Default**

```
none
```

**Parameters**

```
ieee-address — Specifies the static MAC address to an SPBM/sdp-binding interface.  
```

**Values**


```
create — This keyword is mandatory while creating a static MAC.  
```

```
monitor fwd-status — Specifies that this static mac is based on the forwarding status of the SAP or spoke SDP for multi-homed operation. Monitoring is optional but is required for multi-homing.
```
Show Commands

bgp-evpn

Syntax  
bgp-evpn

Context  
show>service>id
show>service

Description  
This command displays the bgp-evpn configured parameters for a given service, including the admin status of vxlan, the configuration for mac-advertisement and unknown-mac-route as well as the mac-duplication parameters. The command shows the duplicate mac addresses that mac-duplication has detected.

Sample Output

*A:DutA# show service id 1 bgp-evpn

===============================================================================
BGP EVPN Table
===============================================================================
MAC Advertisement : Enabled            Unknown MAC Route : Disabled
VXLAN Admin Status : Enabled            Creation Origin : manual
MAC Dup Detn Moves : 5                  MAC Dup Detn Window : 3
MAC Dup Detn Retry : 9                  Number of Dup MACs : 1
-------------------------------------------------------------------------------
Detected Duplicate MAC Addresses             Time Detected
-------------------------------------------------------------------------------
00:12:12:12:12:00                            01/17/2014 16:01:02
-------------------------------------------------------------------------------
===============================================================================

proxy-arp

Syntax  
proxy-arp

Context  
show>service>id

Description  
This command displays the proxy-ARP entries existing for a particular service. This table is populated by the EVPN mac routes containing a MAC and an IP address. A 7x50 receiving an ARP request from a SAP or SDP-binding will perform a lookup in the proxy-arp table for the service. If the 7x50 finds a match, it will reply to the ARP and will not let the ARP be flooded in the VPLS service. If the 7x50 does not find a match, the ARP will be flooded within the service. The command allows for an specific IP addresses to be shown.

Sample Output

*A:DutA# show service id 1 proxy-arp

===============================================================================
VPLS Proxy Arp Table
===============================================================================

Page 534

7950 SR OS Services Guide
vxlan

Syntax
vxlan

Context
show>service>id
show>service

Description
This command displays the VXLAN bindings auto-created in a given service. A VXLAN binding is composed of the remote VTEP (VXLAN Termination Endpoint) and the corresponding egress VNI (VXLAN Network Identifier) to identify the service at the egress node. The command shows the number of MACs associated to each binding as well as the operational status and if the binding is part of the multicast list. The binding will be operationally down when the VTEP address is not found in the base routing table (the VTEP address can’t be reached). A binding will be part of the multicast list if a valid BGP EVPN inclusive multicast route exists for it.

Sample Output

*A:DutA# show service id 1 vxlan

VPLS VXLAN, Ingress VXLAN Network Id: 1

Egress VTEP, VNI

<table>
<thead>
<tr>
<th>VTEP Address</th>
<th>Egress VNI</th>
<th>Num. MACs</th>
<th>In Mcast List?</th>
<th>Oper State</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.0.0.71</td>
<td>1</td>
<td>1</td>
<td>Yes</td>
<td>Up</td>
</tr>
<tr>
<td>192.0.0.72</td>
<td>1</td>
<td>0</td>
<td>Yes</td>
<td>Up</td>
</tr>
<tr>
<td>192.0.0.74</td>
<td>1</td>
<td>0</td>
<td>Yes</td>
<td>Up</td>
</tr>
<tr>
<td>192.0.0.76</td>
<td>1</td>
<td>1</td>
<td>Yes</td>
<td>Down</td>
</tr>
<tr>
<td>192.168.45.2</td>
<td>1</td>
<td>0</td>
<td>Yes</td>
<td>Down</td>
</tr>
</tbody>
</table>

Number of Egress VTEP, VNI : 5

A:DutB#

A:DutB# show service vxlan <vtep> 192.0.2.65 192.0.2.66
A:PE63# show service vxlan 192.0.2.65

VXLAN Tunnel Endpoint: 192.0.2.65

Egress VNI  Service Id  Oper State
Debug Commands

service

Syntax service
Context tools>dump
Description Use this command to configure tools to display service dump information.

id

Syntax id service-id
Context tools>dump
Description Use this command to configure parameters to display service ID information.

vxlan

Syntax vxlan [clear]
Context tools>dump>service>id
Description This command displays the number of times a service could not add a VXLAN binding or <VTEP, Egress VNI> due to the following limits:

- The per System VTEP limit has been reached
- The per System <VTEP, Egress VNI> limit has been reached
- The per Service <VTEP, Egress VNI> limit has been reached
- The per System Bind limit: Total bind limit or vxlan bind limit has been reached.

The command adds a clear option to clear the above statistics.

Sample Output

*A:PE63# tools dump service id 3 vxlan
VTEP, Egress VNI Failure statistics at 000 00:03:55.710:
statistics last cleared at 000 00:00:00.000:

<table>
<thead>
<tr>
<th>Statistic</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>VTEP</td>
<td>0</td>
</tr>
<tr>
<td>Service Limit</td>
<td>0</td>
</tr>
<tr>
<td>System Limit</td>
<td>0</td>
</tr>
<tr>
<td>Egress Mcast List Limit</td>
<td>0</td>
</tr>
<tr>
<td>Duplicate VTEP, Egress VNI</td>
<td>1</td>
</tr>
</tbody>
</table>
usage

Syntax usage
Context tools>dump>service>vxlan
Description This command displays the consumed VXLAN resources in the system.

Sample Output

*A:PE71# tools dump service vxlan usage
VXLAN usage statistics at 001 17:46:11.170:

VTEP : 5/8191
VTEP, Egress VNI : 5/131071
Sdp Bind + VTEP, Egress VNI : 13/196607
RVPLS Egress VNI : 0/40959

dup-vtep-egrvni

Syntax dup-vtep-egrvni [clear]
Context tools>dump>service>vxlan
Description This command dumps the <VTEP, VNI> bindings that have been detected as duplicate attempts, i.e. an attempt to add the same binding to more than one service. The commands provides a clear option.

Sample Output

*A:PE71# tools dump service vxlan dup-vtep-egrvni
Duplicate VTEP, Egress VNI usage attempts at 000 00:03:41.570:
1. 10.1.1.1:100
Virtual Private LAN Service

In This Chapter

This chapter provides information about Virtual Private LAN Service (VPLS), process overview, and implementation notes.

Topics in this chapter include:

- VPLS Service Overview on page 541
- VPLS Features on page 545
  - VPLS Packet Walkthrough on page 542
  - VPLS Enhancements on page 545
  - VPLS over MPLS on page 546
  - VPLS MAC Learning and Packet Forwarding on page 547
  - Pseudowire Control Word on page 551
  - Table Management on page 552
  - VPLS and Spanning Tree Protocol on page 561
  - Multiple Spanning Tree on page 563
  - Egress Multicast Groups on page 570
  - VPLS Redundancy on page 581
  - Object Grouping and State Monitoring on page 599
  - MAC Flush Message Processing on page 601
  - ACL Next-Hop for VPLS on page 605
  - SDP Statistics for VPLS and VLL Services on page 606
  - BGP Auto-Discovery for LDP VPLS on page 607
  - Multicast-Aware VPLS on page 625
  - RSVP and LDP P2MP LSP for Forwarding VPLS/B-VPLS BUM and IP Multicast Packets on page 629
• VPLS Service Considerations on page 638
  → SAP Encapsulations on page 638
• Ingress VLAN Swapping on page 639
VPLS Service Overview

Virtual Private LAN Service (VPLS) as described in RFC 4905, *Encapsulation methods for transport of layer 2 frames over MPLS*, is a class of virtual private network service that allows the connection of multiple sites in a single bridged domain over a provider-managed IP/MPLS network. The customer sites in a VPLS instance appear to be on the same LAN, regardless of their location. VPLS uses an Ethernet interface on the customer-facing (access) side which simplifies the LAN/WAN boundary and allows for rapid and flexible service provisioning.

VPLS offers a balance between point-to-point Frame Relay service and outsourced routed services. VPLS enables each customer to maintain control of their own routing strategies. All customer routers in the VPLS service are part of the same subnet (LAN) which simplifies the IP addressing plan, especially when compared to a mesh constructed from many separate point-to-point connections. The VPLS service management is simplified since the service is not aware of nor participates in the IP addressing and routing.

A VPLS service provides connectivity between two or more SAPs on one (which is considered a local service) or more (which is considered a distributed service) service routers. The connection appears to be a bridged domain to the customer sites so protocols, including routing protocols, can traverse the VPLS service.

Other VPLS advantages include:

- VPLS is a transparent, protocol-independent service.
- There is no Layer 2 protocol conversion between LAN and WAN technologies.
- There is no need to design, manage, configure, and maintain separate WAN access equipment, thus, eliminating the need to train personnel on WAN technologies such as Frame Relay.
VPLS Packet Walkthrough

This section provides an example of VPLS processing of a customer packet sent across the network (Figure 76) from site-A, which is connected to PE-Router-A, to site-B, which is connected to PE-Router-C (Figure 77).

![Figure 76: VPLS Service Architecture](image)

1. PE-Router-A (Figure 77)
   a. Service packets arriving at PE-Router-A are associated with a VPLS service instance based on the combination of the physical port and the IEEE 802.1Q tag (VLAN-ID) in the packet.

![Figure 77: Access Port Ingress Packet Format and Lookup](image)
b. PE-Router-A learns the source MAC address in the packet and creates an entry in the FIB table that associates the MAC address to the service access point (SAP) on which it was received.

c. The destination MAC address in the packet is looked up in the FIB table for the VPLS instance. There are two possibilities: either the destination MAC address has already been learned (known MAC address) or the destination MAC address is not yet learned (unknown MAC address).

For a Known MAC Address (Figure 78):

d. If the destination MAC address has already been learned by PE-Router-A, an existing entry in the FIB table identifies the far-end PE-router and the service VC-label (inner label) to be used before sending the packet to far-end PE-Router-C.

e. PE-Router-A chooses a transport LSP to send the customer packets to PE-Router-C. The customer packet is sent on this LSP once the IEEE 802.1Q tag is stripped and the service VC-label (inner label) and the transport label (outer label) are added to the packet.

For an Unknown MAC Address (Figure 78):

If the destination MAC address has not been learned, PE-Router-A will flood the packet to both PE-Router-B and PE-Router-C that are participating in the service by using the VC-labels that each PE-Router previously signaled for the VPLS instance. Note that the packet is not sent to PE-Router-D since this VPLS service does not exist on that PE-router.
2. Core Router Switching
   a. All the core routers ('P' routers in IETF nomenclature) between PE-Router-A and PE-Router-B and PE-Router-C are Label Switch Routers (LSRs) that switch the packet based on the transport (outer) label of the packet until the packet arrives at far-end PE-Router. All core routers are unaware that this traffic is associated with a VPLS service.

3. PE-Router-C
   a. PE-Router-C strips the transport label of the received packet to reveal the inner VC-label. The VC-label identifies the VPLS service instance to which the packet belongs.
   b. PE-Router-C learns the source MAC address in the packet and creates an entry in the FIB table that associates the MAC address to PE-Router-A and the VC-label that PE-Router-A signaled it for the VPLS service on which the packet was received.
   c. The destination MAC address in the packet is looked up in the FIB table for the VPLS instance. Again, there are two possibilities: either the destination MAC address has already been learned (known MAC address) or the destination MAC address has not been learned on the access side of PE-Router-C (unknown MAC address).
      **Known MAC address** (Figure 79)
   d. If the destination MAC address has been learned by PE-Router-C, an existing entry in the FIB table identifies the local access port and the IEEE 802.1Q tag to be added before sending the packet to customer Location-C. The egress Q tag may be different than the ingress Q tag.

![Figure 79: Access Port Egress Packet Format and Lookup](image-url)
VPLS Features

This section features:

- VPLS Enhancements on page 545
- Pseudowire Control Word on page 551
- Split Horizon SAP Groups and Split Horizon Spoke SDP Groups on page 560
- VPLS and Spanning Tree Protocol on page 561
- VPLS Redundancy on page 581
- VPLS Access Redundancy on page 597

VPLS Enhancements

Alcatel-Lucent’s VPLS implementation includes several enhancements beyond basic VPN connectivity. The following VPLS features can be configured individually for each VPLS service instance:

- Extensive MAC and IP filter support (up to Layer 4). Filters can be applied on a per SAP basis.
- Forwarding Information Base (FIB) management features on a per service level including:
  - Configurable FIB size limit
  - FIB size alarms
  - MAC learning disable
  - Discard unknown
  - Separate aging timers for locally and remotely learned MAC addresses.
- Ingress rate limiting for broadcast, multicast, and destination unknown flooding on a per SAP basis.
- Implementation of Spanning Tree Protocol (STP) parameters on a per VPLS, per SAP and per spoke SDP basis.
- A split horizon group on a per-SAP and per-spoke SDP basis.
- IGMP snooping on a per-SAP and per-SDP basis.
- Optional SAP and/or spoke SDP redundancy to protect against node failure.
VPLS Features

VPLS over MPLS

The VPLS architecture proposed in RFC 4762, *Virtual Private LAN Services Using LDP Signalling* specifies the use of provider equipment (PE) that is capable of learning, bridging, and replication on a per-VPLS basis. The PE routers that participate in the service are connected using MPLS Label Switched Path (LSP) tunnels in a full-mesh composed of mesh SDPs or based on an LSP hierarchy (Hierarchical VPLS (H-VPLS)) composed of mesh SDPs and spoke SDPs.

Multiple VPLS services can be offered over the same set of LSP tunnels. Signaling specified in RFC 4905, *Encapsulation methods for transport of layer 2 frames over MPLS* is used to negotiate a set of ingress and egress VC labels on a per-service basis. The VC labels are used by the PE routers for de-multiplexing traffic arriving from different VPLS services over the same set of LSP tunnels.

VPLS is provided over MPLS by:

- Connecting bridging-capable provider edge routers with a full mesh of MPLS LSP (label switched path) tunnels.
- Negotiating per-service VC labels using *draft-Martini* encapsulation.
- Replicating unknown and broadcast traffic in a service domain.
- Enabling MAC learning over tunnel and access ports (see *VPLS MAC Learning and Packet Forwarding*).
- Using a separate forwarding information base (FIB) per VPLS service.
VPLS MAC Learning and Packet Forwarding

The SR-OS edge devices perform the packet replication required for broadcast and multicast traffic across the bridged domain. MAC address learning is performed by the to reduce the amount of unknown destination MAC address flooding.

SR-OS routers learn the source MAC addresses of the traffic arriving on their access and network ports.

Each SR-OS maintains a Forwarding Information Base (FIB) for each VPLS service instance and learned MAC addresses are populated in the FIB table of the service. All traffic is switched based on MAC addresses and forwarded between all participating nodes using the LSP tunnels. Unknown destination packets (for example, the destination MAC address has not been learned) are forwarded on all LSPs to all participating nodes for that service until the target station responds and the MAC address is learned by the routers associated with that service.

MAC Learning Protection

In a Layer 2 environment, customers connected to SAPs A, B, C can create a denial of service attack by sending packets sourcing the gateway MAC address. This will move the learned gateway MAC from the uplink SDP/SAP to the customer’s SAP causing all communication to the gateway to be disrupted. If local content is attached to the same VPLS (D), a similar attack can be launched against it. Communication between customers is also disallowed but split-horizon will not be sufficient in the topology depicted in Figure 80.
SR-OSs enable MAC learning protection capability for SAPs and SDPs. With this mechanism, forwarding and learning rules apply to the non-protected SAPs. Assume hosts H1, H2 and H3 (Figure 80) are non-protected while IES interfaces G and H are protected. When a frame arrives at a protected SAP/SDP the MAC is learned as usual. When a frame arrives from a non-protected SAP or SDP the frame must be dropped if the source MAC address is protected and the MAC address is not relearned. The system allows only packets with a protected MAC destination address.

The system can be configured statically. The addresses of all protected MACs are configured. Only the IP address can be included and use a dynamic mechanism to resolve the MAC address (cpe-ping). All protected MACs in all VPLS instances in the network must be configured.

In order to eliminate the ability of a customer to cause a DOS attack, the node restricts the learning of protected MAC addresses based on a statically defined list. In addition the destination MAC address is checked against the protected MAC list to verify that a packet entering a restricted SAP has a protected MAC as a destination.

Figure 80: MAC Learning Protection
**DEI in IEEE 802.1ad**

IEEE 802.1ad-2005 standard allows drop eligibility to be conveyed separately from priority in Service VLAN TAGs (STAGs) so that all of the previously introduced traffic types can be marked as drop eligible. The Service VLAN TAG has a new format where the priority and discard eligibility parameters are conveyed in the three bit Priority Code Point (PCP) field and respectively in the DE Bit (Figure 81).

![Figure 81: DE Bit in the 802.1ad S-TAG](image)

The DE bit allows the S-TAG to convey eight forwarding classes/distinct emission priorities, each with a drop eligible indication.

When DE bit is set to 0 (DE=FALSE), the related packet is **not** discard eligible. This is the case for the packets that are within the CIR limits and must be given priority in case of congestion. If the DEI is not used or backwards compliance is required the DE bit should be set to zero on transmission and ignored on reception.

When the DE bit is set to 1 (DE=TRUE), the related packet is discard eligible. This is the case for the packets that are sent above the CIR limit (but below the PIR). In case of congestion these packets will be the first ones to be dropped.
VPLS Using G.8031 Protected Ethernet Tunnels

The use of MPLS tunnels provides a way to scale the core while offering fast failover times using MPLS FRR. In environments where Ethernet services are deployed using native Ethernet backbones Ethernet tunnels are provided to achieve the same fast failover times as in the MPLS FRR case. There are still service provider environments where Ethernet services are deployed using native Ethernet backbones.

The Alcatel-Lucent VPLS implementation offers the capability to use core Ethernet tunnels compliant with ITU-T G.8031 specification to achieve 50 ms resiliency for backbone failures. This is required to comply with the stringent SLAs provided by service providers in the current competitive environment. The implementation also allows a LAG-emulating Ethernet Tunnel providing a complimentary native Ethernet ELAN capability. The LAG-emulating Ethernet tunnels and G.8031 protected Ethernet tunnels operate independently. (refer to LAG emulation using Ethernet Tunnels)

When using Ethernet Tunnels, the Ethernet Tunnel logical interface is created first. The Ethernet tunnel has member ports which are the physical ports supporting the links. The Ethernet tunnel control SAPs carries G.8031 and 802.1ag control traffic and user data traffic. Ethernet Service SAPs are configured on the Ethernet tunnel. Optionally when tunnels follow the same paths end to end services may be configured with, Same-fate Ethernet tunnel SAPs which carry only user data traffic and shares the fate of the Ethernet tunnel port (if properly configured).

When configuring VPLS and BVPLS using Ethernet tunnels the services are very similar.
Pseudowire Control Word

The control word command enables the use of the control word individually on each mesh SDP or spoke sdp. By default, the control word is disabled. When the control word is enabled, all VPLS packets, including the BPDU frames are encapsulated with the control word. The T-LDP control plane behavior will be the same as the control word for VLL services. The configuration for the two directions of the Ethernet pseudowire should match.
Table Management

The following sections describe VPLS features related to management of the Forwarding Information Base (FIB).

FIB Size

The following MAC table management features are required for each instance of a SAP or spoke SDP within a particular VPLS service instance:

- MAC FIB size limits — Allows users to specify the maximum number of MAC FIB entries that are learned locally for a SAP or remotely for a spoke SDP. If the configured limit is reached, then no new addresses will be learned from the SAP or spoke SDP until at least one FIB entry is aged out or cleared.
  → When the limit is reached on a SAP or spoke SDP, packets with unknown source MAC addresses are still forwarded (this default behavior can be changed by configuration). By default, if the destination MAC address is known, it is forwarded based on the FIB, and if the destination MAC address is unknown, it will be flooded. Alternatively, if discard unknown is enabled at the VPLS service level, any packets from unknown source MAC addresses are discarded at the SAP.
  → The log event SAP MAC limit reached is generated when the limit is reached. When the condition is cleared, the log event SAP MAC Limit Reached Condition Cleared is generated.
  → Disable learning allows users to disable the dynamic learning function on a SAP or a spoke SDP of a VPLS service instance.
  → Disable aging allows users to turn off aging for learned MAC addresses on a SAP or a spoke SDP of a VPLS service instance.

FIB Size Alarms

The size of the VPLS FIB can be configured with a low watermark and a high watermark, expressed as a percentage of the total FIB size limit. If the actual FIB size grows above the configured high watermark percentage, an alarm is generated. If the FIB size falls below the configured low watermark percentage, the alarm is cleared by the system.
Local and Remote Aging Timers

Like a Layer 2 switch, learned MACs within a VPLS instance can be aged out if no packets are sourced from the MAC address for a specified period of time (the aging time). In each VPLS service instance, there are independent aging timers for locally learned MAC and remotely learned MAC entries in the forwarding database (FIB). A local MAC address is a MAC address associated with a SAP because it ingressed on a SAP. A remote MAC address is a MAC address received by an SDP from another router for the VPLS instance. The local-age timer for the VPLS instance specifies the aging time for locally learned MAC addresses, and the remote-age timer specifies the aging time for remotely learned MAC addresses.

In general, the remote-age timer is set to a longer period than the local-age timer to reduce the amount of flooding required for destination unknown MAC addresses. The aging mechanism is considered a low priority process. In most situations, the aging out of MAC addresses can happen in within tens of seconds beyond the age time. To minimize overhead, local MAC addresses on a LAG port and remote MAC addresses, in some circumstances, can take up to two times their respective age timer to be aged out.

Disable MAC Aging

The MAC aging timers can be disabled which will prevent any learned MAC entries from being aged out of the FIB. When aging is disabled, it is still possible to manually delete or flush learned MAC entries. Aging can be disabled for learned MAC addresses on a SAP or a spoke SDP of a VPLS service instance.

Disable MAC Learning

When MAC learning is disabled for a service, new source MAC addresses are not entered in the VPLS FIB, whether the MAC address is local or remote. MAC learning can be disabled for individual SAPs or spoke SDPs.

Unknown MAC Discard

Unknown MAC discard is a feature which discards all packets ingressing the service where the destination MAC address is not in the FIB. The normal behavior is to flood these packets to all end points in the service.

Unknown MAC discard can be used with the disable MAC learning and disable MAC aging options to create a fixed set of MAC addresses allowed to ingress and traverse the service.
VPLS Features

VPLS and Rate Limiting

Traffic that is normally flooded throughout the VPLS can be rate limited on SAP ingress through the use of service ingress QoS policies. In a service ingress QoS policy, individual queues can be defined per forwarding class to provide shaping of broadcast traffic, MAC multicast traffic and unknown destination MAC traffic.

MAC Move

The MAC move feature is useful to protect against undetected loops in a VPLS topology as well as the presence of duplicate MACs in a VPLS service.

If two clients in the VPLS have the same MAC address, the VPLS will experience a high re-learn rate for the MAC. When MAC move is enabled, the SR-OS will shut down the SAP or spoke SDP and create an alarm event when the threshold is exceeded.

MAC move allows sequential order port blocking. By configuration, some VPLS ports can be configured as “non-blockable” which allows simple level of control which ports are being blocked during loop occurrence. There are two sophisticated control mechanisms that allow blocking of ports in a sequential order:

1. Configuration capabilities to group VPLS ports and to define the order they should be blocked.
2. Criteria defining when individual groups should be blocked.

For the first, configuration CLI is extended by definition of “primary” and “secondary” ports. Per default, all VPLS ports are considered “tertiary” ports unless they are explicitly declared primary or secondary. The order of blocking will always follow a strict order starting from “tertiary” to secondary and then primary.

The definition of criteria for the second control mechanism is the number of periods during which the given re-learn rate has been exceeded. The mechanism is based on the “cumulative” factor for every group of ports. Tertiary VPLS ports are blocked if the re-learn rate exceeds the configured threshold during one period while secondary ports are blocked only when re-learn rates are exceeded during two consecutive periods, and so forth. The retry timeout period must be larger than the period before blocking the “highest priority port” so it sufficiently spans across the period required to block all ports in sequence. The period before blocking the “highest priority port” is the cumulative factor of the highest configured port multiplied by 5 seconds (the retry timeout can be configured through the CLI).
Auto-Learn MAC Protect

This section provides information about auto-learn-mac-protect and restrict-protected-src discard-frame features.

VPLS solutions usually involve learning of MAC addresses in order for traffic to be forwarded to the correct SAP/SDP. If a MAC address is learned on the wrong SAP/SDP then traffic would be re-directed away from its intended destination. This could occur through a mis-configuration, a problem in the network or by a malicious source creating a DOS attack and is applicable to any type of VPLS network, for example mobile backhaul or residential service delivery networks. **auto-learn-mac-protect** can be used to safe-guard against the possibility of MAC addresses being learned on the wrong SAP/SDP.

This feature provides the ability to automatically protect source MAC addresses which have been learned on a SAP or a spoke/mesh SDP and prevent frames with the same protected source MAC address from entering into a different SAP/spoke or mesh SDP.

This is a complementary solution to features such as **mac-move** and **mac-pinning**, but has the advantage that MAC moves are not seen and it has a low operational complexity. It should be noted that if a MAC is initially learned on the wrong SAP/SDP, the operator can clear the MAC from the MAC FDB in order for it to be re-learned on the correct SAP/SDP.

Two separate commands are used which provide the configuration flexibility of separating the identification (learning) function from the application of the restriction (discard).

The **auto-learn-mac-protect** and **restrict-protected-src** commands allow the following functions:

- The ability to enable the automatic protection of a learned MAC using the auto-learn-mac-protect command under a SAP/spoke or mesh SDP/SHG contexts.
- The ability to discard frames associated with automatically protected MACs instead of shutting down the entire SAP/SDP as with the restrict-protected-src feature. This is enabled using a restrict-protected-src discard-frame command in the SAP/spoke or mesh SDP/SHG context. An optimized alarm mechanism is used to generate alarms related to these discards. The frequency of alarm generation is fixed to be at most one alarm per MAC address per forwarding complex per 10 minutes in a given VPLS service.

Note, if auto-learn-mac-protect or restrict-protected-src discard-frame is configured under an SHG the operation applies only to SAPs in the SHG not to spoke SDPs in the SHG. If required, these parameters can also be enabled explicitly under specific SAPs/spoke SDPs within the SHG.

Applying or removing auto-learn-mac-protect or restrict-protected-src discard-frame to/from a SAP, spoke or mesh SDP or SHG, will clear the MACs on the related objects (for the SHG, this results in clearing the MACs only on the SAPs within the SHG).
The use of restrict-protected-src discard-frame is mutually exclusive with both the restrict-protected-src [alarm-only] command and with the configuration of manually protected MAC addresses, using the mac-protect command, within a given VPLS.

The following rules govern the changes to the state of protected MACs:

- Automatically learned protected MACs are subject to normal removal, aging (unless disabled) and flushing at which time the associated entries are removed from the FDB.
- Automatically learned protected MACs can only move from their learned SAP/spoke or mesh SDP if they enter a SAP/spoke or mesh SDP without restrict-protected-src enabled.

If a MAC address does legitimately move between SAPs/spoke or mesh SDPs after it has been automatically protected on a given SAP/spoke or mesh SDP (thereby causing discards when received on the new SAP/spoke or mesh SDP), the operator must manually clear the MAC from the FDB for it to be learned in the new/correct location.

MAC addresses that are manually created (using static-mac, static-host with a MAC address specified or oam mac-populate) will not be protected even if they are configured on a SAP/x SDP that has auto-learn-mac-protect enabled on it.

MAC addresses that are dynamically created (learned, using static-host with no MAC address specified or lease-populate) will be protected when the MAC address is “learned” on a SAP/x-SDP that has auto-learn-mac-protect enabled on it.

The actions of the following features are performed in the order listed.

1. Restrict-protected-src
2. MAC-pinning
3. MAC-move

---

**Operation**

Figure 82 shows a specific configuration using **auto-learn-mac-protect** and **restrict-protected-src discard-frame** in order to describe their operation.
A VPLS service is configured with SAP1 and SDP1 connecting to access devices and SAP2, SAP3 and SDP2 connecting to the core of the network. auto-learn-mac-protect is enabled on SAP1, SAP3 and SDP1 and restrict-protected-src discard-frame is enabled on SAP1, SDP1 and SDP2. The following series of events describe the details of the functionality:

Assume that the FDB is empty at the start of each sequence.

Sequence 1:

1. A frame with source MAC A enters SAP1, MAC A is learned on SAP1 and MAC-A/SAP1 is protected because of the presence of the auto-learn-mac-protect on SAP1.
2. All subsequent frames with source MAC A entering SAP1 are forwarded into the VPLS.
3. Frames with source MAC A enter either SDP1 or SDP2, these frames are discarded and an alarm indicating MAC A and SDP1/SDP2 is initiated because of the presence of the restrict-protected-src discard-frame on SDP1/SDP2.
4. The above continues, with MAC-A/SAP1 protected in the FDB until MAC A on SAP1 is removed from the FDB.

Sequence 2:

1. A frame with source MAC A enters SAP1, MAC A is learned on SAP1 and MAC-A/SAP1 is protected because of the presence of the auto-learn-mac-protect on SAP1.
2. A frame with source MAC A enters SAP2. As restrict-protected-src is not enabled on SAP2, MAC A is re-learned on SAP2 (but not protected), replacing the MAC-A/SAP1 entry in the FDB.
3. All subsequent frames with source MAC A entering SAP2 are forwarded into the VPLS. This is because restrict-protected-src is not enabled on SAP2 and auto-learn-mac-protect is not enabled on SAP2, so the FDB would not be changed.

4. A frame with source MAC A enters SAP1, MAC A is re-learned on SAP1 and MAC-A/SAP1 is protected because of the presence of the auto-learn-mac-protect on SAP1.

Sequence 3:

1. A frame with source MAC A enters SDP2, MAC A is learned on SDP2 but is not protected as auto-learn-mac-protect is not enabled on SDP2.

2. A frame with source MAC A enters SDP1, MAC A is re-learned on SDP1 as previously it was not protected. Consequently, MAC-A/SDP1 is protected because of the presence of the auto-learn-mac-protect on SDP1.

Sequence 4:

1. A frame with source MAC A enters SAP1, MAC A is learned on SAP1 and MAC-A/SAP1 is protected because of the presence of the auto-learn-mac-protect on SAP1.

2. A frame with source MAC A enters SAP3. As restrict-protected-src is not enabled on SAP3, MAC A is re-learned on SAP3 and the MAC-A/SAP1 entry is removed from the FDB with MAC-A/SAP3 being added as protected to the FDB (because auto-learn-mac-protect is enabled on SAP3).

3. All subsequent frames with source MAC A entering SAP3 are forwarded into the VPLS.

4. A frame with source MAC A enters SAP1, these frames are discarded and an alarm indicating MAC A and SAP1 is initiated because of the presence of the restrict-protected-src discard-frame on SAP1.
Example Use

Figure 83 shows a possible configuration using auto-learn-mac-protect and restrict-protected-src discard-frame in a mobile backhaul network, with the focus on PE1.

Figure 83: Auto-Learn-Mac-Protect Example

In order to protect the MAC addresses of the BNG/RNCs on PE1, auto-learn-mac-protect is enabled on the pseudo-wires connecting it to PE2 and PE3. Enabling restrict-protected-src discard-frame on the SAPs towards the eNodeBs will prevent frames with the source MAC addresses of the BNG/RNCs from entering PE1 from the eNodeBs.

The MAC addresses of the eNodeBs are protected in two ways. In addition to the above commands, enabling auto-learn-mac-protect on the SAPs towards the eNodeBs will prevent the MAC addresses of the eNodeBs being learned on the wrong eNodeB SAP. Enabling restrict-protected-src discard-frame on the pseudowires connecting PE1 to PE2 and PE3 will protect the eNodeB MAC addresses from being learned on the pseudowires. This may happen if their MAC addresses are incorrectly injected into VPLS 40 on PE2/PE3 from another eNodeB aggregation PE.

The above configuration is equally applicable to other Layer 2 VPLS based aggregation networks, for example to business or residential service networks.
Within the context of VPLS services, a loop-free topology within a fully meshed VPLS core is achieved by applying a split-horizon forwarding concept that packets received from a mesh SDP are never forwarded to other mesh SDPs within the same service. The advantage of this approach is that no protocol is required to detect loops within the VPLS core network.

In applications such as DSL aggregation, it is useful to extend this split-horizon concept also to groups of SAPs and/or spoke SDPs. This extension is referred to as a split horizon SAP group or residential bridging.

Traffic arriving on a SAP or a spoke SDP within a split horizon group will not be copied to other SAPs and spoke SDPs in the same split horizon group (but will be copied to SAPs / spoke SDPs in other split horizon groups if these exist within the same VPLS).
VPLS and Spanning Tree Protocol

Alcatel-Lucent’s VPLS service provides a bridged or switched Ethernet Layer 2 network. Equipment connected to SAPs forward Ethernet packets into the VPLS service. The SR-OS participating in the service learns where the customer MAC addresses reside, on ingress SAPs or ingress SDPs.

Unknown destinations, broadcasts, and multicasts are flooded to all other SAPs in the service. If SAPs are connected together, either through misconfiguration or for redundancy purposes, loops can form and flooded packets can keep flowing through the network. Alcatel-Lucent’s implementation of the Spanning Tree Protocol (STP) is designed to remove these loops from the VPLS topology. This is done by putting one or several SAPs and/or spoke SDPs in the discarding state.

Alcatel-Lucent’s implementation of the Spanning Tree Protocol (STP) incorporates some modifications to make the operational characteristics of VPLS more effective.

The STP instance parameters allow the balancing between resiliency and speed of convergence extremes. Modifying particular parameters can affect the behavior. For information on command usage, descriptions, and CLI syntax, refer to Configuring a VPLS Service with CLI on page 651.

Spanning Tree Operating Modes

Per VPLS instance, a preferred STP variant can be configured. The STP variants supported are:

- **rstp** — Rapid Spanning Tree Protocol (RSTP) compliant with IEEE 802.1D-2004 - default mode
- **dot1w** — Compliant with IEEE 802.1w
- **comp-dot1w** — Operation as in RSTP but backwards compatible with IEEE 802.1w (this mode allows interoperability with some MTU types)
- **mstp** — Compliant with the Multiple Spanning Tree Protocol specified in IEEE 802.1Q-REV/D5.0-09/2005. This mode of operation is only supported in an mVPLS.

While the SR-OS initially uses the mode configured for the VPLS, it will dynamically fall back (on a per-SAP basis) to STP (IEEE 802.1D-1998) based on the detection of a BPDU of a different format. A trap or log entry is generated for every change in spanning tree variant.

Some older 802.1W compliant RSTP implementations may have problems with some of the features added in the 802.1D-2004 standard. Interworking with these older systems is improved with the comp-dot1w mode. The differences between the RSTP mode and the comp-dot1w mode are:
VPLS Features

- The RSTP mode implements the improved convergence over shared media feature, for example, RSTP will transition from discarding to forwarding in 4 seconds when operating over shared media. The comp-dot1w mode does not implement this 802.1D-2004 improvement and transitions conform to 802.1w in 30 seconds (both modes implement fast convergence over point-to-point links).

- In the RSTP mode, the transmitted BPDUs contain the port's designated priority vector (DPV) (conforms to 802.1D-2004). Older implementations may be confused by the DPV in a BPDU and may fail to recognize an agreement BPDU correctly. This would result in a slow transition to a forwarding state (30 seconds). For this reason, in the comp-dot1w mode, these BPDUs contain the port's port priority vector (conforms to 802.1w).

The SR-OS supports two BDPU encapsulation formats, and can dynamically switch between the following supported formats (on a per-SAP basis):

- IEEE 802.1D STP
- Cisco PVST
Multiple Spanning Tree

The Multiple Spanning Tree Protocol (MSTP) extends the concept of the IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) by allowing grouping and associating VLANs to Multiple Spanning Tree Instances (MSTI). Each MSTI can have its own topology, which provides architecture enabling load balancing by providing multiple forwarding paths. At the same time, the number of STP instances running in the network is significantly reduced as compared to Per VLAN STP (PVST) mode of operation. Network fault tolerance is also improved because a failure in one instance (forwarding path) does not affect other instances.

The SR-Series implementation of Management VPLS (mVPLS) is used to group different VPLS instances under single RSTP instance. Introducing MSTP into the mVPLS allows interoperating with traditional Layer 2 switches in access network and provides an effective solution for dual homing of many business Layer 2 VPNs into a provider network.

Redundancy Access to VPLS

The GigE MAN portion of the network is implemented with traditional switches. Using MSTP running on individual switches facilitates redundancy in this part of the network. In order to provide dual homing of all VPLS services accessing from this part of the network, the VPLS PEs must participate in MSTP.

This can be achieved by configuring mVPLS on VPLS-PEs (only PEs directly connected to GigE MAN network) and then assign different managed-vlan ranges to different MSTP instances. Typically, the mVPLS would have SAPs with null encapsulations (to receive, send, and transmit MSTP BPDUs) and a mesh SDP to interconnect a pair of VPLS PEs.

Different access scenarios are displayed in Figure 84 as example network diagrams dually connected to the PBB PEs:

- **Access Type A** — Source devices connected by null or Dot1q SAPs
- **Access Type B** — One QinQ switch connected by QinQ/801ad SAPs
- **Access Type C** — Two or more ES devices connected by QinQ/802.1ad SAPs
The following mechanisms are supported for the I-VPLS:

- **STP/RSTP** can be used for all access types.
- **M-VPLS with MSTP** can be used as is just for access Type A. MSTP is required for access type B and C.
- **LAG and MC-LAG** can be used for access Type A and B.
- **Split-horizon-group** does not require residential.

PBB I-VPLS inherits current STP configurations from the regular VPLS and MVPLS.
**MSTP for QinQ SAPs**

MSTP runs in a MVPLS context and can control SAPs from source VPLS instances. QinQ SAPs are supported. The outer tag is considered by MSTP as part of VLAN range control.

---

**Provider MSTP**

Provider MSTP is specified in (IEEE-802.1ad-2005). It uses a provider bridge group address instead of a regular bridge group address used by STP, RSTP, MSTP BPDUs. This allows for implicit separation of source and provider control planes.

The 802.1ad access network sends PBB PE P-MSTP BPDUs using the specified MAC address and also works over QinQ interfaces. P-MSTP mode is used in PBBN for core resiliency and loop avoidance.

Similar to regular MSTP, the STP mode (for example, PMSTP) is only supported in VPLS services where the m-VPLS flag is configured.
MSTP General Principles

MSTP represents modification of RSTP which allows the grouping of different VLANs into multiple MSTIs. To enable different devices to participate in MSTIs, they must be consistently configured. A collection of interconnected devices that have the same MST configuration (region-name, revision and VLAN-to-instance assignment) comprises an MST region.

There is no limit to the number of regions in the network, but every region can support a maximum of 16 MSTIs. Instance 0 is a special instance for a region, known as the Internal Spanning Tree (IST) instance. All other instances are numbered from 1 to 4094. IST is the only spanning-tree instance that sends and receives BPDUs (typically BPDUs are untagged). All other spanning-tree instance information is included in MSTP records (M-records), which are encapsulated within MSTP BPDUs. This means that single BPDU carries information for multiple MSTI which reduces overhead of the protocol.

Any given MSTI is local to an MSTP region and completely independent from an MSTI in other MST regions. Two redundantly connected MST regions will use only a single path for all traffic flows (no load balancing between MST regions or between MST and SST region).

Traditional Layer 2 switches running MSTP protocol assign all VLANs to the IST instance per default. The operator may then “re-assign” individual VLANs to a given MSTI by configuring per VLAN assignment. This means that a SR-Series PE can be considered as the part of the same MST region only if the VLAN assignment to IST and MSTIs is identical to the one of Layer 2 switches in access network.

MSTP in the SR-Series Platform

The SR-Series platform uses a concept of mVPLS to group different SAPs under a single STP instance. The VLAN range covering SAPs to be managed by a given mVPLS is declared under a specific mVPLS SAP definition. MSTP mode-of-operation is only supported in an mVPLS.

When running MSTP, by default, all VLANs are mapped to the CIST. On the VPLS level VLANs can be assigned to specific MSTIs. When running RSTP, the operator must explicitly indicate, per SAP, which VLANs are managed by that SAP.
Enhancements to the Spanning Tree Protocol

To interconnect routers (PE devices) across the backbone, service tunnels (SDPs) are used. These service tunnels are shared among multiple VPLS instances. Alcatel-Lucent’s implementation of the Spanning Tree Protocol (STP) incorporates some enhancements to make the operational characteristics of VPLS more effective. The implementation of STP on the router is modified in order to guarantee that service tunnels will not be blocked in any circumstance without imposing artificial restrictions on the placement of the root bridge within the network. The modifications introduced are fully compliant with the 802.1D-2004 STP specification.

When running MSTP, spoke SDPs cannot be configured. Also, ensure that all bridges connected by mesh SDPs are in the same region. If not, the mesh will be prevented from becoming active (trap is generated).

In order to achieve this, all mesh SDPs are dynamically configured as either root ports or designated ports. The PE devices participating in each VPLS mesh determine (using the root path cost learned as part of the normal protocol exchange) which of the SR-OS devices is closest to the root of the network. This PE device is internally designated as the primary bridge for the VPLS mesh. As a result of this, all network ports on the primary bridges are assigned the designated port role and therefore remain in the forwarding state.

The second part of the solution ensures that the remaining PE devices participating in the STP instance see the SDP ports as a lower cost path to the root rather than a path that is external to the mesh. Internal to the PE nodes participating in the mesh, the SDPs are treated as zero cost paths towards the primary bridge. As a consequence, the path through the mesh are seen as lower cost than any alternative and the PE node will designate the network port as the root port. This approach ensures that network ports always remain in forwarding state.

In combination, these two features ensure that network ports will never be blocked and will maintain interoperability with bridges external to the mesh which are running STP instances.
L2PT Termination

L2PT is used to transparently transport protocol data units (PDUs) of Layer 2 protocols such as STP, CDP, VTP and PAGP and UDLD. This allows running these protocols between customer CPEs without involving backbone infrastructure.

SR-OS routers allow transparent tunneling of PDUs across the VPLS core. However, in some network designs, the VPLS PE is connected to CPEs through a legacy Layer 2 network, rather than having direct connections. In such environments termination of tunnels through such infrastructure is required.

L2PT tunnels protocol PDUs by overwriting MAC destination addresses at the ingress of the tunnel to a proprietary MAC address such as 01-00-0c-cd-cd-d0. At the egress of the tunnel, this MAC address is then overwritten back to MAC address of the respective Layer 2 protocol.

SR-OS routers support L2PT termination for STP BPDUs. More specifically:

- At ingress of every SAP/spoke SDP which is configured as L2PT termination, all PDUs with a MAC destination address, 01-00-0c-cd-cd-d0 will be intercepted and their MAC destination address will be overwritten to MAC destination address used for the corresponding protocol (PVST, STP, RSTP). The type of the STP protocol can be derived from LLC and SNAP encapsulation.

- In egress direction, all STP PDUs received on all VPLS ports will be intercepted and L2PT encapsulation will be performed for SAP/spoke SDPs configured as L2PT termination points. Because of the implementation reasons, PDU interception and redirection to CPM can be performed only at ingress. Therefore, to comply with the above requirement, as soon as at least 1 port of a given VPLS service is configured as L2PT termination port, redirection of PDUs to CPM will be set on all other ports (SAPs, spoke SDPs and mesh SDPs) of the VPLS service.

L2PT termination can be enabled only if STP is disabled in a context of the given VPLS service.
**BPDU Translation**

VPLS networks are typically used to interconnect different customer sites using different access technologies such as Ethernet and bridged-encapsulated ATM PVCs. Typically, different Layer 2 devices can support different types of STP and even if they are from the same vendor. In some cases, it is necessary to provide BPDU translation in order to provide an interoperable e2e solution.

To address these network designs, BPDU format translation is supported on SR-OS devices. If enabled on a given SAP or spoke SDP, the system will intercept all BPDUs destined to that interface and perform required format translation such as STP-to-PVST or vice versa.

Similarly, BPDU interception and redirection to the CPM is performed only at ingress meaning that as soon as at least 1 port within a given VPLS service has BPDU translation enabled, all BPDUs received on any of the VPLS ports will be redirected to the CPM.

BPDU translation involves all encapsulation actions that the data path would perform for a given outgoing port (such as adding VLAN tags depending on the outer SAP and the SDP encapsulation type) and adding or removing all the required VLAN information in a BPDU payload.

This feature can be enabled on a SAP only if STP is disabled in the context of the given VPLS service.

---

**L2PT and BPDU Translation**

Cisco Discovery Protocol (CDP), Digital Trunking Protocol (DTP), Port Aggregation Protocol (PAGP), Uni-directional Link Detection (ULD) and Virtual Trunk Protocol (VTP) are supported. These protocols automatically pass the other protocols tunneled by L2PT towards the CPM and all carry the same specific Cisco MAC.

The existing L2PT limitations apply.

- The protocols apply only to VPLS.
- The protocols are mutually exclusive with running STP on the same VPLS as soon as one SAP has L2PT enabled.
- Forwarding occurs on the CPM.
Egress Multicast Groups

Efficient multicast replication is a method of increasing egress replication performance by combining multiple destinations into a single egress forwarding pass. In standard egress VPLS multicast forwarding, the complete egress forwarding plane is used per destination to provide ACL, mirroring, QoS and accounting for each path with associated receivers. In order to apply the complete set of available egress VPLS features, the egress forwarding plane must loop-back copies of the original packet so that each flooding destination may be processed. While each distributed egress forwarding plane only replicates to the destinations currently reached through its ports, this loop-back and replicate function can be resource intensive. When egress forwarding plane congestion conditions exist, unicast discards may be indiscriminate relative to forwarding priority. Another by-product of this approach is that the ability for the forwarding plane to fill the egress links is affected which could cause under-run conditions on each link while the forwarding plane is looping packets back to itself.

In an effort to provide highly scalable VPLS egress multicast performance for triple play type deployments, an alternative efficient multicast forwarding option is being offered. This method allows the egress forwarding plane to send a multicast packet to a set (called a chain) of destination SAPs with only a single pass through the egress forwarding plane. This minimizes the egress resources (processing and traffic management) used for the set of destinations and allows proper handling of congestion conditions and minimizes line under-run events. However, due to the batch nature of the egress processing, the chain of destinations must share many attributes. Also, egress port and ACL mirroring will be disallowed for packets handled in this manner.

Packets eligible for forwarding by SAP chaining are VPLS flooded packets (broadcast, multicast and unknown destination unicast) and IP multicast packets matching an VPLS Layer 2 (s,g) record (created through IGMP snooping).

Egress Multicast Group Provisioning

To identify SAPs in the chassis that are eligible for egress efficient multicast SAP chaining, an egress multicast group must be created. SAPs from multiple VPLS contexts may be placed in a single group to minimize the number of groups required on the system and to support multicast VPLS registration (MVR) functions.

Some of the parameters associated with the group member SAPs must be configured with identical values. The common parameters are checked as each SAP is provisioned into the group. If the SAP fails to be consistent in one or more parameters, the SAP is not allowed into the egress multicast group. Once a SAP is placed into the group, changing of a common parameter is not permitted.
Required Common SAP Parameters

Only SAPs created on Ethernet ports are allowed into an egress multicast group.

Required common parameters include:

- SAP Port Encapsulation Type on page 571
- SAP Port Dot1Q EtherType on page 571
- Egress Multicast Groups on page 572
- SAP Egress Filter on page 572

SAP Port Encapsulation Type

The access port encapsulation type defines how the system will delineate SAPs from each other on the access port. SAPs placed in the egress multicast group must be of the same type. The supported access port encapsulation types are null and Dot1q. While all SAPs within the egress multicast group share the same encapsulation type, they are allowed to have different encapsulation values defined. The chained replication process will make the appropriate Dot1q value substitution per destination SAP.

The normal behavior of the system is to disallow changing the port encapsulation type once one or more SAPs have been created on the SAP. This being the case, no special effort is required to ensure that a SAP will be changed from null to Dot1q or Dot1q to null while the SAP is a member of a egress multicast group. Deleting the SAP will automatically remove the SAP from the group.

SAP Port Dot1Q EtherType

The access port dot1q-etype parameter defines which EtherType will be expected in ingress dot1q encapsulated frames and the EtherType that will be used to encapsulate egress dot1q frames on the port. SAPs placed in the same egress multicast group must use the same EtherType when dot1q is enabled as the SAPs encapsulation type.

The normal behavior of the system is to allow dynamic changing of the access port dot1q-etype value while SAPs are currently using the port. Once a dot1q SAP on an access port is allowed into an egress multicast group, the port on which the SAP is created will not accept a change of the configured dot1q-etype value. When the port encapsulation type is set to null, the port’s dot1q-etype parameter may be changed at any time.
Egress Multicast Groups

Egress multicast groups to QinQ-encapsulated SAPs support includes:

- All SAP members of the given egress-multicast-group must have the same inner tag.
- A configuration flag, indicates, on a per egress-multicast-group basis, whether all member SAPs have the same inner or outer VLAN tag.

Membership rules for egress-multicast-groups in QinQ SAPs include:

- All SAPs that are members of the same egress-multicast-groups must have the same encapsulation type (as defined by encap-type qinq statement)
- All SAP members of the given multicast group, port, or multicast-group must have the same inner Ethertype as well as outer Ethertype.
- All SAP members of the multicast-group must have the same inner-vlan-tag (the default setting) or must have the same value of outer-vlan-tag as defined by the `qinq-fixed-tag-value` command.

SAP Egress Filter

Due to the chaining nature of egress efficient multicast replication, only the IP or MAC filter defined for the first SAP on each chain is used to evaluate the packet. To ensure consistent behavior for all SAPs in the egress multicast group, when an IP or MAC filter is configured on one SAP it must be configured on all. To prevent inconsistencies, each SAP must have the same egress IP or MAC filter configured (or none at all) prior to allowing the SAP into the egress multicast group.

Attempting to change the egress filter configured on the SAP while the SAP is a member of an egress multicast group is not allowed.

If the configured common egress filter is changed on the egress multicast group, the egress filter on all member SAPs will be overwritten by the new defined filter. If the SAP is removed from the group, the previous filter definition is not restored.

SAP Egress QoS Policy

Each SAP placed in the egress multicast group may have a different QoS policy defined. When the egress forwarding plane performs the replication for each destination in a chain, the internal forwarding class associated with the packet is used to map the packet to an egress queue on the SAP.
In the case where customer SLA management is enabled on the SAP and the SAP queues are not available, the queues created by the non-sub-addr-traffic SLA-profile instance are used.

One caveat is that egress Dot1P markings for Dot1q SAPs in the replication chain are only evaluated for the first SAP in the chain. If the first SAP defines an egress Dot1P override for the packet, all encapsulations in the chain will share the same value. If the first SAP in the chain does not override the egress Dot1P value, either the existing Dot1P value (relative to ingress) will be preserved or the value 0 (zero) will be used for all SAPs in the replication chain. The egress QoS policy Dot1P remark definitions on the other SAPs in the chain are ignored by the system.

---

**Efficient Multicast Egress SAP Chaining**

The egress XCM automatically creates the SAP chains on each egress forwarding plane. The size of each chain is based on the dest-chain-limit command defined on the egress multicast group to which the SAPs in the chain belong.

A set of chains is created by the XCM for each egress flooding list managed by the IOM. While SAPs from multiple VPLS contexts are allowed into a single egress multicast group, an egress flooding list is typically based on a subset of these SAPs. For instance, the broadcast/multicast/unknown flooding list for a VPLS context is limited to the SAPs in that VPLS context. With IGMP snooping on a single VPLS context, the flooding list is per Layer 2 IGMP (s,g) record and is basically limited to the destinations where IGMP joins for the multicast stream have been intercepted. When MVR (Multicast VPLS Registration) is enabled, the (s,g) flooding list may include SAPs from various VPLS contexts based on MVR configuration.

The system maintains a unique flooding list for each forwarding plane VPLS context (see section VPLS Broadcast/Multicast/Unknown Flooding List on page 575). This list will contain all SAPs (except for residential SAPs), spoke SDP and mesh SDP bindings on the forwarding plane that belong to that VPLS context. Each list may contain a maximum of 127 SAPs. In the case where the XCM is able to create an egress multicast chain, the SAPs within the chain are represented in the flooding list by a single SAP entry (the first SAP in the chain).

The system also maintains a unique flooding list for each Layer 2 IP multicast (s,g) record created through IGMP snooping (see sections VPLS IGMP Snooping (s,g) Flooding List on page 576 and MVR IGMP Snooping (s,g) Flooding List on page 576). A flooding list created by IGMP snooping is limited to 127 SAPs, although it may contain other entries representing spoke and mesh SDP bindings. Unlike a VPLS flooding list, a residential SAP may be included in a Layer 2 IP multicast flooding list.

While the system may allow 30 SAPs in a chain, the uninterrupted replication to 30 destinations may have a negative effect on other packets waiting to be processed by the egress forwarding plane. Most notably, massive jitter may be seen on real time VoIP or other time-sensitive applications. The dest-chain-limit parameter should be tuned to allow the proper balance between multicast replication efficiency and the effect on time sensitive application performance. It is
expected that the optimum performance for the egress forwarding plane will be found at around 16 SAPs per chain.
VPLS Broadcast/Multicast/Unknown Flooding List

The XCM includes all VPLS destinations in the egress VPLS Broadcast/Multicast/Unknown (BMU) flooding list that exist on a single VPLS context. Whenever a broadcast, multicast or unknown destination MAC is received in the VPLS, the BMU flooding list is used to flood the packet to all destinations. For normal flooding, care is taken at egress to ensure that the packet is not sent back to the source of the packet. Also, if the packet is associated with a split horizon group (mesh or spoke/SAP) the egress forwarding plane will prevent the packet from reaching destinations in the same split horizon context as the source SAP or SDP-binding.

The VPLS BMU flooding list may contain both egress multicast group SAPs and other SAPs or SDP bindings as destinations. The egress XCM will separate the egress multicast group SAPs from the other destinations to create one or more chains. Egress multicast group SAPs are placed into a chain completely at the discretion of the XCM and the order of SAPs in the list will be nondeterministic. When more SAPs exist on the VPLS context within the egress multicast group then are allowed in a single chain, multiple SAP chains will be created. The XCM VPLS egress BMU flooding list will then contain the first SAP in each chain plus all other VPLS destinations.

The SAPs in the same VPLS context must be in the same split horizon group to allow membership into the egress multicast group. The split horizon context is not required to be the same between VPLS contexts.

SAPs within the same VPLS context may be defined in different egress multicast groups, but SAPs in different multicast groups cannot share the same chain.
**VPLS IGMP Snooping (s,g) Flooding List**

When IGMP snooping is enabled on a VPLS context, a Layer 2 IP multicast record (s,g) is created for each multicast stream entering the VPLS context. Each stream should only be sent to each SAP or SDP binding where either a multicast router exists or a host exists that has requested to receive the stream (known as a receiver). To facilitate egress handling of each stream, the XCM creates a flooding list for each (s,g) record associated with the VPLS context. As with the BMU flooding list, source and split horizon squelching is enforced by the egress forwarding plane.

As with the BMU VPLS flooding list, the egress multicast group SAPs that have either static or dynamic multicast receivers for the (s,g) stream are chained into groups. The chaining is independent of other (s,g) flooding lists and the BMU flooding list on the VPLS instance. As the (s,g) flooding list membership is dynamic, the egress multicast group SAPs in chains in the list are also managed dynamically.

Since all SAPs placed into the egress multicast group for a particular VPLS context are in the same split horizon group, no special function is required for split horizon squelching.

---

**MVR IGMP Snooping (s,g) Flooding List**

When IGMP snooping on a SAP is tied to another VPLS context to facilitate cross VPLS context IP multicast forwarding, a Layer 2 IP multicast (s,g) record is maintained on the VPLS context receiving the multicast stream. This is essentially an extension to the VPLS IGMP snooped flooding described in VPLS IGMP Snooping (s,g) Flooding List on page 576. The (s,g) list is considered to be owned by the VPLS context that the multicast stream will enter. Any SAP added to the list that is outside the target VPLS context (using the `from-vpls` command) is handled as an alien SAP. Split horizon squelching is ignored for alien SAPs.

When chaining the egress multicast group SAPs in an MVR (s,g) list, the XCM will keep the native chained SAPs in separate chains from the alien SAPs to prevent issues with split horizon squelching.

---

**Mirroring and Efficient Multicast Replication**

As previously stated, efficient multicast replication affects the ability to perform mirroring decisions in the egress forwarding plane. In the egress forwarding plane, mirroring decisions are performed prior to the egress chain replication function. Since mirroring decisions are only evaluated for the first SAP in each chain, applying a mirroring condition to packets that egress other SAPs in the chain has no effect. Also, the XCM manages the chain membership automatically and the user has no ability to provision which SAP is first in a chain. Thus, mirroring is not allowed for SAPs within a chain.
Port Mirroring

A SAP created on an access port that is currently defined as an egress mirror source may not be defined into an egress multicast group.

A port that has a SAP defined in an egress multicast group may not be defined as an egress mirror source. If egress port mirroring is desired, then all SAPs on the port must first be removed from all egress multicast groups.

Filter Mirroring

An IP or MAC filter that is currently defined on an egress multicast group as a common required parameter may not have an entry from the list defined as a mirror source.

An IP or MAC filter that has an entry defined as a mirror source may not be defined as a common required parameter for an egress multicast group.

If IP or MAC based filter mirroring is required for packets that egress an egress multicast group SAP, the SAP must first be removed from the egress multicast group and then an IP or MAC filter that is not associated with an egress multicast group must be assigned to the SAP.

SAP Mirroring

While SAP mirroring is not allowed within an IOM chain of SAPs, it is possible to define an egress multicast group member SAP as an egress mirror source. When the IOM encounters a chained SAP as an egress mirror source, it automatically removes the SAP from its chain, allowing packets that egress the SAP to hit the mirror decision. Once the SAP is removed as an egress mirror source, the SAP will be automatically placed back into a chain by the XCM.

It should be noted that all mirroring decisions affect forwarding plane performance due to the overhead of replicating the frame to the mirror destination. This is especially true for efficient multicast replication as removing the SAP from the chain also eliminates a portion of the replication efficiency along with adding the mirror replication overhead.

OAM Commands with EMG

There are certain limitations with using the OAM commands when egress multicast group (EMG) is enabled. This is because OAM commands work by looping the OAM packet back to ingress instead of sending them out of the SAP. Hence, if EMG is enabled, these OAM packets will be looped back once per chain and hence, will only be processed for the first SAP on each chain. Particularly, the mac-ping, mac-trace and mfib-ping commands will only list the first SAP in each chain.
XCM Chain Management

As previously stated, the XCM automatically creates the chain lists from the available egress multicast group SAPs. The XCM will create chains from the available SAPs based on the following rules:

1. SAPs from different egress multicast groups must be in different chains (a chain can only contain SAPs from the same group)
2. Alien and native SAPs must be in different chains
3. A specific chain cannot be longer than the defined dest-chain-limit parameter for the egress multicast group to which the SAPs belong

Given the following conditions for an XCM creating a multicast forwarding list (List 1) for a Layer 2 IP multicast (s, g) native to VPLS instance 100:

- Egress multicast group A
  - Destination chain length = 16
  - 30 member SAPs on VPLS 100 joined (s, g) (native to VPLS 100)
  - 41 member SAPs on other VPLS instances joined (s, g) (alien to VPLS 100)
- Egress multicast group B
  - Destination chain length = 8
  - 17 member SAPs on VPLS 100 joined (s, g) (native to VPLS 100)
- Egress multicast group C
  - Destination chain length = 12
  - 23 member SAPs on other VPLS instances joined (s, g) (alien to VPLS 100)

The system will build the SAP chains for List 1 according to Table 8.

Table 8: SAP Chain Creation

<table>
<thead>
<tr>
<th>Egress Multicast Group A</th>
<th>Egress Multicast Group B</th>
<th>Egress Multicast Group C</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination Chain Length</td>
<td>Destination Chain Length</td>
<td>Destination Chain Length</td>
</tr>
<tr>
<td>16</td>
<td>16</td>
<td>16</td>
</tr>
<tr>
<td>Alien Chains</td>
<td>Native Chains</td>
<td>Alien Chains</td>
</tr>
<tr>
<td>14</td>
<td>16</td>
<td>8</td>
</tr>
<tr>
<td>9</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>
Adding a SAP to a Chain

A SAP must meet all the following conditions to be chained in a VPLS BMU flooding list:

1. The SAP is successfully defined as an egress multicast group member
2. The SAP is not currently an egress mirror source

Further, a SAP must meet the following conditions to be chained in an egress IP multicast \((s,g)\) flooding list:

1. The SAP is participating in IGMP snooping
2. A static or dynamic join to the \((s,g)\) record exists for the SAP or the SAP is defined as a multicast router port

Note: While an operationally down SAP is placed into replication chains, the system ignores that SAP while in the process of replication.

Based on the egress multicast group and the native or alien nature of the SAP in the list, a set of chains are selected for the SAP. The XCM will search the chains for the first empty position in an existing chain and place the SAP in that position. If an empty position is not found, the XCM will create a new chain with that SAP in the first position and add the SAP to the flooding list to represent the new chain.

Removing a SAP from a Chain

A SAP will be removed from a chain in a VPLS BMU flooding list or egress IP multicast \((s,g)\) flooding list for any of the following conditions:

1. The SAP is deleted from the VPLS instance
2. The SAP is removed from the egress multicast group of which it was a member
3. The SAP is defined as an egress mirror source

Further, a SAP will be removed from an egress IP multicast \((s,g)\) flooding list for the following conditions:

1. IGMP snooping removes the SAP as an \((s,g)\) destination or the SAP is removed as a multicast router port

When the SAP is only being removed from the efficient multicast replication function, it may still need to be represented as a stand alone SAP in the flooding list. If the removed SAP is the first SAP in the list, the second SAP in the list is added to the flooding list when the first SAP is de-chained. If the removed SAP is not the first SAP, it is first de-chained and then added to the
flooding list. If the removed SAP is the only SAP in the chain, the chain is removed along with removing the SAP from the flooding list.

Moving a SAP from a chain to a stand alone condition or from a stand alone condition to a chain may cause a momentary glitch in the forwarding plane for the time that the SAP is being moved. Care is taken to prevent or minimize the possibility of duplicate packets being replicated to a destination while the chains and flooding lists are being manipulated.

Chain Optimization

Chains are only dynamically managed during SAP addition and removal events. The system does not attempt to automatically optimize existing chains. It is possible that excessive SAP removal may cause multiple chains to exist with lengths less than the maximum chain length. For example, if four chains exist with eight SAPs each, it is possible that seven of the SAPs from each chain are removed. The result would be four chains of one SAP each effectively removing any benefit of egress SAP replication chaining.

While it may appear that optimization would be beneficial each time a SAP is removed, this is not the case. Rearranging the chains each time a SAP is removed may cause either packet duplication or omitting replication to a destination SAP. Also, it could be argued that if the loop back replication load is acceptable before the SAP is removed, continuing with the same loop back replication load once the SAP is removed is also acceptable. It is important to note that the overall replication load is lessened with each SAP removal from a chain.

While dynamic optimization is not supported, a manual optimization command is supported in each egress multicast group context. When executed the system will remove and add each SAP, rebuilding the replication chains.

When the dest-chain-limit is modified for an egress multicast group, the system will reorganize the replication chains that contain SAPs from that group according to the new maximum chain size.
VPLS Redundancy

The VPLS standard (RFC 4762, *Virtual Private LAN Services Using LDP Signalling*) includes provisions for hierarchical VPLS, using point-to-point spoke SDPs. Two applications have been identified for spoke SDPs:

- To connect to Multi-Tenant Units (MTUs) to PEs in a metro area network;
- To interconnect the VPLS nodes of two metro networks.

In both applications the spoke SDPs serve to improve the scalability of VPLS. While node redundancy is implicit in non-hierarchical VPLS services (using a full mesh of SDPs between PEs), node redundancy for spoke SDPs needs to be provided separately.

Alcatel-Lucent routers have implemented special features for improving the resilience of hierarchical VPLS instances, in both MTU and inter-metro applications.

Spoke SDP Redundancy for Metro Interconnection

When two or more meshed VPLS instances are interconnected by redundant spoke SDPs (as shown in Figure 85), a loop in the topology results. In order to remove such a loop from the topology, Spanning Tree Protocol (STP) can be run over the SDPs (links) which form the loop such that one of the SDPs is blocked. As running STP in each and every VPLS in this topology is not efficient, the node includes functionality which can associate a number of VPLSes to a single STP instance running over the redundant SDPs. Node redundancy is thus achieved by running STP in one VPLS, and applying the conclusions of this STP to the other VPLS services. The VPLS instance running STP is referred to as the “management VPLS” or mVPLS.

In the case of a failure of the active node, STP on the management VPLS in the standby node will change the link states from disabled to active. The standby node will then broadcast a MAC flush LDP control message in each of the protected VPLS instances, so that the address of the newly active node can be re-learned by all PEs in the VPLS.

It is possible to configure two management VPLS services, where both VPLS services have different active spokes (this is achieved by changing the path-cost in STP). By associating different user VPLSes with the two management VPLS services, load balancing across the spokes can be achieved.
Figure 85: HVPLS with Spoke Redundancy
Spoke SDP Based Redundant Access

This feature provides the ability to have a node deployed as MTUs (Multi-Tenant Unit Switches) to be multi-homed for VPLS to multiple routers deployed as PEs without requiring the use of mVPLS.

In the configuration example displayed in Figure 85, the MTUs have spoke SDPs to two PEs devices. One is designated as the primary and one as the secondary spoke SDP. This is based on a precedence value associated with each spoke.

The secondary spoke is in a blocking state (both on receive and transmit) as long as the primary spoke is available. When the primary spoke becomes unavailable (due to link failure, PEs failure, etc.), the MTU immediately switches traffic to the backup spoke and starts receiving traffic from the standby spoke. Optional revertive operation (with configurable switch-back delay) is supported. Forced manual switchover is also supported.

To speed up the convergence time during a switchover, MAC flush is configured. The MTUs generates a MAC flush message over the newly unblocked spoke when a spoke change occurs. As a result, the PEs receiving the MAC flush will flush all MACs associated with the impacted VPLS service instance and forward the MAC flush to the other PEs in the VPLS network if “propagate-mac-flush” is enabled.
Inter-Domain VPLS Resiliency Using Multi-Chassis Endpoints

Inter-domain VPLS refers to a VPLS deployment where sites may be located in different domains. An example of inter-domain deployment can be where different Metro domains are interconnected over a Wide Area Network (Metro1-WAN-Metro2) or where sites are located in different autonomous systems (AS1-ASBRs-AS2).

Multi-chassis endpoint (MC-EP) provides an alternate solution that does not require RSTP at the gateway VPLS PEs while still using pseudowires to interconnect the VPLS instances located in the two domains. It is supported in both VPLS and PBB-VPLS on the B-VPLS side.

MC-EP expands the single chassis endpoint based on active-standby pseudowires for VPLS shown in Figure 86.

The active-standby pseudowire solution is appropriate for the scenario when only one VPLS PE (MTU-s) needs to be dual-homed to two core PEs (PE1 and PE2). When multiple VPLS domains need to be interconnected the above solution provides a single point of failure at the MTU-s. The example depicted in Figure 87 can be used.
Figure 87: Multi-Chassis Pseudowire Endpoint for VPLS

The two gateway pairs, PE3-PE3and PE1-PE2, are interconnected using a full mesh of four pseudowires out of which only one pseudowire is active at any point in time.

The concept of pseudowire endpoint for VPLS provides multi-chassis resiliency controlled by the MC-EP pair, PE3-PE3 in this example. This scenario, referred to as multi-chassis pseudowire endpoint for VPLS, provides a way to group pseudowires distributed between PE3 and PE3 chassis in a virtual endpoint that can be mapped to a VPLS instance.

The MC-EP inter-chassis protocol is used to ensure configuration and status synchronization of the pseudowires that belong to the same MC-EP group on PE3 and PE3. Based on the information received from the peer shelf and the local configuration the master shelf will make a decision on which pseudowire will become active.

The MC-EP solution is built around the following components:

- Multi-chassis protocol used to perform the following functions:
  - Selection of master chassis.
  - Synchronization of the pseudowire configuration and status.
  - Fast detection of peer failure or communication loss between MC-EP peers using either centralized BFD if configured or its own keep-alive mechanism.
- T-LDP signaling of pseudowire status:
  - Informs the remote PEs about the choices made by the MC-EP pair
- Pseudowire data plane — Represented by the four pseudowires inter-connecting the gateway PEs.
Only one of the pseudowires is activated based on the primary/secondary, preference configuration and pseudowire status. In case of a tie the pseudowire located on the master chassis will be chosen.

The rest of the pseudowires are blocked locally on the MC-EP pair and on the remote PEs as long as they implement the pseudowire active/standby status.

Fast Detection of Peer Failure using BFD

Although the MC-EP protocol has its own keep-alive mechanisms, sharing a common mechanism for failure detection with other protocols (for example, BGP, RSVP-TE) scales better. MC-EP can be configured to use the centralized BFD mechanism.

Similar as other protocols, MC-EP will register with BFD if the `bfd-enable` command is active under the `config>redundancy>multi-chassis>peer>mc-ep` context. As soon as the MC-EP application is activated using no shutdown, it tries to open a new BFD session or register automatically with an existing one. The source-ip configuration under redundancy multi-chassis peer-ip is used to determine the local interface while the peer-ip is used as the destination IP for the BFD session. After MC-EP registers with an active BFD session, it will use it for fast detection of MC-EP peer failure. If BFD registration or BFD initialization fails, the MC-EP will keep using its own keep-alive mechanism and it will send a trap to the NMS signaling the failure to register with/open BFD session.

In order to minimize operational mistakes and wrong peer interpretation for the loss of BFD session, the following additional rules are enforced when the MC-EP is registering with a certain BFD session:

- Only the centralized BFD sessions using system or loopback IP interfaces (source-ip parameter) are accepted in order for MC-EP to minimize the false indication of peer loss.
- If the BFD session associated with MC-EP protocol is using a certain interface (system/loopback) then the following actions are not allowed under the interface: IP address change, “shutdown”, “no bfd” commands. If one of these action is required under the interface, the operator needs to disable BFD using the following procedures:
  - The `no bfd-enable` command in the `config>redundancy>multi-chassis>peer>mc-ep` context – this is the recommended procedure.
  - The `shutdown` command in the `config>redundancy>multi-chassis>peer>mc-ep` or from under `config>redundancy>multi-chassis>peer` contexts.

MC-EP keep-alives are still exchanged for the following reasons:

- As a backup - if the BFD session does not come up or is disabled, the MC-EP protocol will use its own keep-alives for failure detection.
- To ensure the database is cleared if the remote MC-EP peer is shutdown or miss-configured (each x seconds – one second suggested as default).
If MC-EP de-registers with BFD using the “no bfd-enable” command, the following processing steps occur:

- Local peer indicates to the MC-EP peer the fact that local BFD is being disabled using MC-EP peer-config-TLV fields ([BFD local : BFD remote]). This is done to avoid wrong interpretation of BFD session loss.
- Remote peer acknowledges reception indicating through the same peer-config-TLV fields that it is de-registering with the BFD session.
- Both MC-EP peers de-register and are going to use only keep-alives for failure detection.
- There should be no pseudowire status change during this process.

Traps are sent when the status of the monitoring of the MC-EP session through BFD changes in the following instances:

- When red/mc/peer is no shutdown and BFD is not enabled, send a notification indicating BFD is not monitoring MC-EP peering session.
- When BFD changes to open, send a notification indicating BFD is monitoring MC-EP peering session.
- When BFD changes to down/close, send a notification indicating BFD is not monitoring MC-EP peering session.

**MC-EP Passive Mode**

The MC-EP mechanisms are built to minimize the possibility of loops. It is possible that human error could create loops through the VPLS service. One way to prevent loops is to enable the MAC move feature in the gateway PEs (PE3, PE3’, PE1 and PE2).

An MC-EP passive mode can also be used on the second PE pair, PE1 and PE2, as a second layer of protection to prevent any loops from occurring if the operator introduces operational errors on the MC-EP PE3, PE3 pair.
When in passive mode, the MC-EP peers stay dormant as long as one active pseudowire is signaled from the remote end. If more than one pseudowire belonging to the passive MC-EP becomes active, then the PE1 and PE2 pair applies the MC-EP selection algorithm to select the best choice and blocks all others. No signaling is sent to the remote pair to avoid flip-flop behavior. A trap is generated each time MC-EP in passive mode activates. Every occurrence of this kind of trap should be analyzed by the operator as it is an indication of possible misconfiguration on the remote (active) MC-EP peering.

In order for the MC-EP passive mode to work, the pseudowire status signaling for active/standby pseudowires should be enabled. This involves the following CLI configurations:

For the remote MC-EP PE3, PE3 pair:

```
cfg>service>vpls>endpoint# no suppress-standby-signaling
```

When MC-EP passive mode is enabled on the PE1 and PE2 pair the following command is always enabled internally, regardless of the actual configuration:

```
cfg>service>vpls>endpoint no ignore-standby-signaling
```

**Support for Single Chassis Endpoint Mechanisms**

In cases of SC-EP, there is consistency check to ensure that the configuration of the member pseudowires is the same. For example, mac-pining, mac-limit and ignore standby signaling must
be the same. In the MC-EP case, there is no consistency check between the member endpoints located on different chassis. The operator must verify carefully the configuration of the two endpoints to ensure consistency.

The following rules apply for suppress-standby-signaling and ignore-standby parameters:

- Regular MC-EP mode (non-passive) will follow the suppress-standby-signaling and ignore-standby settings from the related endpoint configuration.
- For MC-EP configured in passive mode, the following settings will be used, regardless of previous configuration: **suppress-standby-sig** and **no ignore-standby-sig**. It is expected that when passive mode is used at one side that the regular MC-EP side will activate signaling with **no suppress-stdby-sig**.
- When passive mode is configured in just one of the nodes in the MC-EP peering, the other node will be forced to change to passive mode. A trap is sent to the operator to signal the wrong configuration.

This section describes also how the main mechanisms used for single chassis endpoint are adapted for the MC-EP solution.

---

**MAC Flush Support in MC-EP**

In an MC-EP scenario, failure of a pseudowire or gateway PE will determine activation of one of the next best pseudowire in the MC-EP group. This section describes the MAC flush procedures that can be applied to ensure black-hole avoidance.

**Figure 89** depicts a pair of PE gateways (PE3 and PE3) running MC-EP towards PE1 and PE2 where F1 and F2 are used to indicate the possible direction of the MAC flush signaled using T-LDP MAC withdraw message. PE1 and PE2 can only use regular VPLS pseudowires and do not have to use a MC-EP or a regular pseudowire endpoint.
Regular MAC flush behavior will apply for the LDP MAC withdraw sent over the T-LDP Sessions associated with the active pseudowire in the MC-EP, for example PE3 to PE1. That is for any TCN events or failures associated with SAPs or pseudowires not associated with the MC-EP.

The following MAC flush behaviors apply to changes in the MC-EP pseudowire selection:

- If the local PW2 becomes active on PE3:
  - On PE3 the MACs mapped to PW1 are moved to PW2.
  - A T-LDP “flush-all-but-mine” message is sent toward PE2 in F2 direction and is propagated by PE2 in the local VPLS mesh.
  - No MAC flush is sent to F1 direction from PE3.
- If one of the pseudowires on the pair PE3 becomes active, for example PW4:
  - On PE3, the MACs mapped to PW1 are flushed, same as a regular endpoint.
  - PE3 must be configured with send-flush-on-failure to send a T-LDP “flush-all-from-me” message towards VPLS mesh in the F1 direction.
  - PE3 sends a T-LDP flush-all-but-mine message towards PE2 in the F2 direction which is propagated by PE2 in the local VPLS mesh. Note that when MC-EP is in passive mode and the first spoke becomes active, a no mac flush-all-but-mine message will be generated.
Block-on-Mesh-Failure Support in MC-EP Scenario

The following rules describe how the block-mesh-on-failure must be ported to the MC-EP solution (see Figure 89):

- If PE3 does not have any forwarding path towards Domain1 mesh, it should block both PW1 and PW2 and inform PE3 so one of its pseudowires can be activated.
- In order to allow the use of block-on-mesh-failure for MC-EP, a new block-on-mesh-failure parameter can be specified in the config>service>vpls>endpoint context with the following rules:
  - The default is no block-on-mesh-failure to allow for easy migration from previous releases.
  - For a spoke SDP to be added under an endpoint, the setting for its block-on-mesh-failure parameter must be in sync with the endpoint parameter.
  - After the spoke SDP is added to an endpoint, the configuration of its block-on-mesh-failure parameter is disabled. A change in endpoint configuration for the block-on-mesh-failure parameter is propagated to the individual spoke SDP configuration.
  - When a spoke SDP is removed from the endpoint group, it will inherit the last configuration from the endpoint parameter.
  - Adding an MC-EP under the related endpoint configuration does not affect in any way the above behavior.

Prior to Release 7.0, the block-on-mesh-failure command could not be enabled under config>service>vpls>endpoint context. In order for a spoke SDP to be added to an (single-chassis) endpoint, its block-on-mesh-failure had to be disabled (config>service>vpls>spoke-sdp>no block-on-mesh-failure). Then, the configuration of block-on-mesh-failure under a spoke SDP is blocked.

- If block-on-mesh-failure is enabled on PE1 and PE2, these PEs will signal pseudowire standby status toward the MC-EP PE pair. PE3 and PE3 should consider the pseudowire status signaling from remote PE1 and PE2 when making the selection of the active pseudowire.

Support for Force Spoke SDP in MC-EP

In a regular (single chassis) endpoint scenario, the following command can be used to force a specific SDP binding (pseudowire) to become active:

```
tools perform service id service-id endpoint endpoint-name force
```

In the MC-EP case, this command has a similar effect when there is a single forced SDP binding in an MC-EP. The forced SDP binding (pseudowire) will be elected as active.
However, when the command is run at the same time as both MC-EP PEs, when the endpoints belong to the same mc-endpoint, the regular MC-EP selection algorithm (for example, the operational status -> precedence value) will be applied to determine the winner.

Revertive Behavior for Primary Pseudowire(s) in a MC-EP

For a single-chassis endpoint a revert-time command is provided under the VPLS endpoint. Refer to the VPLS Services Command Reference on page 711 for syntax and command usage information.

In a regular endpoint the revert-time setting affects just the pseudowire defined as primary (precedence 0). For a failure of the primary pseudowire followed by restoration the revert-timer is started. After it expires the primary pseudowire takes the active role in the endpoint. This behavior does not apply for the case when both pseudowires are defined as secondary: i.e. if the active secondary pseudowire fails and is restored it will stay in standby until a configuration change or a force command occurs.

In the MC-EP case the revertive behavior is supported for pseudowire defined as primary (precedence 0). The following rules apply:

- The revert-time setting under each individual endpoint control the behavior of the local primary pseudowire if one is configured under the local endpoint.
- The secondary pseudowires behave as in the regular endpoint case

Using B-VPLS for Increased Scalability and Reduced Convergence Times

The PBB-VPLS solution can be used to improve scalability of the solution and to reduce convergence time. If PBB-VPLS is deployed starting at the edge PEs, the gateway PEs will contain only BVPLS instances. The MC-EP procedures described for regular VPLS apply.

PBB-VPLS can be also enabled just on the gateway MC-EP PEs as depicted in Figure 90 below.
Multiple I-VPLS instances may be used to represent in the gateway PEs the customer VPLS instances using PBB-VPLS M:1 model described in the PBB section. A backbone VPLS (B-VPLS) is used in this example to administer the resiliency for all customer VPLS instances at the domain borders. Just one MC-EP is required to be configured in the B-VPLS to address 100s or even 1000s of customers VPLS instances. If load balancing is required, multiple B-VPLS instances may be used to ensure even distribution of the customers across all the pseudowires interconnecting the two domains. In this example, four B-VPLS will be able to loadshare the customers across all four possible pseudowire paths.

The use of MC-EP with B-VPLS is strictly limited to cases where VPLS mesh exists on both sides of a B-VPLS. For example, active/standby pseudowires resiliency in the I-VPLS context where PE3, PE3’ are PEs cannot be used because there is no way to synchronize the active/standby selection between the two domains.

For a similar reason, MC-LAG resiliency in the I-VPLS context on the gateway PEs participating in the MC-EP (PE3, PE3) should not be used.

Note that for the PBB topology described in Figure 90, block-on-mesh-failure in the I-VPLS domain will not have any effect on the B-VPLS MC-EP side. That is because mesh failure in one I-VPLS should not affect other I-VPLS sharing the same B-VPLS.
MAC Flush Additions for PBB VPLS

The scenario depicted in Figure 91 is used to define the blackholing problem in PBB-VPLS using MC-EP.

In topology displayed in Figure 91, PE A and PE B are regular VPLS PEs participating in the VPLS mesh deployed in the metro and respectively WAN region. As the traffic flows between CEs with CMAC X and CMAC Y, the FIB entries in blue are installed. A failure of the active PW1 will result in the activation of PW4 between PE3 and PE2 in this example. An LDP flush-all-but-mine will be sent from PE3 to PE2 to clear the BVPLS FIBs. The traffic between CMAC X and CMAC Y will be blackholed as long as the entries from the VPLS and I-VPLS FIBs along the path are not removed. This may take as long as 300 seconds, the usual aging timer used for MAC entries in a VPLS FIB.

A MAC flush is required in the I-VPLS space from PBB PEs to PEA and PEB to avoid blackholing in the regular VPLS space.

In the case of a regular VPLS the following procedure is used:

- PE3 sends a flush-all-from-me towards its local blue IVPLS mesh to PE3 and PEA when its MC-Endpoint becomes disabled
- PE3 sends a flush-all-but-mine on the active PW4 to PE2 which is then propagated by PE2 (propagate-mac-flush must be on) to PEB in the WAN IVPLS mesh.
For consistency, a similar procedure is used for the BVPLS case as depicted in Figure 92.

![Resilient Inter-domain Handoff](image)

**Figure 92: MC-EP with B-VPLS Mac Flush Solution**

In this example, the MC-EP activates B-VPLS PW4 because of either a link/node failure or because of an MC-EP selection re-run that affected the previously active PW1. As a result, the endpoint on PE3 containing PW1 goes down.

The following steps apply:

- PE3 sends in the local I-VPLS context a LDP flush-all-from-me (marked with F1) to PE A and to the other regular VPLS PEs, including PE3. The following command enables this behavior on a per I-VPLS basis: `configure>service>vpls ivpls>send-flush-on-bvpls-failure`.
  - Result: PEA, PE3 and the other local VPLS PEs in the metro clear the VPLS FIB entries associated to PW to PE3.
- PE3 clears the entries associated to PW1 and sends in the B-VPLS context an LDP flush-all-but-mine (marked with F2) towards PE2 on the active PW4.
  - Result: PE2 clears the BVPLS FIB entries not associated with PW4.
- PE2 propagates the MAC flush-all-but-mine (marked with F3) from B-VPLS in the related I-VPLS context(s) towards all participating VPLS PEs – for example, in the blue IVPLS to PE B, PE1. It also clears all the CMAC entries associated with IVPLS pseudowires.

The following command enables this behavior on a per I-VPLS basis:
configure>service>vpls ivpls>propagate-mac-flush-from-bvpls

→ Result: PE B, PE1 and the other local VPLS PEs in the WAN clear the VPLS FIB entries associated to PW to PE2.

→ This command does not control though the propagation in the related IVPLS of the BVPLS LDP MAC flush containing a PBB TLV (BMAC and ISID –list).

- Similar to regular VPLS, LDP signaling of the MAC flush will follow the active topology: for example, no MAC flush will be generated on standby pseudowires.

Other failure scenarios are addressed using the same or a subset of the above steps:

- If the pseudowire (PW2) in the same endpoint with PW1 becomes active instead of PW4, there will be no MAC flush of F1 type.

- If the pseudowire (PW3) in the same endpoint becomes active instead of PW4, the same procedure applies.

Note that for an SC/MC endpoint configured in a BVPLS, failure/de-activation of the active pseudowire member always generates a local MAC flush of all the BMAC associated with the pseudowire. It never generates a MAC move to the newly active pseudowire even if the endpoint stays up. That is because in SC-EP/MC-EP topology, the remote PE might be the terminating PBB PE and may not be able to reach the BMAC of the other remote PE. In other words, connectivity between them exists only over the regular VPLS Mesh.

For the same reasons, it is recommended that static BMAC not be used on SC/MC endpoints.
VPLS Access Redundancy

A second application of hierarchical VPLS is using MTUs that are not MPLS-enabled which must have Ethernet links to the closest PE node. To protect against failure of the PE node, an MTU can be dual-homed and have two SAPs on two PE nodes.

There are several mechanisms that can be used to resolve a loop in an access circuit, however from operation perspective they can be subdivided into two groups:

- STP-based access, with or without mVPLS.
- Non-STP-based access using mechanisms such as MC_LAG, MC-APS, MC-RING.

STP-Based Redundant Access to VPLS

In configuration shown in Figure 93, STP is activated on the MTU and two PEs in order to resolve a potential loop. Note that STP only needs to run in a single VPLS instance, and the results of the STP calculations are applied to all VPLSes on the link.

In this configuration the scope of STP domain is limited to MTU and PEs, while any topology change needs to be propagated in the whole VPLS domain including mesh SDPs. This is done by using so called “MAC-flush” messages defined by RFC 4762. In case of STP as an loop resolution mechanism, every TCN (Topology Change Notification) received in a context of STP instance is translated into LDP- MAC address withdrawal message (also referred to as MAC-flush message) requesting to clear all FDB entries, but the ones learned from originating PE. Such messages are sent to all PE peers connected through SDPs (mesh and spoke) in the context of VPLS service(s) which are managed by the given STP instance.
Redundant Access to VPLS Without STP

The Alcatel-Lucent implementation also alternative methods for providing a redundant access to LAYER 2 services, such as MC-LAG, MC-APS or MC-RING. Also in this case, the topology change event needs to be propagated into VPLS topology in order to provide fast convergence.

Figure 85 illustrates a dual-homed connection to VPLS service (PE-A, PE-B, PE-C, PE-D) and operation in case of link failure (between PE-C and L2-B). Upon detection of a link failure PE-C will send MAC-Address-Withdraw messages, which will indicate to all LDP peers that they should flush all MAC addresses learned from PE-C. This will lead that to a broadcasting of packets addressing affected hosts and re-learning process in case an alternative route exists.

Note that the message described here is different than the message described in previous section and in RFC 4762, *Virtual Private LAN Services Using LDP Signaling*. The difference is in the interpretation and action performed in the receiving PE. According to the standard definition, upon receipt of a MAC withdraw message, all MAC addresses, except the ones learned from the source PE, are flushed.

This section specifies that all MAC addresses learned from the source are flushed. This message has been implemented as an LDP address message with vendor-specific type, length, value (TLV), and is called the flush-mine message.

The advantage of this approach (as compared to RSTP based methods) is that only MAC-affected addresses are flushed and not the full forwarding database. While this method does not provide a mechanism to secure alternative loop-free topology, the convergence time is dependent on the speed of the given CE device will open alternative link (L2-B switch in Figure 57) as well as on the speed PE routers will flush their FDB.

In addition, this mechanism is effective only if PE and CE are directly connected (no hub or bridge) as it reacts to physical failure of the link.
Object Grouping and State Monitoring

This feature introduces a generic operational group object which associates different service endpoints (pseudowires, SAPs, IP interfaces) located in the same or in different service instances.

The operational group status is derived from the status of the individual components using certain rules specific to the application using the concept. A number of other service entities, the monitoring objects, can be configured to monitor the operational group status and to perform certain actions as a result of status transitions. For example, if the operational group goes down, the monitoring objects will be brought down.

VPLS Applicability — Block on VPLS a Failure

This concept is used in VPLS to enhance the existing BGP MH solution by providing a block-on-group failure function similar with the Block-on-mesh failure feature implemented in the past for LDP VPLS mesh. On the PE selected as the Designated Forwarder (DF), if the rest of the VPLS endpoints fail (pseudowire spoke(s)/pseudowire mesh and/or SAP(s)), there is no path forward for the frames sent to the MH site selected as DF. The status of the VPLS endpoints, other than the MH site, is reflected by bringing down/up the object(s) associated with the MH site.

Support for the feature is provided initially in VPLS and BVPLS instance types for LDP VPLS with or without BGP-AD and for BGP VPLS. The following objects may be placed as components of an operational group: BGP VPLS pseudowires, SAPs, spoke-pseudowire, BGP-AD pseudowires. The following objects are supported as monitoring objects: BGP MH site, Individual SAP, spoke-pseudowire.

The following rules apply:

- An object can only belong to one group at a time.
- An object that is part of a group cannot monitor the status of a group.
- An object that monitors the status of a group it cannot be part of a group.
- An operational group may contain any combination of member types: SAP, spoke-pseudowire, BGP-AD or BGP VPLS pseudowires.
- An operational group may contain members from different VPLS service instances.
- Objects from different services may monitor the oper-group.
- Operational group feature may co-exist in parallel with the block-on-mesh feature as long as they are running in different VPLS instances.
There are two steps involved in enabling the block on group failure in a VPLS scenario:

1. Identify a set of objects whose forwarding state should be considered as a whole group then group them under an operational group using the `oper-group` CLI command.

2. Associate other existing objects (clients) with the `oper-group` using the `monitor-group` CLI command; its forwarding state will be derived from the related operational group state.

The status of the operational group (oper-group) is dictated by the status of one or more members according to the following rule:

- The oper-group goes down if all the objects in the oper-group go down; the oper-group comes up if at least one of the components is up.

- An object in the group is considered down if it is not forwarding traffic in at least one direction. That could be because the operational state is down or the direction is blocked through some resiliency mechanisms.

- If a group is configured but no members are specified yet then its status is considered up. As soon as the first object is configured the status of the operational group is dictated by the status of the provisioned member(s).

- For BGP-AD or BGP VPLS pseudowire(s) associated with the oper-group (under the `config>service-vpls>bgp>pw-template-binding` context), the status of the oper-group is down as long as the pseudowire members are not instantiated (auto-discovered and signaled).

A simple configuration example is described for the case of a BGP VPLS mesh used to interconnect different customer location. If we assume a customer edge (CE) device is dual-homed to two PEs using BGP MH the following configuration steps apply:

- The `oper-group bgp-vpls-mesh` is created
- The BGP VPLS mesh is added to the `bgp-vpls-mesh` group through the pseudowire template used to create the BGP VPLS mesh
- The BGP MH site defined for the access endpoint is associated with the `bgp-vpls-mesh` group; its status from now on will be influenced by the status of the BGP VPLS mesh

A simple configuration example follows:

```
service>oper-group bgp-vpls-mesh-1 create
service>vpls>bgp>pw-template-binding> oper-group bgp-vpls-mesh-1
service>vpls>site> monitor-group bgp-vpls-mesh-1
```
MAC Flush Message Processing

The previous sections described operation principle of several redundancy mechanisms available in context of VPLS service. All of them rely on MAC flush message as a tool to propagate topology change in a context of the given VPLS. This section aims to summarize basic rules for generation and processing of these messages.

As described on respective sections, the SR-OS supports two types of MAC flush message, flush-all-but-mine and flush-mine. The main difference between these messages is the type of action they signal. Flush-all-but-mine requests clearing of all FDB entries which were learned from all other LDP peers except the originating PE. This type is also defined by RFC 4762 as an LDP MAC address withdrawal with an empty MAC address list.

Flush-all-mine message requests clearing all FDB entries learned from originating PE. This means that this message has exactly other effect then flush-all-but-mine message. This type is not included in RFC 4762 definition and it is implemented using vendor specific TLV.

The advantages and disadvantages of the individual types should be apparent from examples in the previous section. The description here focuses on summarizing actions taken on reception and conditions individual messages are generated.

Upon reception of MAC flush messages (regardless the type) SR-Series PE will take following actions:

- Clears FDB entries of all indicated VPLS services conforming the definition.
- Propagates the message (preserving the type) to all LDP peers, if “propagate-mac-flush” flag is enabled at corresponding VPLS level.

The flush-all-but-mine message is generated under following conditions:

- The flush-all-but-mine message is received from LDP peer and propagate-mac-flush flag is enabled. The message is sent to all LDP peers in the context of VPLS service it was received in.
- TCN message in a context of STP instance is received. The flush-all-but-mine message is sent to all LDP-peers connected with spoke and mesh SDPs in a context of VPLS service controlled by the given STP instance (based on mVPLS definition). If all LDP peers are in the STP domain, i.e. the mVPLS and the uVPLS both have the same topology, the router will not send any flush-all-but-mine message. If the router has uVPLS LDP peers outside the STP domain, the router will send flush-all-but-mine messages to all its uVPLS peers.

NOTE: The 7750 will not send a withdrawal if the mVPLS does not contain a mesh SDP. A mesh SDP must be configured in the mVPLS to send withdrawals.
Flush-all-but-mine message is generated when switch over between spoke SDPs of the same endpoint occurs. The message is sent to LDP peer connected through newly active spoke SDP.

The flush-mine message is generated under following conditions:

- The flush-mine message is received from LDP peer and “propagate-mac-flush” flag is enabled. The message is sent to all LDP peers in the context of VPLS service it was received.
- The flush-mine message is generated when on a SAP or SDP transition from operationally up to an operationally down state and send-flush-on-failure flag is enabled in the context of the given VPLS service. The message is sent to all LDP peers connected in the context of the given VPLS service. The send-flush-on-failure flag is blocked in mVPLS and is only allowed to be configured in a VPLS service managed by mVPLS. This is to prevent that both messages are sent at the same time.
- The flush-mine message is generated when on a MC-LAG SAP or MC-APS SAP transition from an operationally up state to an operationally down state. The message is sent to all LDP peers connected in the context of the given VPLS service.
- The flush-mine message is generated when on a MC-RING SAP transition from operationally up to an operationally down state or when MC-RING SAP transitions to slave state. The message is sent to all LDP peers connected in the context of the given VPLS service.
Figure 94: Dual Homed CE Connection to VPLS

Figure 94 illustrates a dual-homed connection to VPLS service (PE-A, PE-B, PE-C, PE-D) and operation in case of link failure (between PE-C and L2-B). Upon detection of a link failure PE-C will send MAC-Address-Withdraw messages, which will indicate to all LDP peers that they should flush all MAC addresses learned from PE-C. This will lead that to a broadcasting of packets addressing affected hosts and re-learning process in case an alternative route exists.

Note that the message described here is different than the message described in draft-ietf-l2vpn-vpls-ldp-xx.txt, Virtual Private LAN Services over MPLS. The difference is in the interpretation and action performed in the receiving PE. According the draft definition, upon receipt of a MAC-withdraw message, all MAC addresses, except the ones learned from the source PE, are flushed. This section specifies that all MAC addresses learned from the source are flushed. This message has been implemented as an LDP address message with vendor-specific type, length, value (TLV), and is called the flush-all-from-ME message.
The draft definition message is currently used in management VPLS which is using RSTP for recovering from failures in Layer 2 topologies. The mechanism described in this document represent an alternative solution.

The advantage of this approach (as compared to RSTP based methods) is that only MAC-affected addresses are flushed and not the full forwarding database. While this method does not provide a mechanism to secure alternative loop-free topology, the convergence time is dependent on the speed of the given CE device will open alternative link (L2-B switch in Figure 94) as well as on the speed PE routers will flush their FDB.

In addition, this mechanism is effective only if PE and CE are directly connected (no hub or bridge) as it reacts to physical failure of the link.

---

**MC-Ring and VPLS**

The use of multi-chassis ring control in a combination with the plain VPLS SAP is supported FDB in individual ring nodes in case of the link (or ring node) failure cannot be cleared.

This combination is not easily blocked in the CLI. If configured, the combination may be functional but the switchover times will be proportional to MAC aging in individual ring nodes and/or to relearning rate due to downstream traffic.

Redundant plain VPLS access in ring configurations, therefore, exclude corresponding SAPs from the multi-chassis ring operation. Configurations such as mVPLS can be applied.
The ACL next-hop for VPLS feature enables an ACL that has a forward next-hop SAP or SDP action specified to be used in a VPLS service to direct traffic with specific match criteria to a SAP or SDP. This allows traffic destined to the same gateway to be split and forwarded differently based on the ACL.

Policy routing is a popular tool used to direct traffic in Layer 3 networks. As Layer 2 VPNs become more popular, especially in network aggregation, policy forwarding is required. Many providers are using methods such as DPI servers, transparent firewalls or Intrusion Detection/Prevention Systems (IDS/IPS). Since these devices are bandwidth limited providers want to limit traffic forwarded through them. A mechanism is required to direct some traffic coming from a SAP to the DPI without learning and other traffic coming from the same SAP directly to the gateway uplink based learning. This feature will allow the provider to create a filter that will forward packets to a specific SAP or SDP. The packets are then forwarded to the destination SAP regardless of learned destination or lack thereof. The SAP can either terminate a Layer 2 firewall, deep packet inspection (DPI) directly or may be configured to be part of a cross connect bridge into another service. This will be useful when running the DPI remotely using VLLs. If an SDP is used the provider can terminate it in a remote VPLS or VLL service where the firewall is connected. The filter can be configured under a SAP or SDP in a VPLS service. All packets (unicast, multicast, broadcast and unknown) can be delivered to the destination SAP/SDP.

The filter may be associated SAPs/SDPs belonging to a VPLS service only if all actions in the ACL forward to SAPs/SDPs that are within the context of that VPLS. Other services do not support this feature. An ACL that contains this feature is allowed but the system will drop any packet that matches an entry with this action.
SDP Statistics for VPLS and VLL Services

The simple three-node network described in Figure 96 shows two MPLS SDPs and one GRE SDP defined between the nodes. These SDPs connect VPLS1 and VPLS2 instances that are defined in the three nodes. With this feature the operator will have local CLI based as well as SNMP based statistics collection for each VC used in the SDPs. This will allow for traffic management of tunnel usage by the different services and with aggregation the total tunnel usage.

SDP statistics allow providers to bill customers on a per-SDP per-byte basis. This destination-based billing model is can be used by providers with a variety of circuit types and have different costs associated with the circuits. An accounting file allows the collection of statistics in a bulk manner.
BGP Auto-Discovery for LDP VPLS

BGP Auto Discovery (BGP AD) for LDP VPLS is a framework for automatically discovering the endpoints of a Layer 2 VPN offering an operational model similar to that of an IP VPN. This allows carriers to leverage existing network elements and functions, including but not limited to, route reflectors and BGP policies to control the VPLS topology.

BGP AD is an excellent complement to an already established and well deployed Layer 2 VPN signaling mechanism target LDP providing one touch provisioning for LDP VPLS where all the related PEs are discovered automatically. The service provider may make use of existing BGP policies to regulate the exchanges between PEs in the same, or in different, autonomous system (AS) domains. The addition of BGP AD procedures does not require carriers to uproot their existing VPLS deployments and to change the signaling protocol.

BGP AD Overview

The BGP protocol establishes neighbor relationships between configured peers. An open message is sent after the completion of the three-way TCP handshake. This open message contains information about the BGP peer sending the message. This message contains Autonomous System Number (ASN), BGP version, timer information and operational parameters, including capabilities. The capabilities of a peer are exchanged using two numerical values: the Address Family Identifier (AFI) and Subsequent Address Family Identifier (SAFI). These numbers are allocated by the Internet Assigned Numbers Authority (IANA). BGP AD uses AFI 65 (L2VPN) and SAFI 25 (BGP VPLS). The complete list of allocations may be found at: http://www.iana.org/assignments/address-family-numbers and SAFI http://www.iana.org/assignments/safi-namespace.

Information Model

Following the establishment of the peer relationship, the discovery process begins as soon as a new VPLS service instance is provisioned on the PE.

Two VPLS identifiers are used to indicate the VPLS membership and the individual VPLS instance:

- VPLS-ID — Membership information, unique network wide identifier; same value assigned for all VPLS switch instances (VSi)s belonging to the same VPLS; encodable and carried as a BGP extended community in one of the following formats:
  - A two-octet AS specific extended community
  - An IPv4 address specific extended community
VPLS Features

- **VSI-ID**— The unique identifier for each individual VSI, built by concatenating a route distinguisher (RD) with a 4 bytes identifier (usually the system IP of the VPLS PE); encoded and carried in the corresponding BGP NLRI.

In order to advertise this information, BGP AD employs a simplified version of the BGP VPLS NLRI where just the RD and the next 4 bytes are used to identify the VPLS instance. There is no need for Label Block and Label Size fields as T-LDP will take care of signaling the service labels later on.

The format of the BGP AD NLRI is very similar with the one used for IP VPN as depicted in Figure 97. The system IP may be used for the last 4 bytes of the VSI ID further simplifying the addressing and the provisioning process.

<table>
<thead>
<tr>
<th><strong>BGP AD NLRI Usage</strong></th>
<th><strong>IP VPN NLRI Usage</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Route Distinquisher (8 Octets)</td>
<td>Route Distinquisher (8 Octets)</td>
</tr>
<tr>
<td>VSI id (4) (IP Prefix)</td>
<td>IP Prefix</td>
</tr>
</tbody>
</table>

**Figure 97: BGP AD NLRI versus IP VPN NLRI**

Network Layer Reachability Information (NLRI) is exchanged between BGP peers indicating how to reach prefixes. The NLRI is used in the Layer 2 VPN case to tell PE peers how to reach the VSI rather than specific prefixes. The advertisement includes the BGP next hop and a route target (RT). The BGP next hop indicates the VSI location and is used in the next step to determine which signaling session is used for pseudowire signaling. The RT, also coded as an extended community, can be used to build a VPLS full mesh or a HVPLS hierarchy through the use of BGP import/export policies.

BGP is only used to discover VPN endpoints and the corresponding far end PEs. It is not used to signal the pseudowire labels. This task remains the responsibility of targeted-LDP (T-LDP).
FEC Element for T-LDP Signaling

Two LDP FEC elements are defined in RFC 4447, *PW Setup & Maintenance Using LDP*. The original pseudowire-ID FEC element 128 (0x80) employs a 32-bit field to identify the virtual circuit ID and it was used extensively in the initial VPWS and VPLS deployments. The simple format is easy to understand but it does not provide the required information model for BGP auto-discovery function. In order to support BGP AD and other new applications a new Layer 2 FEC element, the generalized FEC (0x81) is required.

The generalized pseudowire-ID FEC element has been designed for auto discovery applications. It provides a field, the address group identifier (AGI), that is used to signal the membership information from the VPLS-ID. Separate address fields are provided for the source and target address associated with the VPLS endpoints called the Source Attachment Individual Identifier (SAII) and respectively, Target Attachment Individual Identifier (TAII). These fields carry the VSI ID values for the two instances that are to be connected through the signaled pseudowire.

The detailed format for FEC 129 is depicted in Figure 98.

```
0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Gen PWid (0x81) | C | PW Type             | PW info Length |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| AGI Type      | Length | Value               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
~                    AGI  Value (contd.)                     ~
|                                                            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| AII Type      | Length | Value               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
~                   SAII  Value (contd.)                      ~
|                                                            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| AII Type      | Length | Value               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
~                   TAII Value (contd.)                      ~
|                                                            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

*Figure 98: Generalized Pseudowire-ID FEC Element*
Each of the FEC fields are designed as a sub-TLV equipped with its own type and length providing support for new applications. To accommodate the BGP AD information model the following FEC formats are used:

- AGI (type 1) is identical in format and content with the BGP extended community attribute used to carry the VPLS-ID value.
- Source AII (type 1) is a 4 bytes value destined to carry the local VSI-id (outgoing NLRI minus the RD).
- Target AII (type 1) is a 4 bytes value destined to carry the remote VSI-ID (incoming NLRI minus the RD).

**BGP-AD and Target LDP (T-LDP) Interaction**

BGP is responsible for discovering the location of VSIs that share the same VPLS membership. LDP protocol is responsible for setting up the pseudowire infrastructure between the related VSIs by exchanging service specific labels between them.

Once the local VPLS information is provisioned in the local PE, the related PEs participating in the same VPLS are identified through BGP AD exchanges. A list of far-end PEs is generated and will trigger the creation, if required, of the necessary T-LDP sessions to these PEs and the exchange of the service specific VPN labels. The steps for the BGP AD discovery process and LDP session establishment and label exchange are shown in Figure 99.
Figure 99: BGP-AD and T-LDP Interaction

Key:

1. Establish I-BGP connectivity RR.
2. Configure VPN (10) on edge node (PE3).
3. Announce VPN to RR using BGP-AD.
4. Send membership update to each client of the cluster.
5. LDP exchange or inbound FEC filtering (IFF) of non-match or VPLS down.
6. Configure VPN (10) on edge node (PE2).
7. Announce VPN to RR using BGP-AD.
8. Send membership update to each client of the cluster.
9. LDP exchange or inbound FEC filtering (IFF) of non-match or VPLS down.
10. Complete LDP bidirectional pseudowire establishment FEC 129.
SDP Usage

Service Access Points (SAP) are linked to transport tunnels using Service Distribution Points (SDP). The service architecture allows services to be abstracted from the transport network.

MPLS transport tunnels are signaled using the Resource Reservation Protocol (RSVP-TE) or by the Label Distribution Protocol (LDP). The capability to automatically create an SDP only exists for LDP based transport tunnels. Using a manually provisioned SDP is available for both RSVP-TE and LDP transport tunnels. Refer to the appropriate OS MPLS Guide for more information about MPLS, LDP, and RSVP.

Automatic Creation of SDPs

When BGP AD is used for LDP VPLS and LDP is used as the transport tunnel there is no requirement to manually create an SDP. The LDP SDP can be automatically instantiated using the information advertised by BGP AD. This simplifies the configuration on the service node.

Enabling LDP on the IP interfaces connecting all nodes between the ingress and the egress builds transport tunnels based on the best IGP path. LDP bindings are automatically built and stored in the hardware. These entries contain an MPLS label pointing to the best next hop along the best path toward the destination.

When two endpoints need to connect and no SDP exists, a new SDP will automatically be constructed. New services added between two endpoints that already have an automatically created SDP will be immediately used. No new SDP will be constructed. The far-end information is gleaned from the BGP next hop information in the NLRI. When services are withdrawn with a BGP_Unreach_NLRI, the automatically established SDP will remain up as long as at least one service is connected between those endpoints. An automatically created SDP will be removed and the resources released when the only or last service is removed.

Manually Provisioned SDP

The carrier is required to manually provision the SDP if they create transport tunnels using RSVP-TE. Operators have the option to choose a manually configured SDP if they use LDP as the tunnel signaling protocol. The functionality is the same regardless of the signaling protocol.

Creating a BGP AD enabled VPLS service on an ingress node with the manually provisioned SDP option causes the Tunnel Manager to search for an existing SDP that connects to the far-end PE. The far-end IP information is gleaned from the BGP next hop information in the NLRI. If a single SDP exists to that PE, it is used. If no SDP is established between the two endpoints, the service will remain down until a manually configured SDP becomes active.
When multiple SDPs exist between two endpoints, the tunnel manager will select the appropriate SDP. The algorithm will prefer SDPs with the best (lower) metric. Should there be multiple SDPs with equal metrics, the operational state of the SDPs with the best metric will be considered. If the operational state is the same, the SDP with the higher sdp-id will be used. If an SDP with a preferred metric is found with an operational state that is not active, the tunnel manager will flag it as ineligible and restart the algorithm.

**Automatic Instantiation of Pseudowires (SDP Bindings)**

The choice of manual or auto provisioned SDPs has limited impact on the amount of required provisioning. Most of the savings are achieved through the automatic instantiation of the pseudowire infrastructure (SDP bindings). This is achieved for every auto-discovered VSIs through the use of the pseudowire template concept. Each VPLS service that uses BGP AD contains the “pw-template-binding” option defining specific layer 2 VPN parameters. This command references a “pw-template” which defines the pseudowire parameters. The same “pw-template” may be referenced by multiple VPLS services. As a result, changes to these pseudowire templates have to be treated with great care as they may impact many customers at once.

The Alcatel-Lucent implementation provides for safe handling of pseudowire templates. Changes to the pseudowire templates are not automatically propagated. Tools are provided to evaluate and distribute the changes. The following command is used to distribute changes to a “pw-template” at the service level to one or all services that use that template.

```
PERs-4# tools perform service id 300 eval-pw-template 1 allow-service-impact
```

If the service ID is omitted, then all services will be updated. The type of change made to the “pw-template” will influence how the service is impacted.

1. Adding or removing a split-horizon-group will cause the router to destroy the original object and recreate using the new value.

2. Changing parameters in the `vc-type {ether | vlan}` command requires LDP to re-signal the labels.

Both of these changes are service affecting. Other changes will not be service affecting.
Mixing Statically Configured and Auto-Discovered Pseudowires in a VPLS

The services implementation allows for manually provisioned and auto-discovered pseudowire (SDP bindings) to coexist in the same VPLS instance (for example, both FEC128 and FEC 129 are supported). This allows for gradual introduction of auto discovery into an existing VPLS deployment.

As FEC 128 and 129 represent different addressing schemes, it is important to make sure that only one is used at any point in time between the same two VPLS instances. Otherwise, both pseudowires may become active causing a loop that might adversely impact the correct functioning of the service. It is recommended that FEC128 pseudowire be disabled as soon as the FEC129 addressing scheme is introduced in a portion of the network. Alternatively, RSTP may be used during the migration as a safety mechanism to provide additional protection against operational errors.

Resiliency Schemes

The use of BGP AD on the network side, or in the backbone, does not affect the different resiliency schemes Alcatel-Lucent has developed in the access network. This means that both Multi-Chassis Link Aggregation (MC-LAG) and Management-VPLS (M-VPLS) can still be used.

BGP AD may coexist with Hierarchical-VPLS (H-VPLS) resiliency schemes (for example, dual homed MTU-s devices to different PE-rs nodes) using existing methods (M-VPLS and statically configured Active/Standby pseudowire endpoint).

If provisioned SDPs are used by BGP AD, M-VPLS may be employed to provide loop avoidance. However, it is currently not possible to auto-discover active/standby pseudowires and to instantiate the related endpoint.
BGP VPLS

The Alcatel-Lucent BGP VPLS solution, compliant with RFC 4761, *Virtual Private LAN Service (VPLS) Using BGP for Auto-Discovery and Signaling*, is described in this section.

**Figure 100: BGP VPLS Solution**

*Figure 100* depicts the service representation for BGP VPLS mesh. The major BGP VPLS components and the deltas from LDP VPLS with BGP AD are explained below:

- Data plane is identical with the LDP VPLS solution: for example, VPLS instances interconnected by pseudowire mesh. Split horizon groups may be used for loop avoidance between pseudowires.
- Addressing is based on two (2) bytes VE ID assigned to the VPLS instance.
  - BGP-AD for LDP VPLS: 4 bytes VSI-ID (system IP) identifies the VPLS instance.
- The target VPLS instance is identified by the Route Target (RT) contained in the MP-BGP advertisement (extended community attribute).
  - BGP-AD: a new MP-BGP extended community is used to identify the VPLS. RT is used for topology control.
- Auto-discovery is MP-BGP based. Same AFI, SAFI used as for LDP VPLS BGP-AD.
  - The BGP VPLS updates are distinguished from the BGP-AD ones based on the value of the NLRI prefix length: 17 bytes for BGP VPLS, 12 bytes for BGP-AD.
  - BGP-AD NLRI is shorter since there is no need to carry pseudowire label information as T-LDP does the pseudowire signaling for LDP VPLS.
- Pseudowire label signaling is MP-BGP based. As a result the BGP NLRI content includes also label related information – for example, block offset, block size and label base.
  - LDP VPLS: target LDP (T-LDP) is used for signaling the pseudowire service label.
The Layer 2 extended community proposed in RFC 4761 is used to signal pseudowire characteristics – for example, VPLS status, control word, sequencing.

### Pseudowire Signaling Details

The pseudowire is setup using the following NLRI fields:

- **VE Block offset (VBO):** used to define for each VE-ID set the NLRI is targeted:
  - \( \text{VBO} = n \times \text{VBS} + 1 \); for VBS=8 this results in 1, 9, 17, 25, …
  - Targeted Remote VE-IDs are from VBO to \((\text{VBO} + \text{VBS} - 1)\)

- **VE Block size (VBS):** defines how many contiguous pseudowire labels are reserved starting with the Label Base.
  - Alcatel-Lucent implementation uses always a value of eight (8).

- **Label Base (LB):** local allocated label base.
  - The next eight (8) labels allocated for remote PEs.

This BGP update is telling the other PE(s) that accept the RT: “in order to reach me (VE-ID = x) use a pseudowire label of LB + VE-ID – VBO using the BGP NLRI for which VBO <= local VE-ID < VBO + VBS.

Here is an example of how this algorithm works assuming PE1 has VE-ID 7 configured:

- PE1 founds a Label Block of eight (8) consecutive labels available, starting with LB = 1000
- PE1 then starts sending BGP Update with pseudowire information of \((\text{VBO} = 1, \text{VBS}=8, \text{LB}=1000)\) in the NLRI.
- This pseudowire information will be accepted by all participating PEs with VE-IDs from one (1) to eight (8).
- Each of the receiving PEs will use the pseudowire label = LB +VE-ID-VBO to send traffic back to the originator PE. For example VE-ID 2 will use pseudowire label 1001.

Assuming that VE-ID = 10 is configured in another PE4 the following procedure applies:

- PE4 sends BGP Update with the new VE-ID in the network that will be received by all the other participating PEs, including PE1.
- PE1 upon reception will generate another label block of 8 labels for the VBO = 9. For example the initial PE will create now new pseudowire signaling information of \((\text{VBO} = 9, \text{VBS} = 8, \text{LB} = 3000)\) and insert it in a new NLRI and BGP Update that is sent in the network.
This new NLRI will be used by the VE-ID from 9 to 16 to establish pseudowires back to
the originator PE1. For example PE4 with VE-ID 10 will use pseudowire label 3001 to
send VPLS traffic back to PE1.

The PEs owning the set of VE-IDs from 1 to 8 will ignore this NLRI.

In addition to the pseudowire label information, the **Layer2 Info Extended Community** attribute
must be included in the BGP Update for BGP VPLS to signal the attributes of all the pseudowires
that converge towards the originator VPLS PE.

The format is described below:

```
+------------------------------------+
| Extended community type (2 octets) |
+------------------------------------+
| Encaps Type (1 octet)              |
+------------------------------------+
| Control Flags (1 octet)            |
+------------------------------------+
| Layer-2 MTU (2 octet)              |
+------------------------------------+
| Reserved (2 octets)                |
+------------------------------------+
```

The meaning of the fields:

- **Extended community type** – the value allocated by IANA for this attribute is 0x800A
- **Encaps Type** - Encapsulation type, identifies the type of pseudowire encapsulation. The
  only value used by BGP VPLS is 19 (13 in HEX). This value identifies the encapsulation
to be used for pseudowire instantiated through BGP Signaling which is the same as the
one used for Ethernet pseudowire type in regular VPLS. There is no support for an
  equivalent Ethernet VLAN pseudowire in BGP VPLS in BGP signaling.
- **Control Flags** - control information regarding the pseudowires, see below for details.
- **Layer-2 MTU** is the Maximum Transmission Unit to be used on the pseudowires.
- **Reserved** – this field is reserved and must be set to zero and ignored on reception except
  where it is used for VPLS preference.

The detailed format for the Control Flags bit vector is described below:

```
0 1 2 3 4 5 6 7
+----------------+
|D| MBZ     |C|S| (MBZ = MUST Be Zero) |
+----------------+
```

The following bits in the Control Flags are defined:
VPLS Features

- S, sequenced delivery of frames MUST or MUST NOT be used when sending VPLS packets to this PE, depending on whether S is 1 or 0, respectively.
- C, a Control word MUST or MUST NOT be present when sending VPLS packets to this PE, depending on whether C is 1 or 0, respectively. By default, Alcatel-Lucent implementation uses value 0.
- MBZ, Must Be Zero bits, set to zero when sending and ignored when receiving.
- D indicates the status of the whole VPLS instance (VSI); D=0 if Admin & Operational status are up, D=1 otherwise.

Here are the events that set the D-bit to 1 to indicate VSI down status in BGP update message sent out from a PE:

- local VSI is shutdown administratively using the “config service vpls shutdown”
- all the related endpoints (SAPs or LDP pseudowires) are down
- There are no related endpoints (SAPs or LDP pseudowires) configured yet in the VSI
  → The idea is to save the core bandwidth by not establishing the BGP pseudowires to an empty VSI
- Upon reception of a BGP Update message with D-bit set to 1 all the receiving VPLS PEs must mark related pseudowires as down.

The following events do not set the D-bit to 1:

- The local VSI is deleted — a BGP Update with unreach-NLRI is sent out. Upon reception all remote VPLS PEs must remove the related pseudowires and BGP routes.
- If the local SDP goes down, only the BGP pseudowire(s) mapped to that SDP goes down. There is no BGP-update sent.

---

Supported VPLS Features

BGP VPLS just added support for a new type of pseudowire signaling based on MP-BGP. It is based on the existing VPLS instance hence it inherited all the existing Ethernet switching functions. Here are some of the most important existing VPLS features ported also to BGP VPLS:

- VPLS data plane features: for example FIB management, SAPs, LAG access, BUM rate limiting.
- MPLS tunneling: LDP, LDP over RSVP-TE, RSVP-TE, MP-BGP based on RFC3107 (Option C solution)
- HVPLS topologies, Hub and Spoke traffic distribution
- Coexists with LDP VPLS (with or without BGP-AD) in the same VPLS instance.
  → LDP, BGP-signaling should operate in disjoint domains to simplify loop avoidance
• Coexist with BGP-based multi-homing.
• BGP VPLS is supported as the control plane for BVPLS.
• Supports IGMP/PIM snooping
• Support for High Availability is provided
• Ethernet Service OAM toolset is supported: IEEE 802.1ag, Y.1731.
  → Not supported OAM features: CPE Ping, MAC trace/ping/populate/purge.
• Support for RSVP and LSP P2MP LSP for VPLS/B-VPLS BUM
BGP Multi-Homing for VPLS

This section describes BGP based procedures for electing a designated forwarder among the set of PEs that are multi-homed to a customer site. Only the local PEs are actively participating in the selection algorithm. The PE(s) remote from the dual homed CE are not required to participate in the designated forwarding election for a remote dual-homed CE.

The main components of the BGP based multi-homing solution for VPLS are:

- Provisioning model
- MP-BGP procedures
- Designated Forwarder Election
- Blackhole avoidance – indicating the designated forwarder change towards the core PEs and access PEs or CEs
- The interaction with pseudowire signaling (BGP/LDP)

Figure 101: BGP Multi-Homing for VPLS

Figure 101 depicts the VPLS using BGP Multi-homing for the case of multi-homed CEs. Although the picture depicts the case of a pseudowire infrastructure signaled with LDP for a LDP VPLS using BGP-AD for discovery, the procedures are identical for BGP VPLS or for a mix of BGP and LDP signaled pseudowires.
Information Model and Required Extensions to L2VPN NLRI

VPLS Multi-homing using BGP-MP expands on the BGP AD and BGP VPLS provisioning model. The addressing for the Multi-homed site is still independent from the addressing for the base VSI (VSI-ID or respectively VE-ID). Every multi-homed CE is represented in the VPLS context through a site-id, which is the same on the local PEs. The site-id is unique within the scope of a VPLS. It serves to differentiate between the multi-homed CEs connected to the same VPLS Instance (VSI). For example, in Figure 102, CE5 will be assigned the same site-id on both PE1 and PE4. For the same VPLS instance though, different SITE-IDs are assigned for multi-homed CE5 and CE6: for example, site id 5 is assigned for CE5 and site id 6 is assigned for CE6. The single-homed CEs (CE1, 2, 3 and 4) do not require allocation of a multi-homed site-id. They are associated with the addressing for the base VSI, either VSI-ID or VE-ID.

The new information model required changes to the BGP usage of the NLRI for VPLS. The extended MH NLRI for Multi-Homed VPLS is compared with the BGP AD and BGP VPLS NLRIIs in Figure 102.

![Figure 102: BGP MH-NLRI for VPLS Multi-Homing](attachment:image.png)

The BGP VPLS NLRI described in RFC 4761 is used to carry a two (2) byte site-ID that identifies the MH Site. The last seven (7) bytes of the BGP VPLS NLRI used to instantiate the pseudowire are not used for BGP-MH and are ZEROed out. This NLRI format translates into the following processing path in the receiving VPLS PE:

- BGP VPLS PE: no Label information means there is no need to setup up a BGP pseudowire
- BGP AD for LDP VPLS: length =17 indicates a BGP VPLS NLRI that does not require any pseudowire LDP Signaling.

The processing procedures described in this section start from the above identification of the BGP Update as not destined for pseudowire signaling.
The RD ensures the NLRIs associated with a certain site-id on different PEs are seen as different by any of the intermediate BGP nodes (RRs) on the path between the multi-homed PEs. In other words, different RDs must be used on the MH PEs every time an RR or an ASBR is involved to guarantee the MH NLRIs reach the PEs involved in VPLS MH.

The L2-Info extended community from RFC 4761 is used in the BGP update for MH NLRI to initiate a MAC flush for blackhole avoidance to indicate the operational and admin status for the MH Site or the DF election status.

After the pseudowire infrastructure between VSIs is built using either RFC 4762, *Virtual Private LAN Service (VPLS) Using Label Distribution Protocol (LDP) Signaling*, or RFC 4761 procedures or a mix of pseudowire Signaling procedure, on activation of a multi-homed site, an election algorithm must be run on the local and remote PEs to determine which site will be the designated forwarder (DF). The end result is that all the related MH sites in a VPLS will be placed in standby except for the site selected as DF. Alcatel-Lucent BGP-based multi-homing solution uses the DF election procedure described in the IETF working group document *draft-ietf-l2vpn-vpls-multihoming*. The implementation allows the use of BGP Local Preference and the received VPLS preference but does not support setting the VPLS preference to a non-zero value.

The implementation allows the use of BGP Local Preference and the received VPLS preference, but does not support setting the VPLS preference to a non-zero value.

---

**Supported Services and Multi-Homing Objects**

This feature is supported for the following services:

- LDP VPLS with or without BGP-AD
- BGP VPLS
- mix of the above
- PBB BVPLS on BCB
- PBB I-VPLS (see section BGP Multi-homing for I-VPLS on page 995)

The following access objects can be associated with MH SITE:

- SAPs
- SDP bindings (pseudowire object), both mesh SDP and spoke SDP
- Split Horizon Group
  - Under the SHG we can associate either one or multiple of the following objects: SAP(s), pseudowires (BGP VPLS, BGP-AD, provisioned and LDP signaled spoke SDP and mesh SDP)
Blackhole Avoidance

Blackholing refers to the forwarding of frames to a PE that is no longer carrying the designated forwarder. This could happen for traffic from:

- Core PE participating in the main VPLS
- Customer Edge devices (CEs)
- Access PEs - pseudowires between them and the MH PEs are associated with MH Sites

Changes in DF election results or MH site status must be detected by all of the above network elements to provide for Blackhole Avoidance.

MAC Flush to the Core PEs

Assuming there is a transition of the existing DF to non-DF status. The PE that owns the MH site experiencing this transition will generate a MAC flush-all-from-me (negative MAC flush) towards the related core PEs. Upon reception, the remote PEs will flush all the MACs learned from the MH PE.

MAC flush-all-from-me indication is sent using the following core mechanisms:

- For LDP VPLS running between core PEs, existing LDP MAC flush will be used.
- For pseudowire signaled with BGP VPLS, MAC flush will be provided implicitly using the L2-Info Extended community to indicate a transition of the active MH-site: for example the attached object(s) going down or more generically, the entire site going from Designated Forwarder (DF) to non-DF.
- Note that double flushing will not happen as it is expected that between any pair of PEs it will exist only one type of pseudowires – either BGP or LDP pseudowire but not both.

Indicating non-DF status towards the access PE or CE

For the CEs or access PEs support is provided for indicating the blocking of the MH site using the following procedures:

- For MH Access PE running LDP pseudowires the LDP standby-status is sent to all LDP pseudowires.
- For MH CEs site de-activation is linked to a CCM failure on a SAP that has a down MEP configured.
BGP Multi-Homing for VPLS Inter-Domain Resiliency

BGP MH for VPLS can be used to provide resiliency between different VPLS domains. An example of a Multi-Homing topology is depicted in Figure 103.

Figure 103: BGP MH Used in an HVPLS Topology

LDP VPLS domains are interconnected using a core VPLS domain either BGP VPLS or LDP VPLS. The gateway PEs, for example PE2 and PE3, are running BGP multi-homing where one MH site is assigned to each of the pseudowires connecting the access PE, PE7, and PE8 in this example.

Alternatively, one may choose to associate the MH site to multiple access pseudowires using an access SHG. The `config>service>vpls>site>failed-threshold` command can be used to indicate the number of pseudowire failures that are required for the MH site to be declared down.
Multicast-Aware VPLS

VPLS is a Layer 2 service, hence, multicast and broadcast frames are normally flooded in a VPLS. Broadcast frames are targeted to all receivers. However, for IP multicast, normally for a multicast group, only some receivers in the VPLS are interested. Flooding to all sites can cause wasted network bandwidth and unnecessary replication on the ingress PE router.

In order to improve this condition, VPLS is IP multicast aware so it forwards IP multicast traffic based on multicast states.

PIM Snooping for VPLS

PIM snooping for VPLS allows a VPLS PE router to build multicast states by snooping PIM protocol packets that are sent over the VPLS. The VPLS PE then forwards multicast traffic based on the multicast states. When all receivers in a VPLS are IP multicast routers running PIM, multicast forwarding in the VPLS is efficient when PIM snooping for VPLS is enabled.

Because of PIM join/prune suppression, in order to make PIM snooping operate over VPLS pseudowires, two options are available, plain PIM snooping and PIM proxy. PIM proxy is the default behavior when PIM snooping is enabled for a VPLS.

Plain PIM Snooping

In plain PIM snooping configuration, VPLS PE routers only snoop, PIM messages generated on their own. Join/prune suppression must be disabled on CE routers.

When plain PIM snooping is configured, a VPLS PE router detects a condition where join/prune suppression is not disabled on one or multiple CE routers, the PE router should put PIM snooping into PIM proxy state. A trap is generated which reports the condition to the operator and is logged to syslog. If the condition changes, for example, join/prune suppression was disabled on CE routers, the PE reverts to plain PIM snooping state. A trap is generated and is logged to syslog.
PIM Proxy

For PIM proxy configurations, VPLS PE routers perform the following:

- Snoop hellos and flood hellos in fast data path.
- Consume join/prune messages from CE routers.
- Generate join/prune messages upstream using the IP address of one of the downstream CE routers.
- Run an upstream PIM state machine to determine whether a join/prune message should be sent upstream.
- When LDP multicast state distribution is enabled, generate PIM messages for LDP.

Join/prune suppression is not required to be disabled on CE routers, but it requires all PEs in the VPLS to have PIM proxy enabled. Otherwise, CEs behind the PE(s) that do not have PIM proxy enabled may not be able to get multicast traffic that they are interested in if they have join/prune suppression enabled.

When PIM proxy is enabled, but a VPLS PE router detects a condition where join/prune suppression is disabled on all CE routers, the PE router put PIM proxy into a plain PIM snooping state to improve efficiency. A trap is generated to report the scenario to the operator and is logged to syslog. If the condition changes, for example, join/prune suppression enabled on a CE router, PIM proxy is placed back into operational state. Again, a trap is generated to report the condition to the operator and is logged to syslog.
Multicast Listener Discovery (MLD) Snooping and MAC-Based Multicast Forwarding

VPLS-based transport is a popular architecture as it better handles IPv6 multicast on the transport configurations for those backbones who use IPv6 instead of IPv4.

The VPLS based transport architecture combines MLD snooping and MAC based multicast forwarding.

MLD Snooping

MLD snooping is basically a IPv6 version of IGMP snooping. The guidelines and procedures are similar to IGMP snooping as well.

MAC-Based IPv6 Multicast Forwarding

IPv6 multicast address to MAC address mapping — Ethernet MAC addresses in the range of 33-33-00-00-00-00 to 33-33-FF-FF-FF-FF are reserved for IPv6 multicast. To map an IPv6 multicast address to a MAC-layer multicast address, the low order 32 bits of the IPv6 multicast address are mapped directly to the low order 32 bits in the MAC-layer multicast address.

IPv6 multicast forwarding entries — IPv6 multicast snooping forwarding entries are based on MAC addresses, while native IPv6 multicast forwarding entries are based on IPv6 addresses. Thus, when both MLD snooping and native IPv6 multicast are enabled on the same device, both formats are supported on the same XMA, although they are used for different services.
PIM and IGMP Snooping Interaction

This section describes how to handle the scenario where IGMP snooping and PIM snooping are both enabled for the same VPLS.

When both PIM snooping and IGMP snooping are enabled for a VPLS, multicast traffic is forwarded based on the combined multicast forwarding table.

VPLS Multicast-Aware High Availability Features

The following features are HA capable:

- Configuration redundancy — All the VPLS multicast-aware configurations can be synchronized to the standby CPM.
- Local snooping states as well as states distributed by LDP can be synchronized to the standby CPM.
- Operational states can also be synchronized, for example, the operational state of PIM proxy.
RSVP and LDP P2MP LSP for Forwarding VPLS/B-VPLS BUM and IP Multicast Packets

This feature enables the use of a P2MP LSP as the default tree for forwarding Broadcast, Unicast unknown and Multicast (BUM) packets of a VPLS or B-VPLS instance. The P2MP LSP is referred to in this case as the Inclusive Provider Multicast Service Interface (I-PMSI).

When enabled, this feature relies on BGP Auto-Discovery (BGP-AD) or BGP-VPLS to discover the PE nodes participating in a given VPLS/B-VPLS instance. The BGP route contains the information required to signal both the point-to-point (P2P) PWs used for forwarding unicast known Ethernet frames and the RSVP P2MP LSP used to forward the BUM frames. The root node signals the P2MP LSP based on an LSP template associated with the I-PMSI at configuration time. The leaf node will join automatically the P2MP LSP which matches the I-PMSI tunnel information discovered via BGP.

If IGMP or PIM snooping are configured on the VPLS/B-VPLS instance, multicast packets matching a L2 multicast Forwarding Information Base (FIB) record will also be forwarded over the P2MP LSP.

The user enables the use of an RSVP P2MP LSP as the I-PMSI for forwarding Ethernet BUM and IP multicast packets in a VPLS/B-VPLS instance using the following commands:

```
config>service>vpls [b-vpls]>provider-tunnel>inclusive>rsvp>lsp-template p2mp-lsp-template-name
```

The user enables the use of an LDP P2MP LSP as the I-PMSI for forwarding Ethernet BUM and IP multicast packets in a VPLS instance using the following command:

```
config>service>vpls [b-vpls]>provider-tunnel>inclusive>mldp
```

After the user performs a ‘no shutdown’ under the context of the inclusive node and the expiration of a delay timer, BUM packets will be forwarded over an automatically signaled mLDP P2MP LSP or over an automatically signaled instance of the RSVP P2MP LSP specified in the LSP template.

The user can specify if the node is both root and leaf in the VPLS instance:

```
config>service>vpls [b-vpls]>provider-tunnel>inclusive>root-and-leaf
```

The `root-and-leaf` command is required; otherwise, this node will behave as a leaf only node by default. When the node is leaf only for the I-PMSI of type P2MP RSVP LSP, no PMSI Tunnel Attribute is included in BGP-AD route update messages and thus no RSVP P2MP LSP is signaled but the node can join RSVP P2MP LSP rooted at other PE nodes participating in this VPLS/B-VPLS service. Note that the user must still configure a LSP template even if the node is a leaf only. For the I-PMSI of type mLDP, the leaf-only node will join I-PMSI rooted at other nodes it
discovered but will not include a PMSI Tunnel Attribute in BGP route update messages. This way, a leaf only node will forward packets to other nodes in the VPLS/B-VPLS using the point-to-point spoke SDPs.

Note that BGP-AD (or BGP-VPLS) must have been enabled in this VPLS/B-VPLS instance or the execution of the ‘no shutdown” command under the context of the inclusive node is failed and the I-PMSI will not come up. A

Any change to the parameters of the I-PMSI, such as disabling the P2MP LSP type or changing the LSP template requires that the inclusive node be first shutdown. The LSP template is configured in MPLS.

If the P2MP LSP instance goes down, VPLS/B-VPLS immediately reverts the forwarding of BUM packets to the P2P PWs. The user can, however, restore at any time the forwarding of BUM packets over the P2P PWs by performing a ‘shutdown’ under the context of the inclusive node.

This feature is supported with VPLS, H-VPLS, B-VPLS and BGP-VPLS. It is not supported with I-VPLS and Routed VPLS.

The allow-ip-int-binding VPLS Flag

The allow-ip-int-binding flag on a VPLS service context is used to inform the system that the VPLS service is enabled for routing support. The system uses the setting of the flag as a key to determine what type of ports and which type of forwarding planes the VPLS service may span.

The system also uses the flag state to define which VPLS features are configurable on the VPLS service to prevent enabling a feature that is not supported when routing support is enabled.

Routed VPLS SAPs Only Supported on Standard Ethernet Ports

The allow-ip-int-binding flag is set (routing support enabled) on a VPLS/I-VPLS service. SAPs within the service can be created on standard Ethernet, HSMDA.

LAG Port Membership Constraints

If a LAG has a non-supported port type as a member, a SAP for the routing-enabled VPLS service cannot be created on the LAG. Once one or more routing enabled VPLS SAPs are associated with a LAG, a non-supported Ethernet port type cannot be added to the LAG membership.
**Routed VPLS Feature Restrictions**

When the `allow-ip-int-binding` flag is set on a VPLS service, the following features cannot be enabled (The flag also cannot be enabled while any of these features are applied to the VPLS service.):

- SAP ingress QoS policies applied to the VPLS SAPs cannot have MAC match criteria defined.
- SDPs used in spoke or mesh SDP bindings cannot be configured as GRE.
- The VPLS service type cannot be B-VPLS or M-VPLS and it cannot be an I-VPLS service bound to a B-VPLS context.
- MVR from Routed VPLS and to another SAP is not supported.
- Enhanced and Basic Subscriber Management (BSM) features.
- Network domain on SDP bindings.
- Per Service Hashing not supported
- No BGP-AD
- No BGP-VPLS
- IOM3+ cards only

Note: IES/VPRN Saps can be on non IOM3+ cards but traffic on them will not be forwarding on Routed VPLS/Routed I-VPLS

- No Time of Day accounting on Routed VPLS SAPs.
- No Ingress Queuing for Split-Horizon Groups
- No Multiple Virtual Router support

**Routed I-VPLS Feature Restrictions**

- No Multicast support
- No VC-VLAN on SDPs
- `force-qtag-forwarding` is Not supported
- No Control word on B-VPLS SDPs with Routed I-VPLS
- No Hash Label on B-VPLS SDPs with Routed I-VPLS
IES IP Interface VPLS Binding and Chassis Mode Interaction

It is possible to bind both IES and VPRN IP interfaces to a VPLS in chassis mode A. Chassis - mode D is not required.

VPRN IP Interface VPLS Binding and Forwarding Plane Constraints

When an IP interface within a VPRN service context is bound to a VPLS or an I-VPLS service name, all of the SAPs within the VPRN service context must be created on ports that are attached to FP2 forwarding planes or better. If a VPRN SAP is on a non-supported forwarding plane, the service name cannot be bound to the VPRN’s IP interface. Once an IP interface on the VPRN service is bound to a service name, a SAP on the VPRN service cannot be created on a port (or LAG) on an FP1 forwarding plane.

This restriction prevents a packet from entering the VPRN service on a port that cannot reach a routed VPLS next-hop.

Route Leaking Between Routing Contexts

While the system prevents a routing context from existing on FP1 based forwarding planes while a VPLS service is bound to the routing context, it is possible to create conditions using route leaking (importing or exporting routes using routing policies) where an FP1 based IP interface is asked to route to a routed VPLS next-hop. The system reacts to this condition by populating the next-hop in the FP1 forwarding plane with a null egress IP interface index. This causes any packets that are associated with that next-hop on an FP1 forwarding plane to be discarded. If ICMP destination unreachable messaging is enabled, unreachable messages will be sent.
**Ingress LAG and FP1 to Routed VPLS Discards**

If the chassis is connected by LAG to an upstream router and the LAG is split between FP1 and FP2 forwarding plane ports while routes have been shared between routing contexts, flows that are sent to the FP2 ports by the upstream router are capable of reaching a next-hop in a routed VPLS while flows going to the FP1 ports cannot.
IPv4 Multicast Routing Support

IPv4 multicast routing is supported when the source of the multicast stream is on the IP side of the routed VPLS service, and the multicast traffic is either flooded in the VPLS service or sent to IGMP clients. The IP interface supports the configuration of PIM and IGMP. When IGMP is configured on the IP interface, it is mandatory to enable. IGMP snooping in the VPLS service and to configure the associated IP interface to be both the PIM designated router and the IGMP querier in order that the multicast traffic is sent into the VPLS service, as IGMP joins are only propagated to the IP interface if it is the IGMP querier.

Figure 104: IPv4 Multicast with a Router VPLS service

An example scenario is shown in Figure 104. The IP multicast traffic entering the system is replicated to IP interfaces, two of which are part of an IES routed VPLS service. The IP multicast traffic is sent only to those SAPs/SDPs from which a corresponding IGMP join has been received as igmp-snooping is enabled in the VPLS services.

It is possible to configure PIM on the IP interface and have neighboring downstream PIM routers connecting via the VPLS, however, any multicast traffic will be flooded in the VPLS service.

If a multicast source was connected by a SAP/SDP into the VPLS service, any multicast traffic would be replicated within the VPLS service but would be dropped at the routed VPLS IP interface.
BGP Auto Discovery (BGP-AD) for Routed VPLS Support

BGP Auto Discovery (BGP-AD) for Routed VPLS is supported. BGP-AD for LDP VPLS is an already supported framework for automatically discovering the endpoints of a Layer 2 VPN offering an operational model similar to that of an IP VPN.
Routed VPLS Caveats

VPLS SAP Ingress IP Filter Override

When an IP Interface is attached to a VPLS or an I-VPLS service context, the VPLS SAP provisioned IP filter for ingress routed packets may be optionally overridden in order to provide special ingress filtering for routed packets. This allows different filtering for routed packets and non-routed packets. The filter override is defined on the IP interface bound to the VPLS service name. A separate override filter may be specified for IPv4 and IPv6 packet types.

If a filter for a given packet type (IPv4 or IPv6) is not overridden, the SAP specified filter is applied to the packet (if defined).

IP Interface Defined Egress QoS Reclassification

The SAP egress QoS policy defined forwarding class and profile reclassification rules are not applied to egress routed packets. To allow for egress reclassification, a SAP egress QoS policy ID may be optionally defined on the IP interface which will be applied to routed packets that egress the SAPs on the VPLS or I-VPLS service associated with the IP interface. Both unicast directed and MAC unknown flooded traffic apply to this rule. Only the reclassification portion of the QoS policy is applied which includes IP precedence or DSCP classification rules and any defined IP match criteria and their associated actions.

The policers and queues defined within the QoS policy applied to the IP interface are not created on the egress SAPs of the VPLS service. Instead, the actual QoS policy applied to the egress SAPs defines the egress policers and queues that will be used by both routed and non-routed egress packets. The forwarding class mappings defined in the egress SAP’s QoS policy will also define which policer or queue will handle each forwarding class for both routed and non-routed packets.
VPLS Egress Remarking and Egress Routed Packets

The egress remaking defined in the SAP egress QoS policy is not performed for packets that are routed out an egress VPLS SAP. However, ingress derived egress remaking is performed for egress routed packets.

IPv4 Multicast Routing

When using IPv4 Multicast routing, the following are not supported:

- Multicast VLAN registration functions within the associated VPLS service.
- The configuration of a video ISA within the associated VPLS service.
- The configuration of MFIB-allowed MDA destinations under spoke/mesh SDPs within the associated VPLS service.
- IPv4 multicast routing is not supported in Routed I-VPLS.

Routed VPLS Supported Routing Related Protocols

The following protocols are supported on IP interfaces bound to a VPLS service:

- BGP
- OSPF
- ISIS
- PIM
- IGMP
- BFD
- VRRP
- ARP

Spanning Tree and Split Horizon

A routed VPLS context supports all spanning tree and split horizon capabilities that a non-routed VPLS service supports.
VPLS Service Considerations

This section describes various SR-OS service features and any special capabilities or considerations as they relate to VPLS services.

SAP Encapsulations

VPLS services are designed to carry Ethernet frame payloads, so it can provide connectivity between any SAPs and SDPs that pass Ethernet frames. The following SAP encapsulations are supported on the SR-OS VPLS service:

- Ethernet null
- Ethernet Dot1q
- Ethernet QinQ

VLAN Processing

The SAP encapsulation definition on Ethernet ingress ports defines which VLAN tags are used to determine the service that the packet belongs:

1. Null encapsulation defined on ingress — Any VLAN tags are ignored and the packet goes to a default service for the SAP.
2. Dot1q encapsulation defined on ingress — Only first label is considered.
3. QinQ encapsulation defined on ingress— Both labels are considered.
   Note that the SAP can be defined with a wildcard for the inner label (for example, “100:100.*”). In this situation all packets with an outer label of 100 will be treated as belonging to the SAP. If, on the same physical link, there is also a SAP defined with a QinQ encapsulation of 100:100.1, then traffic with 100:1 will go to that SAP and all other traffic with 100 as the first label will go to the SAP with the 100:100.* definition.

In situations 2 and 3 above, traffic encapsulated with tags for which there is no definition are discarded.
Ingress VLAN Swapping

This feature is supported on VPLS and VLL service where the end to end solution is built using two node solutions (requiring SDP connections between the nodes).

In VLAN swapping, only the VLAN-id value will be copied to the inner VLAN position. Ethertype of the inner tag will be preserved and all consecutive nodes will work with that value. Similarly, the dot1p bits value of outer-tag will not be preserved.

The network diagram describes the network where at user access side (DSLAM facing SAPs) every subscriber is represented by several QinQ SAPs with inner-tag encoding service and outer-tag encoding subscriber (DSL line). The aggregation side (BRAS or PE facing SAPs) the is represented by DSL line number (inner VLAN tag) and DSLAM (outer VLAN tag). The effective operation on VLAN tag is to drop inner tag at access side and push another tag at the aggregation side.
Service Auto-Discovery using Multiple VLAN Registration Protocol (MVRP)

IEEE 802.1ak Multiple VLAN Registration Protocol (MVRP) is used to advertise throughout a native Ethernet switching domain one or multiple VLAN IDs to build automatically native Ethernet connectivity for multiple services. These VLAN IDs can be either Customer VLAN IDs (CVID) in an enterprise switching environment, Stacked VLAN IDs (SVID) in a Provider Bridging, QinQ Domain (see IEEE 802.1ad) or Backbone VLAN IDs (BVID) in a Provider Backbone Bridging (PBB) domain (see IEEE 802.1ah).

The initial focus of Alcatel-Lucent MVRP implementation is a Service Provider QinQ domain with or without a PBB core. The QinQ access into a PBB core example is used throughout this section to describe the MVRP implementation. With the exception of end-station components, a similar solution can be used to address a QinQ only or enterprise environments.

The components involved in the MVRP control plane are depicted in Figure 106.

All the devices involved are QinQ switches with the exception of the PBB BEB which delimits the QinQ domain and ensures the transition to the PBB core. The red circles represent Management VPLS instances interconnected by SAPs to build a native Ethernet switching domain used for MVRP control plane exchanges.

The following high level steps are involved in auto-discovery of VLAN connectivity in a native Ethernet domain using MVRP:
• Configure the MVRP infrastructure
  → This involves the configuration of a Management VPLS (M-VPLS) context
  → MSTP may be used in M-VPLS to provide the loop-free topology over which the
    MVRP exchanges take place.
• Instantiate related VLAN FIB, trunks in the MVRP, M-VPLS scope
  → The VLAN FIBs (VPLS instances) and associated trunks (SAPs) are instantiated in
    the same Ethernet switches and on the same “trunk ports” as the M-VPLS
  → There is no need to instantiate data VPLS instances in the BEB. IVPLS instances and
    related downward facing SAPs will be provisioned manually because the ISID to
    VLAN association must be configured.
• MVRP activation of service connectivity
  → When the first two customer UNI and/or PBB end-station SAPs are configured on
    different Ethernet switches in a certain service context the MVRP exchanges will
    activate service connectivity

---

**Configure the MVRP Infrastructure using an M-VPLS Context**

The following provisioning steps apply:

- Configure M-VPLS instances in the switches that will participate in MVRP control plane
- Configure under the M-VPLS the untagged SAP(s) to be used for MVRP exchanges; only
  dot1q or qinq ports are accepted for MVRP enabled M-VPLS
- Configure MVRP parameters at M-VPLS instance or SAP level

---

**Instantiate Related VLAN FIBs and Trunks in MVRP Scope**

This involves the configuration in the M-VPLS, under vpls-group of the following attributes:
VLAN range(s), vpls-template and vpls-sap-template bindings. As soon as the VPLS group is
enabled the configured attributes are used to auto-instantiate on a per VLAN basis a VPLS FIB
and related SAP(s) in the switches and on the “trunk ports” specified in the M-VPLS context. The
trunk ports are ports associated with an M-VPLS SAP not configured as an end-station.

The following procedure is used:

- The vpls-template binding is used to instantiate the VPLS instance where the service ID is
  derived from the VLAN value as per service-range configuration
- The vpls-sap-template binding is used to create dot1q SAP(s) by deriving from the VLAN
  value the service delimiter as per service-range configuration
The above procedure may be used outside of the MVRP context to pre-provision a large number of VPLS contexts that share the same infrastructure and attributes.

The MVRP control of the auto-instantiated services can be enabled using the `mvrp-contrl` command under `vpls-group`:

- If mvrp-control is disabled the auto-created VPLS instance(s) and related SAP(s) are ready to forward.
- If mvrp-control is enabled the auto-created VPLS instances will be instantiated initially with an empty flooding domain. The MVRP exchanges will gradually enabled service connectivity according to the operator configuration – between configured SAPs in the data VPLS context
  → This provides also protection against operational mistakes that may generate flooding throughout the auto-instantiated VLAN FIBs.

From an MVRP perspective these SAPs can be either “full MVRP” or “end-stations” interfaces.

A full MVRP interface is a full participant in the local M-VPLS scope:

- VLAN attributes received in an MVRP registration on this MVRP interface are declared on all the other full MVRP SAPs in the control VPLS.
- VLAN attributes received in an MVRP registration on other full MVRP interfaces in the local M-VPLS context are declared on this MVRP interface.

In an MVRP end-station the attribute(s) registered on that interface have local significance:

- VLAN attributes received in an MVRP registration on this interface are not declared on any other MVRP SAPs in the control VPLS. The attributes are registered only on the local port.
- Only locally active VLAN attributes are declared on the end-station interface; VLAN attributes registered on any other MVRP interfaces are not declared on end-station interfaces
- Also defining an M-VPLS SAP as end-station does not instantiate any objects on the local switch; the command is used just to define which SAP needs to be monitored by MVRP to declare the related VLAN value.

The following example describes the M-VPLS configuration required to auto-instantiate the VLAN FIBs and related trunks in non-PBB switches:
A similar M-VPLS configuration may be used to auto-instantiate the VLAN FIBs and related trunks in PBB switches. The vpls-group command is replaced by the end-station command under the downwards SAPs as in the following example:

```
config>service>vpls control-mvrp m-vpls create customer 1
[..]
sap 1/1/1:0
  mrp mvrp
    endstation-vid-group 1 vlan-id 100-2000
    no shutdown
```
MVRP Activation of Service Connectivity

As new Ethernet services are activated, UNI SAPs need to be configured and associated with the VLAN IDs (VPLS instances) auto-created using the procedures described in the previous sections. These UNI SAPs may be located in the same VLAN domain or over a PBB backbone. When UNI SAPs are located in different VLAN domains, an intermediate service translation point must be used at the PBB BEB which maps the local VLAN ID through an IVPLS SAP to a PBB ISID. This BEB SAP will be playing the role of an end-station from an MVRP perspective for the local VLAN domain. This section will discuss how MVRP is used to activate service connectivity between a BEB SAP and a UNI SAP located on one of the switches in the local domain. Similar procedure is used for the case of UNI SAPs configured on two switches located in the same access domain. No end-station configuration is required on the PBB BEB if all the UNI SAPs in a service are located in the same VLAN domain.

The service connectivity instantiation through MVRP is depicted in Figure 107.

In this example the UNI and service translation SAPs are configured in the data VPLS represented by the yellow circle. This instance and associated trunk SAPs were instantiated using the procedures described in the previous sections. The following configuration steps are involved:

- on the BEB an IVPLS SAP must be configured towards the local switching domain – see yellow triangle facing downwards
• on the UNI facing the customer a “customer” SAP is configured on the bottom left switch – see yellow triangle facing upwards

As soon as the first UNI SAP becomes “active” in the data VPLS on the ES, the associated VLAN value is advertised by MVRP throughout the related M-VPLS context. As soon as the second UNI SAP becomes available on a different switch or in our example on the PBB BEB the MVRP proceeds to advertise the associated VLAN value throughout the same M-VPLS. The trunks that experience MVRP declaration and registration in both directions will become active instantiating service connectivity as represented by the big and small yellow circles depicted in the picture.

A hold-time parameter (config>service>vpls>mrp>mvrp>hold-time) is provided in the M-VPLS configuration to control when the end-station or last UNI SAP is considered active from an MVRP perspective. The hold-time controls the amount of MVRP advertisements generated on fast transitions of the end-station or UNI SAPs.

If the no hold-time setting is used:

• MVRP will stop declaring the VLAN only when the last provisioned UNI SAP associated locally with the service is deleted.
• MVRP will start declare the VLAN as soon as the first provisioned SAP is created in the associated VPLS instance, regardless of the operational state of the SAP.

If a non-zero “hold-time” setting is used:

• When a SAP in down state is added, MVRP does not declare the associated VLAN attribute. The attribute is declared immediately when the SAP comes up.
• When the SAP goes down, MVRP will wait until “hold-time” expiry before withdrawing the declaration.

Note that for QinQ endstation SAPs only “no hold-time” setting is allowed.

Only the following PBB Epipe and I-VPLS SAP types are eligible to activate MVRP declarations:

• dot1q: for example 1/1/2:100
• qinq or qinq default: for example, 1/1/1:100.1 and respectively 1/1/1:100.*; the outer VLAN 100 will be used as MVRP attribute as long as it belongs to the MVRP range configured for the port
• null port and dot1q default cannot be used

An example of steps required to activate service connectivity for VLAN 100 using MVRP follows.
In the data VPLS instance (VLAN 100) controlled by MVRP, on the QinQ switch:

```
config>service>vpls 100
  sap 9/1/1:10 //UNI sap using CVID 10 as service delimiter.
  no shutdown
```

In I-VPLS on PBB BEB:

```
config>service>vpls 1000 i-vpls
  sap 8/1/2:100 //sap (using MVRP VLAN 100 on endstation port in VPLS.)
  no shutdown
```
MVRP Control Plane

MVRP is based on the IEEE 802.1ak MRP specification where STP is the supported method to be used for loop avoidance in a native Ethernet environment. M-VPLS and associated MSTP (or P-MSTP) control plane provides the loop avoidance component in Alcatel-lucent implementation. Alcatel-Lucent MVRP may be used also in a non- MSTP, loop free topology.

STP-MVRP Interaction

The following table captures the expected interaction between STP (MSTP or P-MSTP) and MVRP:

Table 9: MSTP and MVRP Interaction Table

<table>
<thead>
<tr>
<th>Item</th>
<th>M-VPLS Service xSTP</th>
<th>M-VPLS SAP STP</th>
<th>Register/Declare Data VPLS VLAN on M-VPLS SAP</th>
<th>DSFS (Data SAP Forwarding State) controlled by</th>
<th>Data Path Forwarding with MVRP enabled controlled by</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>(p)MSTP</td>
<td>Enabled</td>
<td>based on M-VPLS SAP’s MSTP forwarding state</td>
<td>MSTP only</td>
<td>DSFS and MVRP</td>
</tr>
<tr>
<td>2</td>
<td>(p)MSTP</td>
<td>Disabled</td>
<td>based on M-VPLS SAP’s oper state</td>
<td>None</td>
<td>MVRP</td>
</tr>
<tr>
<td>3</td>
<td>Disabled</td>
<td>Enabled or Disabled</td>
<td>based on M-VPLS SAP’s oper state</td>
<td>None</td>
<td>MVRP</td>
</tr>
</tbody>
</table>

Notes:

- Running STP in data VPLS instances controlled by MVRP is not allowed.
- Running STP on MVRP-controlled end-station SAPs is not allowed.
Interaction Between MVRP and Instantiated SAP Status

This section describes how MVRP reacts to changes in the instantiated SAP status.

There are a number of mechanisms that may generate operational or admin down status for the SAPs and VPLS instances controlled by MVRP:

1. Port down
2. MAC Move
3. Port MTU too small
4. Service MTU too small

Note that the shutdown of the whole instantiated VPLS or instantiated SAPs is disabled in both VPLS and VPLS SAP templates. The no shutdown option is automatically configured.

In the port down case MVRP will also be operationally down on the port so no VLAN declaration will take place.

When MAC move is enabled in a data VPLS controlled by MVRP, in case a MAC move hit happens, one of the instantiated SAPs controlled by MVRP may be blocked. The SAP blocking by MAC Move is not reported though to the MVRP control plane. As a result MVRP keeps declaring and registering the related VLAN value on the control SAPs including the one which shares the same port with the instantiate SAP blocked by MAC move as long as MVRP conditions are met. For MVRP, an active control SAP is one that has MVRP enabled and MSTP is not blocking it for the VLAN value on the port. Also in the related data VPLS one of the two conditions must be met for the declaration of the VLAN value: there must be either a local user SAP or at least one MVRP registration received on one of the control SAPs for that VLAN.

In the last two cases VLAN attributes get declared or registered even when the instantiated SAP is operationally down, similarly with the MAC move case.
Using Temporary Flooding to Optimize Failover Times

MVRP advertisements use the active topology which may be controlled through loop avoidance mechanisms like MSTP. When the active topology changes as a result of network failures, the time it takes for MVRP to bring up the optimal service connectivity may be added on top of the regular MSTP convergence time. Full connectivity also depends on the time it takes for the system to complete flushing of bad MAC entries.

In order to minimize the effects of MAC Flushing and MVRP convergence, a temporary flooding behavior is implemented. When enabled the temporary flooding eliminates the time it takes to flush the MAC tables. In the initial implementation the temporary flooding is initiated only on reception of an STP TCN.

While temporary flooding is active all the frames received in the extended data VPLS context are flooded while the MAC flush and MVRP convergence takes place. The extended data VPLS context comprises all instantiated trunk SAPs regardless of MVRP activation status. A timer option is also available to configure a fixed amount of time, in seconds, during which all traffic is flooded (BUM or known unicast). Once the flood-time expires, traffic will be delivered according to the regular FIB content. The timer value should be configured to allow auxiliary processes like MAC Flush and MVRP to converge. The temporary flooding behavior applies to all VPLS types. Note that MAC learning continues during temporary flooding. Temporary flooding behavior is enabled using the temp-flooding command under `config> service>vpls` or `config> service>template>vpls-template` contexts and is supported in VPLS regardless of whether MVRP is enabled or not.

The following rules apply for temporary flooding in VPLS:

- If discard-unknown is enabled then there is no temporary flooding
- Temporary flooding while active applies also to static MAC entries; after the MAC FIB is flushed it reverts back to the static MAC entries
- If MAC learning is disabled fast or temporary flooding is still enabled
- Temporary flooding is not supported in B-VPLS context when MMRP is enabled. The use of flood-time procedure provides a better procedure for this kind of environment.
Ingress VLAN Swapping
Configuring a VPLS Service with CLI

This section provides information to configure VPLS services using the command line interface.

Topics in this section include:

- Basic Configuration on page 652
- Common Configuration Tasks on page 654
  - Configuring VPLS Components on page 655
    - Creating a VPLS Service on page 657
    - Configuring a VPLS SAP on page 668
- Configuring VPLS Redundancy on page 691
  - Creating a Management VPLS for SAP Protection on page 691
- Service Management Tasks on page 705
  - Modifying VPLS Service Parameters on page 705
  - Modifying Management VPLS Parameters on page 706
  - Deleting a VPLS Service on page 708
  - Disabling a VPLS Service on page 708
  - Re-Enabling a VPLS Service on page 709
Basic Configuration

The following fields require specific input (there are no defaults) to configure a basic VPLS service:

- Customer ID (refer to Configuring Customers on page 84)
- For a local service, configure two SAPs, specifying local access ports and encapsulation values.
- For a distributed service, configure a SAP and an SDP for each far-end node.

The following example displays a sample configuration of a local VPLS service on ALA-1.

*A:ALA-1>config>service>vpls# info
---------------------------------------------------------------
    vpls 9001 customer 6 create
test shutdown
exit
.sap 1/2/2:0 create
description "SAP for local service"
exit
.sap 1/1/5:0 create
description "SAP for local service"
exit
no shutdown
---------------------------------------------------------------
*A:ALA-1>config>service>vpls#

The following example displays a sample configuration of a distributed VPLS service between ALA-1, ALA-2, and ALA-3.

*A:ALA-1>config>service# info
---------------------------------------------------------------
    vpls 9000 customer 6 create
.shutdown
description "This is a distributed VPLS."
def-mesh-vc-id 750
stp
    shutdown
exit
.sap 1/1/5:16 create
description "VPLS SAP"
exite
.spoke-sdp 2:22 create
.exit
.mesh-sdp 7:750 create
.exit

---------------------------------------------------------------
*A:ALA-1>config>service#
vpls 9000 customer 6 create
description "This is a distributed VPLS."
def-mesh-vc-id 750
stp
  shutdown
exit
sap 1/1/5:16 create
description "VPLS SAP"
exit
spoke-sdp 2:22 create
exit
mesh-sdp 8:750 create
exit
no shutdown
exit
...
Common Configuration Tasks

This section provides a brief overview of the tasks that must be performed to configure both local and distributed VPLS services and provides the CLI commands.

For egress multicast groups (optional):

1. Define egress multicast group name(s)
2. Specify the destinations per pass
3. Define SAP common requirements

For VPLS services:

1. Associate VPLS service with a customer ID
2. Define SAPs:
   - Select node(s) and port(s)
   - Optional — Select QoS policies other than the default (configured in `config>qos context`)
   - Optional — Select filter policies (configured in `config>filter context`)
   - Optional — Select accounting policy (configured in `config>log context`)
   — Optional — Specify SAP egress multicast-group name
3. Associate SDPs for (distributed services)
4. Modify STP default parameters (optional) (see VPLS and Spanning Tree Protocol on page 561)
5. Enable service
Configuring VPLS Components

Use the CLI syntax displayed below to configure the following entities:

- Configuring Egress Multicast Groups on page 656
- Creating a VPLS Service on page 657
  - Enabling MAC Move on page 660
- Configuring a VPLS SAP on page 668
  - Local VPLS SAPs on page 668
  - Distributed VPLS SAPs on page 669
  - Configuring SAP-Specific STP Parameters on page 671
  - STP SAP Operational States on page 675
  - Configuring VPLS SAPs with Split Horizon on page 677
  - Configuring Overrides on Service SAPs on page 679
- Configuring SDP Bindings on page 678
  - Mesh SDP on page 680
  - Spoke SDP on page 681
- Configuring VPLS Redundancy on page 691
Configuring Egress Multicast Groups

Use the following CLI syntax to configure egress multicast groups:

**CLI Syntax:**
```
config>service# egress-multicast-group group-name
description description-string
dest-chain-limit [destinations per pass]
sap-common-requirements
dot1q-etype 0x0600..0xffff
egress-filter [ip ip-filter-id]
egress-filter [ipv6 ipv6-filter-id]
egress-filter [mac mac-filter-id]
qinq-etype [0x0600..0xffff]
qinq-fixed-tag-value tag-value
```

The following example displays an egress multicast group configuration:

```
A:ALA-48>config>service>egress-multicast-group# info
---------------------------------------------
dest-chain-limit 10
.sap-common-requirements
  dot1q-etype 0x060e
egress-filter ip 10
.exit
---------------------------------------------
A:ALA-48>config>service>egress-multicast-group#
```
Creating a VPLS Service

Use the following CLI syntax to create a VPLS service:

**CLI Syntax:**
```
config>service# vpls service-id [customer customer-id] [vpn vpn-id] [m-vpls] [b-vpls | i-vpls] [create]
description description-string
no shutdown
```

The following example displays a VPLS configuration:

```
*A:ALA-1>config>service>vpls# info
----------------------------------------------
... vpls 9000 customer 6 create
description "This is a distributed VPLS."
def-mesh-vc-id 750
stp
shutdown
exit
exit
... ----------------------------------------------
*A:ALA-1>config>service>vpls#
```
Enabling Multiple MAC Registration Protocol (MMRP)

Once MMRP is enabled in the B-VPLS, it advertises the presence of the I-VPLS instances associated with this B-VPLS.

The following example displays a configuration with MMRP enabled.

```
*A:PE-B>config>service# info
----------------------------------------------
vpls 11 customer 1 vpn 11 i-vpls create
  backbone-vpls 100:11
  exit
  stp
    shutdown
  exit
  sap 1/5/1:11 create
  exit
  sap 1/5/1:12 create
  exit
  no shutdown
exit
vpls 100 customer 1 vpn 100 b-vpls create
  service-mtu 2000
  stp
    shutdown
  exit
  mrp
    flood-time 10
    no shutdown
  exit
  sap 1/5/1:100 create
  exit
  spoke-sdp 3101:100 create
  exit
  spoke-sdp 3201:100 create
  exit
  no shutdown
exit
----------------------------------------------
*A:PE-B>config>service#
```

Since I-VPLS 11 is associated with B-VPLS 100, MMRP advertises the group B-MAC (01:1e:83:00:00:0b) associated with I-VPLS 11 through a declaration on all the B-SAPs and B-SDPs. If the remote node also declares an I-VPLS 11 associated to its B-VPLS 10, then this results in a registration for the group B-MAC. This also creates the MMRP multicast tree (MFIB entries).

In this case, sdp 3201:100 is connected to a remote node that declares the group B-MAC.

The following show commands display the current MMRP information for this scenario:

```
*A:PE-C# show service id 100 mrp
-------------------------------------------------------------------------------
MRP Information
-------------------------------------------------------------------------------
Admin State : Up                  Failed Register Cnt: 0
Max Attributes : 1023    Attribute Count : 1
```
Attr High Watermark: 95%                Attr Low Watermark : 90%
Flood Time             : 10
-------------------------------------------------------------------------------
*A:PE-C# show service id 100 mmrp mac
-------------------------------------------------------------------------------
SAP/SDP                  MAC Address       Registered  Declared
-------------------------------------------------------------------------------
sap:1/5/1:100           01:1e:83:00:00:0b No          Yes
sdp:3101:100            01:1e:83:00:00:0b No          Yes
sdp:3201:100            01:1e:83:00:00:0b Yes         Yes
-------------------------------------------------------------------------------
*A:PE-C# show service id 100 sdp 3201:100 mrp
-------------------------------------------------------------------------------
Sdp Id 3201:100 MRP Information
-------------------------------------------------------------------------------
Join Time          : 0.2 secs                 Leave Time        : 3.0 secs
Leave All Time     : 10.0 secs                Periodic Time     : 1.0 secs
Periodic Enabled   : false
Rx Pdus            : 7                        Tx Pdus           : 23
Dropped Pdus       : 0
Rx New Event       : 0                        Rx Join-In Event  : 6
Rx In Event        : 0                        Rx Join Empty Evt : 1
Rx Empty Event     : 0                        Rx Leave Event    : 0
Tx New Event       : 0                        Tx Join-In Event  : 4
Tx In Event        : 0                        Tx Join Empty Evt : 19
Tx Empty Event     : 0                        Tx Leave Event    : 0
-------------------------------------------------------------------------------
SDP MMRP Information
-------------------------------------------------------------------------------
MAC Address       Registered        Declared
-------------------------------------------------------------------------------
01:1e:83:00:00:0b Yes               Yes
-------------------------------------------------------------------------------
Number of MACs=1 Registered=1 Declared=1
-------------------------------------------------------------------------------
*A:PE-C#

*A:PE-C# show service id 100 mfib
-------------------------------------------------------------------------------
Multicast FIB, Service 100
-------------------------------------------------------------------------------
Source Address  Group Address         Sap/Sdp Id               Svc Id   Fwd/Blk
-------------------------------------------------------------------------------
*               01:1E:83:00:00:0B         sdp:3201:100       Local    Fwd
-------------------------------------------------------------------------------
Number of entries: 1
-------------------------------------------------------------------------------
*A:PE-C#
Enabling MAC Move

The mac-move feature is useful to protect against undetected loops in your VPLS topology as well as the presence of duplicate MACs in a VPLS service. For example, if two clients in the VPLS have the same MAC address, the VPLS will experience a high re-learn rate for the MAC and will shut down the SAP or spoke SDP when the threshold is exceeded.

Use the following CLI syntax to configure mac-move parameters.

**CLI Syntax:**
```
config>service# vpls service-id [customer customer-id] [vpn vpn-id] [m-vpls]
  mac-move
    primary-ports
    spoke-sdp
    cumulative-factor
    exit
  secondary-ports
    spoke-sdp
    sap
    exit
    move-frequency frequency
    retry-timeout timeout
    no shutdown
```

The following example displays a mac-move configuration:

```
*A:ALA-2009>config>service>vpls>mac-move# show service id 500 mac-move
===============================================================================
Service Mac Move Information
===============================================================================
Service Id        : 500                 Mac Move          : Enabled
Primary Factor    : 4                   Secondary Factor  : 2
Mac Move Rate     : 2                   Mac Move Timeout  : 10
Mac Move Retries  : 3
-------------------------------------------------------------------------------
SAP Mac Move Information: 2/1/3:501
-------------------------------------------------------------------------------
Admin State       : Up                  Oper State        : Down
Flags              : RelearnLimitExceeded
Time to come up   : 1 seconds           Retries Left      : 1
Mac Move          : Blockable           Blockable Level   : Tertiary
-------------------------------------------------------------------------------
SAP Mac Move Information: 2/1/3:502
-------------------------------------------------------------------------------
Admin State       : Up                  Oper State        : Up
Flags              : None
Time to RetryReset: 267 seconds        Retries Left      : none
Mac Move          : Blockable           Blockable Level   : Tertiary
-------------------------------------------------------------------------------
SDP Mac Move Information: 21:501
-------------------------------------------------------------------------------
Admin State       : Up                  Oper State        : Up
Flags              : None
Time to RetryReset: never                Retries Left      : 3
Mac Move          : Blockable           Blockable Level   : Secondary
```
SDP Mac Move Information: 21:502

Admin State       : Up                  Oper State        : Down
Flags              : RelearnLimitExceeded
Time to come up   : never               Retries Left      : none
Mac Move           : Blockable           Blockable Level   : Tertiary

*A:*A:ALA-2009>config>service>vpls>mac-move#
Configuring STP Bridge Parameters in a VPLS

Modifying some of the Spanning Tree Protocol parameters allows the operator to balance STP between resiliency and speed of convergence extremes. Modifying particular parameters, mentioned below, must be done in the constraints of the following two formulae:

\[
2 \times (\text{Bridge Forward Delay} - 1.0 \text{ seconds}) \geq \text{Bridge Max Age}
\]
\[
\text{Bridge Max Age} \geq 2 \times (\text{Bridge Hello Time} + 1.0 \text{ seconds})
\]

The following STP parameters can be modified at VPLS level:

- Bridge STP Admin State on page 662
- Mode on page 663
- Bridge Priority on page 663
- Max Age on page 664
- Forward Delay on page 664
- Hello Time on page 665
- MST Instances on page 666
- MST Max Hops on page 666
- MST Name on page 666
- MST Revision on page 666

STP always uses the locally configured values for the first three parameters (Admin State, Mode and Priority).

For the parameters Max Age, Forward Delay, Hello Time and Hold Count, the locally configured values are only used when this bridge has been elected root bridge in the STP domain, otherwise the values received from the root bridge are used. The exception to this rule is: when STP is running in RSTP mode, the Hello Time is always taken from the locally configured parameter. The other parameters are only used when running mode MSTP.

---

Bridge STP Admin State

The administrative state of STP at the VPLS level is controlled by the shutdown command.

When STP on the VPLS is administratively disabled, any BPDUs are forwarded transparently through the SR-OS. When STP on the VPLS is administratively enabled, but the administrative state of a SAP is down, BPDUs received on such a SAP are discarded.

CLI Syntax:  
```sh
config>service>vpls service-id# stp
   no shutdown
```
Mode

To be compatible with the different iterations of the IEEE 802.1D standard, the SR-OS supports several variants of the Spanning Tree protocol:

- **rstp** — Rapid Spanning Tree Protocol (RSTP) compliant with IEEE 802.1D-2004 - default mode.
- **dot1w** — Compliant with IEEE 802.1w.
- **comp-dot1w** — Operation as in RSTP but backwards compatible with IEEE 802.1w (this mode was introduced for interoperability with some MTU types).
- **mstp** — Compliant with the Multiple Spanning Tree Protocol specified in IEEE 802.1Q REV/D5.0-09/2005. This mode of operation is only supported in an mVPLS.
- **pmstp** — Compliant with the Multiple Spanning Tree Protocol specified in IEEE 802.1Q REV/D3.0-04/2005 but with some changes to make it backwards compatible to 802.1Q 2003 edition and IEEE 802.1w.

See section Spanning Tree Operating Modes on page 561 for details on these modes.

**CLI Syntax:**
```
config>service>vpls service-id# stp
    mode {rstp | comp-dot1w | dot1w | mstp}
    Default: rstp
```

Bridge Priority

The **bridge-priority** command is used to populate the priority portion of the bridge ID field within outbound BPDUs (the most significant 4 bits of the bridge ID). It is also used as part of the decision process when determining the best BPDU between messages received and sent. When running MSTP, this is the bridge priority used for the CIST.

All values will be truncated to multiples of 4096, conforming with IEEE 802.1t and 802.1D-2004.

**CLI Syntax:**
```
config>service>vpls service-id# stp
    priority bridge-priority
    Range: 1 to 65535
    Default: 32768
    Restore Default: no priority
```
Max Age

The **max-age** command indicates how many hops a BPDU can traverse the network starting from the root bridge. The message age field in a BPDU transmitted by the root bridge is initialized to 0. Each other bridge will take the message_age value from BPDU's received on their root port and increment this value by 1. The message_age thus reflects the distance from the root bridge. BPDU's with a message age exceeding max-age are ignored.

STP uses the max-age value configured in the root bridge. This value is propagated to the other bridges by the BPDU's. The default value of **max-age** is 20. This parameter can be modified within a range of 6 to 40, limited by the standard STP parameter interaction formulae.

**CLI Syntax:**
```
config>service>vpls service-id# stp
max-age max-info-age
```
- **Range:** 6 to 40 seconds
- **Default:** 20 seconds
- **Restore Default:** no max-age

Forward Delay

RSTP, as defined in the IEEE 802.1D-2004 standards, will normally transition to the forwarding state by a handshaking mechanism (rapid transition), without any waiting times. If handshaking fails (e.g. on shared links, see below), the system falls back to the timer-based mechanism defined in the original STP (802.1D-1998) standard.

A shared link is a link with more than two Ethernet bridges (for example, a shared 10/100BaseT segment). The **port-type** command is used to configure a link as point-to-point or shared (see section **SAP Link Type** on page 674).

For timer-based transitions, the 802.1D-2004 standard defines an internal variable **forward-delay**, which is used in calculating the default number of seconds that a SAP or spoke SDP spends in the discarding and learning states when transitioning to the forwarding state. The value of the forward-delay variable depends on the STP operating mode of the VPLS instance:

- in **rstp** mode, but only when the SAP or spoke SDP has not fallen back to legacy STP operation, the value configured by the **hello-time** command is used;
- in all other situations, the value configured by the **forward-delay** command is used.

**CLI Syntax:**
```
config>service>vpls service-id# stp
forward-delay seconds
```
- **Range:** 4 to 30 seconds
- **Default:** 15 seconds
- **Restore Default:** no forward-delay
Hello Time

The **hello-time** command configures the Spanning Tree Protocol (STP) hello time for the Virtual Private LAN Service (VPLS) STP instance.

The *seconds* parameter defines the default timer value that controls the sending interval between BPDU configuration messages by this bridge, on ports where this bridge assumes the designated role.

The active hello time for the spanning tree is determined by the root bridge (except when the STP is running in RSTP mode, then the hello time is always taken from the locally configured parameter).

The configured hello-time value can also be used to calculate the bridge forward delay, see **Forward Delay on page 664**.

**CLI Syntax:**
```
config>service>vpls service-id# stp
    hello-time hello-time
    Range: 1 to 10 seconds
    Default: 2 seconds
    Restore Default: no hello-time
```

Hold Count

The **hold-count** command configures the peak number of BPDUs that can be transmitted in a period of one second.

**CLI Syntax:**
```
config>service>vpls service-id# stp
    hold-count count-value
    Range: 1 to 10
    Default: 6
    Restore Default: no hold-count
```
**MST Instances**

You can create up to 15 MST-instances. They can range from 1 to 4094. By changing path-cost and priorities, you can make sure that each instance will form its own tree within the region, thus making sure different VLANs follow different paths.

You can assign non overlapping VLAN ranges to each instance. VLANs that are not assigned to an instance are implicitly assumed to be in instance 0, which is also called the CIST. This CIST cannot be deleted or created.

The parameter that can be defined per instance are mst-priority and vlan-range.

- **mst-priority** — The bridge-priority for this specific mst-instance. It follows the same rules as bridge-priority. For the CIST, the bridge-priority is used.
- **vlan-range** — The VLANs are mapped to this specific mst-instance. If no VLAN-ranges are defined in any mst-instances, then all VLANs are mapped to the CIST.

**MST Max Hops**

The mst-max-hops command defines the maximum number of hops the BPDU can traverse inside the region. Outside the region max-age is used.

**MST Name**

The MST name defines the name that the operator gives to a region. Together with MST revision and the VLAN to MST-instance mapping, it forms the MST configuration identifier. Two bridges that have the same MST configuration identifier form a region if they exchange BPDUs.

**MST Revision**

The MST revision together with MST-name and VLAN to MST-instance mapping define the MST configuration identifier. Two bridges that have the same MST configuration identifier form a region if they exchange BPDUs.
Configuring GSMP Parameters

The following parameters must be configured in order for GSMP to function:

- One or more GSMP sessions
- One or more ANCP policies
- For basic subscriber management only, ANCP static maps
- For enhanced subscriber management only, associate subscriber profiles with ANCP policies.

Use the following CLI syntax to configure GSMP parameters.

**CLI Syntax:**

```
config>service>vpls# gsm

   group name [create]

   ancp
dynamic-topology-discover

   oam
description description-string

   hold-multiplier multiplier

   keepalive seconds

   neighbor ip-address [create]
description v

   local-address ip-address

   priority-marking dscp dscp-name

   priority-marking prec ip-prec-value

   [no] shutdown

   [no] shutdown

   [no] shutdown
```

This example displays a GSMP group configuration.

```
A:ALA-48>config>service>vpls>gsm# info

----------------------------------------------

   group "group1" create

description "test group config"

   neighbor 10.10.10.104 create
description "neighbor1 config"

   local-address 10.10.10.103

   no shutdown

   exit

   no shutdown

   exit

   no shutdown

----------------------------------------------

A:ALA-48>config>service>vpls>gsm#
```
Configuring a VPLS SAP

A default QoS policy is applied to each ingress SAP. Additional QoS policies can be configured in the `config>qos` context. There are no default filter policies. Filter policies are configured in the `config>filter` context and must be explicitly applied to a SAP.

Use the following CLI syntax to create:

- Local VPLS SAPs on page 668
- Distributed VPLS SAPs on page 669

Local VPLS SAPs

To configure a local VPLS service, enter the `sap sap-id` command twice with different port IDs in the same service configuration.

The following example displays a local VPLS configuration:

```
*A:ALA-1>config>service# info
----------------------------------------------
... vpls 90001 customer 6 create
    description "Local VPLS"
    stp shutdown
    exit
    sap 1/2/2:0 create
    description "SAP for local service"
    exit
    sap 1/1/5:0 create
    description "SAP for local service"
    exit
    no shutdown
    exit
----------------------------------------------
*A:ALA-1>config>service#
*A:ALA-1>config>service# info
----------------------------------------------
vpls 1150 customer 1 create
    fdb-table-size 1000
    fdb-table-low-wmark 5
    fdb-table-high-wmark 80
    local-age 60
    stp
    shutdown
    exit
    sap 1/1/1:1155 create
    exit
    sap 1/1/2:1150 create
    exit
    no shutdown
    exit
----------------------------------------------
*A:ALA-1>config>service#
```
Distributed VPLS SAPs

To configure a distributed VPLS service, you must configure service entities on originating and far-end nodes. You must use the same service ID on all ends (for example, create a VPLS service ID 9000 on ALA-1, ALA-2, and ALA-3). A distributed VPLS consists of a SAP on each participating node and an SDP bound to each participating node.

For SDP configuration information, see Configuring an SDP on page 87. For SDP binding information, see Configuring SDP Bindings on page 678.

The following example displays a configuration of VPLS SAPs configured for ALA-1, ALA-2, and ALA-3.

```
*A:ALA-1>config>service# info
--------------------------------------------
... vpls 9000 customer 6 vpn 750 create
      description "Distributed VPLS services."
      def-mesh-vc-id 750
      stp
      shutdown
      exit
      sap 1/2/5:0 create
      description "VPLS SAP"
      multi-service-site "West"
      exit
      exit
...--------------------------------------------
*A:ALA-1>config>service#

*A:ALA-2>config>service# info
--------------------------------------------
... vpls 9000 customer 6 vpn 750 create
      description "Distributed VPLS services."
      def-mesh-vc-id 750
      stp
      shutdown
      exit
      sap 1/2/22 create
      description "VPLS SAP"
      multi-service-site "West"
      exit
      exit
...--------------------------------------------
*A:ALA-2>config>service#

*A:ALA-3>config>service# info
--------------------------------------------
... vpls 9000 customer 6 vpn 750 create
      description "Distributed VPLS services."
      def-mesh-vc-id 750
```
Configuring a VPLS Service with CLI

stp
  shutdown
exit
sap 1/1/3:33 create
description "VPLS SAP"
multi-service-site "West"
exit
exit
...
=================================================================
*A:ALA-3>config>service#
Configuring SAP-Specific STP Parameters

When a VPLS has STP enabled, each SAP within the VPLS has STP enabled by default. The operation of STP on each SAP is governed by:

- SAP STP Administrative State on page 671
- SAP Virtual Port Number on page 672
- SAP Priority on page 672
- SAP Path Cost on page 673
- SAP Edge Port on page 673
- SAP Auto Edge on page 674
- SAP Link Type on page 674

SAP STP Administrative State

The administrative state of STP within a SAP controls how BPDUs are transmitted and handled when received. The allowable states are:

- SAP Admin Up
  The default administrative state is up for STP on a SAP. BPDUs are handled in the normal STP manner on a SAP that is administratively up.
- SAP Admin Down
  An administratively down state allows a service provider to prevent a SAP from becoming operationally blocked. BPDUs will not originate out the SAP towards the customer. If STP is enabled on VPLS level, but disabled on the SAP, received BPDUs are discarded. Discarding the incoming BPDUs allows STP to continue to operate normally within the VPLS service while ignoring the down SAP. The specified SAP will always be in an operationally forwarding state.

  **NOTE:** The administratively down state allows a loop to form within the VPLS.

CLI Syntax:  
```
cfg>service>vpls>sap>stp#  
[no] shutdown
  Range: shutdown or no shutdown
  Default: no shutdown (SAP admin up)
```
SAP Virtual Port Number

The virtual port number uniquely identifies a SAP within configuration BPDUs. The internal representation of a SAP is unique to a system and has a reference space much bigger than the 12 bits definable in a configuration BPDU. STP takes the internal representation value of a SAP and identifies it with its own virtual port number that is unique to every other SAP defined on the VPLS. The virtual port number is assigned at the time that the SAP is added to the VPLS.

Since the order in which SAPs are added to the VPLS is not preserved between reboots of the system, the virtual port number may change between restarts of the STP instance. To achieve consistency after a reboot, the virtual port number can be specified explicitly.

CLI Syntax: config>service>vpls>sap# stp
  port-num number
  Range: 1 — 2047
  Default: (automatically generated)
  Restore Default: no port-num

SAP Priority

SAP priority allows a configurable “tie breaking” parameter to be associated with a SAP. When configuration BPDUs are being received, the configured SAP priority will be used in some circumstances to determine whether a SAP will be designated or blocked.

In traditional STP implementations (802.1D-1998), this field is called the port priority and has a value of 0 to 255. This field is coupled with the port number (0 to 255 also) to create a 16 bit value. In the latest STP standard (802.1D-2004) only the upper 4 bits of the port priority field are used to encode the SAP priority. The remaining 4 bits are used to extend the port ID field into a 12 bit virtual port number field. The virtual port number uniquely references a SAP within the STP instance. See SAP Virtual Port Number on page 672 for details on the virtual port number.

STP computes the actual SAP priority by taking the configured priority value and masking out the lower four bits. The result is the value that is stored in the SAP priority parameter. For example, if a value of 0 was entered, masking out the lower 4 bits would result in a parameter value of 0. If a value of 255 was entered, the result would be 240.

The default value for SAP priority is 128. This parameter can be modified within a range of 0 to 255, 0 being the highest priority. Masking causes the values actually stored and displayed to be 0 to 240, in increments of 16.

CLI Syntax: config>service>vpls>sap>stp# priority stp-priority
  Range: 0 to 255 (240 largest value, in increments of 16)
  Default: 128
  Restore Default: no priority
SAP Path Cost

The SAP path cost is used by STP to calculate the path cost to the root bridge. The path cost in BPDUs received on the root port is incremented with the configured path cost for that SAP. When BPDUs are sent out other egress SAPs, the newly calculated root path cost is used. These are the values used for CIST when running MSTP.

STP suggests that the path cost is defined as a function of the link bandwidth. Since SAPs are controlled by complex queuing dynamics, in the 7950 SR, the STP path cost is a purely static configuration.

The default value for SAP path cost is 10. This parameter can be modified within a range of 1 to 65535, 1 being the lowest cost.

CLI Syntax: config>service>vpls>sap>stp#
  path-cost sap-path-cost
  Range: 1 to 200000000
  Default: 10
  Restore Default: no path-cost

SAP Edge Port

The SAP edge-port command is used to reduce the time it takes a SAP to reach the forwarding state when the SAP is on the edge of the network, and thus has no further STP bridge to handshake with.

The edge-port command is used to initialize the internal OPER_EDGE variable. At any time, when OPER_EDGE is false on a SAP, the normal mechanisms are used to transition to the forwarding state (see Forward Delay on page 664). When OPER_EDGE is true, STP assumes that the remote end agrees to transition to the forwarding state without actually receiving a BPDU with an agreement flag set.

The OPER_EDGE variable will dynamically be set to false if the SAP receives BPDUs (the configured edge-port value does not change). The OPER_EDGE variable will dynamically be set to true if auto-edge is enabled and STP concludes there is no bridge behind the SAP.

When STP on the SAP is administratively disabled and re-enabled, the OPER_EDGE is re-initialized to the value configured for edge-port.

Valid values for SAP edge-port are enabled and disabled with disabled being the default.

CLI Syntax: config>service>vpls>sap>stp#
  [no] edge-port
  Default: no edge-port
SAP Auto Edge

The SAP **edge-port** command is used to instruct STP to dynamically decide whether the SAP is connected to another bridge.

If auto-edge is enabled, and STP concludes there is no bridge behind the SAP, the OPER_EDGE variable will dynamically be set to true. If auto-edge is enabled, and a BPDU is received, the OPER_EDGE variable will dynamically be set to true (see SAP Edge Port on page 673).

Valid values for SAP auto-edge are enabled and disabled with enabled being the default.

**CLI Syntax:**

```
config>service>vpls>sap>stp#
  [no] auto-edge
  Default: auto-edge
```

SAP Link Type

The SAP **link-type** parameter instructs STP on the maximum number of bridges behind this SAP. If there is only a single bridge, transitioning to forwarding state will be based on handshaking (fast transitions). If more than two bridges are connected by a shared media, their SAPs should all be configured as shared, and timer-based transitions are used.

Valid values for SAP link-type are shared and pt-pt with pt-pt being the default.

**CLI Syntax:**

```
config>service>vpls>sap>stp#
link-type {pt-pt|shared}
  Default: link-type pt-pt
  Restore Default: no link-type
```
STP SAP Operational States

The operational state of STP within a SAP controls how BPDUs are transmitted and handled when received. Defined states are:

- Operationally Disabled on page 675
- Operationally Discarding on page 675
- Operationally Learning on page 675
- Operationally Forwarding on page 676

Operationally Disabled

Operationally disabled is the normal operational state for STP on a SAP in a VPLS that has any of the following conditions:

- VPLS state administratively down
- SAP state administratively down
- SAP state operationally down

If the SAP enters the operationally up state with the STP administratively up and the SAP STP state is up, the SAP will transition to the STP SAP discarding state.

When, during normal operation, the router detects a downstream loop behind a SAP or spoke SDP, BPDUs can be received at a very high rate. To recover from this situation, STP will transition the SAP to disabled state for the configured forward-delay duration.

Operationally Discarding

A SAP in the discarding state only receives and sends BPDUs, building the local proper STP state for each SAP while not forwarding actual user traffic. The duration of the discarding state is explained in section Forward Delay on page 664.

Note: in previous versions of the STP standard, the discarding state was called a blocked state.

Operationally Learning

The learning state allows population of the MAC forwarding table before entering the forwarding state. In this state, no user traffic is forwarded.
Operationally Forwarding

Configuration BPDUs are sent out a SAP in the forwarding state. Layer 2 frames received on the SAP are source learned and destination forwarded according to the FIB. Layer 2 frames received on other forwarding interfaces and destined for the SAP are also forwarded.

SAP BPDU Encapsulation State

Each SAP has a Read-Only operational state that shows which BPDU encapsulation is currently active on the SAP. The states are:

- **Dot1d** — This state specifies that the switch is currently sending IEEE 802.1d standard BPDUs. The BPDUs are tagged or non-tagged based on the encapsulation type of the egress interface and the encapsulation value defined in the SAP. A SAP defined on an interface with encapsulation type Dot1q continues in the dot1d BPDU encapsulation state until a PVST encapsulated BPDU is received in which case, the SAP will convert to the PVST encapsulation state. Each received BPDU must be properly IEEE 802.1q tagged if the interface encapsulation type is defined as Dot1q. PVST BPDUs will be silently discarded if received when the SAP is on an interface defined with encapsulation type null.

- **PVST** — This state specifies that the switch is currently sending proprietary encapsulated BPDUs. PVST BPDUs are only supported on Ethernet interfaces with the encapsulation type set to dot1q. The SAP continues in the PVST BPDU encapsulation state until a dot1d encapsulated BPDU is received, in which case, the SAP reverts to the dot1d encapsulation state. Each received BPDU must be properly IEEE 802.1q tagged with the encapsulation value defined for the SAP. PVST BPDUs are silently discarded if received when the SAP is on an interface defined with a null encapsulation type.

Dot1d is the initial and only SAP BPDU encapsulation state for SAPs defined on Ethernet interface with encapsulation type set to null.
Configuring VPLS SAPs with Split Horizon

To configure a VPLS service with a split horizon group, add the split-horizon-group parameter when creating the SAP. Traffic arriving on a SAP within a split horizon group will not be copied to other SAPs in the same split horizon group.

The following example displays a VPLS configuration with split horizon enabled:

```
*A:ALA-1>config>service# info
----------------------------------------------
... vpls 800 customer 6001 vpn 700 create
description "VPLS with split horizon for DSL"
  stp
  shutdown
  exit
  sap 1/1/3:100 split-horizon-group DSL-group1 create
description "SAP for residential bridging"
  exit
  sap 1/1/3:200 split-horizon-group DSL-group1 create
description "SAP for residential bridging"
  exit
  split-horizon-group DSL-group1
description "Split horizon group for DSL"
  exit
  no shutdown
  exit
... ----------------------------------------------
*A:ALA-1>config>service#
```
Configuring SDP Bindings

VPLS provides scaling and operational advantages. A hierarchical configuration eliminates the need for a full mesh of VCs between participating devices. Hierarchy is achieved by enhancing the base VPLS core mesh of VCs with access VCs (spoke) to form two tiers. Spoke SDPs are generally created between Layer 2 switches and placed at the Multi-Tenant Unit (MTU). The PE routers are placed at the service provider's Point of Presence (POP). Signaling and replication overhead on all devices is considerably reduced.

A spoke SDP is treated like the equivalent of a traditional bridge port where flooded traffic received on the spoke SDP is replicated on all other “ports” (other spoke and mesh SDPs or SAPs) and not transmitted on the port it was received (unless a split horizon group was defined on the spoke SDP, see section Configuring VPLS Spoke SDPs with Split Horizon on page 690).

A spoke SDP connects a VPLS service between two sites and, in its simplest form, could be a single tunnel LSP. A set of ingress and egress VC labels are exchanged for each VPLS service instance to be transported over this LSP. The PE routers at each end treat this as a virtual spoke connection for the VPLS service in the same way as the PE-MTU connections. This architecture minimizes the signaling overhead and avoids a full mesh of VCs and LSPs between the two metro networks.

A mesh SDP bound to a service is logically treated like a single bridge “port” for flooded traffic where flooded traffic received on any mesh SDP on the service is replicated to other “ports” (spoke SDPs and SAPs) and not transmitted on any mesh SDPs.

A VC-ID can be specified with the SDP-ID. The VC-ID is used instead of a label to identify a virtual circuit. The VC-ID is significant between peer SRs on the same hierarchical level. The value of a VC-ID is conceptually independent from the value of the label or any other datalink specific information of the VC.

Figure 108 displays an example of a distributed VPLS service configuration of spoke and mesh SDPs (uni-directional tunnels) between routers and MTUs.
Configuring Overrides on Service SAPs

The following output displays a service SAP queue override configuration example.

*A:ALA-48>config>service>vpls>sap# info
----------------------------------------------
... exit
ingress
   scheduler-policy "SLA1"
   qos 100 multipoint-shared
   queue-override
       queue 1 create
           rate 1500000 cir 2000
   exit
exit
exit
egress
   scheduler-policy "SLA1"
   queue-override
       queue 1 create
           adaptation-rule pir max cir max
   exit
exit
filter ip 10
exit
----------------------------------------------
*A:ALA-48>config>service>vpls>sap#
Use the following CLI syntax to create a mesh or spoke SDP bindings with a distributed VPLS service. SDPs must be configured prior to binding. Refer to Configuring an SDP on page 87 for information about creating SDPs.

Use the following CLI syntax to configure mesh SDP bindings:

```
CLI Syntax:  config>service# vpls service-id
            mesh-sdp sdp-id[vc-id] [vc-type {ether|vlan}]
            egress
            filter [ip ip-filter-id|mac mac-filter-id]
            mfib-allowed-mda-destinations
            mda mda-id
            vc-label egress-vc-label
            ingress
            filter [ip ip-filter-id|mac mac-filter-id]
            vc-label ingress-vc-label
            no shutdown
            static-mac ieee-address
            vlan-vc-tag 0..4094
```

Figure 108: SDPs — Uni-Directional Tunnels

Use the following CLI syntax to create a mesh or spoke SDP bindings with a distributed VPLS service. SDPs must be configured prior to binding. Refer to Configuring an SDP on page 87 for information about creating SDPs.

Use the following CLI syntax to configure mesh SDP bindings:
Use the following CLI syntax to configure spoke SDP bindings:

**CLI Syntax:**
```
config>service# vpls service-id
spoke-sdp sd-id:vc-id [vc-type {ether | vlan}] [split-hori-
zon-group group-name]
egress
  filter {ip ip-filter-id|mac mac-filter-id}
  vc-label egress-vc-label
ingress
  filter {ip ip-filter-id|mac mac-filter-id}
  vc-label ingress-vc-label
limit-mac-move[non-blockable]
  vlan-vc-tag 0..4094
no shutdown
static-mac ieee-address
stp
  path-cost stp-path-cost
  priority stp-priority
no shutdown
  vlan-vc-tag [0..4094]
```

The following displays SDP binding configurations for ALA-1, ALA-2, and ALA-3 for VPLS service ID 9000 for customer 6:

*A:ALA-1>config>service# info

```
... vpls 9000 customer 6 create
description "This is a distributed VPLS."
def-mesh-vc-id 750
stp
  shutdown
exit
sap 1/2/5:0 create
exit
spoke-sdp 2:22 create
exit
mesh-sdp 5:750 create
exit
mesh-sdp 7:750 create
exit
no shutdown
exit
```

*A:ALA-1>config>service#

*A:ALA-2>config>service# info

```
... vpls 9000 customer 6 create
description "This is a distributed VPLS."
```
def-mesh-vc-id 750
stp
  shutdown
exit
sap 1/1/2:22 create
exit
spoke-sdp 2:22 create
exit
mesh-sdp 5:750 create
exit
mesh-sdp 7:750 create
exit
no shutdown
exit

*A:ALA-3>config>service# info

vpls 9000 customer 6 create
description "This is a distributed VPLS."
def-mesh-vc-id 750
stp
  shutdown
exit
sap 1/1/3:33 create
exit
spoke-sdp 2:22 create
exit
mesh-sdp 5:750 create
exit
mesh-sdp 7:750 create
exit
no shutdown
exit

*A:ALA-3>config>service#
Configuring Spoke SDP Specific STP Parameters

When a VPLS has STP enabled, each spoke SDP within the VPLS has STP enabled by default. The operation of STP on each spoke SDP is governed by:

- Spoke SDP STP Administrative State on page 683
- Spoke SDP Virtual Port Number on page 684
- Spoke SDP Priority on page 684
- Spoke SDP Path Cost on page 685
- Spoke SDP Edge Port on page 685
- Spoke SDP Auto Edge on page 686
- Spoke SDP Link Type on page 686

Spoke SDP STP Administrative State

The administrative state of STP within a spoke SDP controls how BPDUs are transmitted and handled when received. The allowable states are:

- Spoke SDP Admin Up
  The default administrative state is up for STP on a spoke SDP. BPDUs are handled in the normal STP manner on a spoke SDP that is administratively up.
- Spoke SDP Admin Down
  An administratively down state allows a service provider to prevent a spoke SDP from becoming operationally blocked. BPDUs will not originate out the spoke SDP towards the customer.

If STP is enabled on VPLS level, but disabled on the spoke SDP, received BPDUs are discarded. Discarding the incoming BPDUs allows STP to continue to operate normally within the VPLS service while ignoring the down spoke SDP. The specified spoke SDP will always be in an operationally forwarding state.

NOTE: The administratively down state allows a loop to form within the VPLS.

CLI Syntax:  
```bash
config>service>vpls>spoke-sdp>stp#
[no] shutdown
  Range: shutdown or no shutdown
  Default: no shutdown (spoke SDP admin up)```
Spoke SDP Virtual Port Number

The virtual port number uniquely identifies a spoke SDP within configuration BPDUs. The internal representation of a spoke SDP is unique to a system and has a reference space much bigger than the 12 bits definable in a configuration BPDU. STP takes the internal representation value of a spoke SDP and identifies it with its own virtual port number that is unique to every other spoke SDP defined on the VPLS. The virtual port number is assigned at the time that the spoke SDP is added to the VPLS.

Since the order in which spoke SDPs are added to the VPLS is not preserved between reboots of the system, the virtual port number may change between restarts of the STP instance. To achieve consistency after a reboot, the virtual port number can be specified explicitly.

**CLI Syntax:**
```
config>service>vpls>spoke-sdp# stp
    port-num number
    Range: 1 — 2047
    Default: (automatically generated)
    Restore Default: no port-num
```

Spoke SDP Priority

Spoke SDP priority allows a configurable tie breaking parameter to be associated with a spoke SDP. When configuration BPDUs are being received, the configured spoke SDP priority will be used in some circumstances to determine whether a spoke SDP will be designated or blocked.

In traditional STP implementations (802.1D-1998), this field is called the port priority and has a value of 0 to 255. This field is coupled with the port number (0 to 255 also) to create a 16 bit value. In the latest STP standard (802.1D-2004) only the upper 4 bits of the port priority field are used to encode the spoke SDP priority. The remaining 4 bits are used to extend the port ID field into a 12 bit virtual port number field. The virtual port number uniquely references a spoke SDP within the STP instance. See Spoke SDP Virtual Port Number on page 684 for details on the virtual port number.

STP computes the actual spoke SDP priority by taking the configured priority value and masking out the lower four bits. The result is the value that is stored in the spoke SDP priority parameter. For instance, if a value of 0 was entered, masking out the lower 4 bits would result in a parameter value of 0. If a value of 255 was entered, the result would be 240.

The default value for spoke SDP priority is 128. This parameter can be modified within a range of 0 to 255, 0 being the highest priority. Masking causes the values actually stored and displayed to be 0 to 240, in increments of 16.

**CLI Syntax:**
```
config>service>vpls>spoke-sdp>stp#
    priority stp-priority
    Range: 0 to 255 (240 largest value, in increments of 16)
    Default: 128
    Restore Default: no priority
```
Spoke SDP Path Cost

The spoke SDP path cost is used by STP to calculate the path cost to the root bridge. The path cost in BPDUs received on the root port is incremented with the configured path cost for that spoke SDP. When BPDUs are sent out other egress spoke SDPs, the newly calculated root path cost is used.

STP suggests that the path cost is defined as a function of the link bandwidth. Since spoke SDPs are controlled by complex queuing dynamics, the STP path cost is a purely static configuration.

The default value for spoke SDP path cost is 10. This parameter can be modified within a range of 1 to 200000000 (1 is the lowest cost).

**CLI Syntax:**
```
config>service>vpls>spoke-sdp>stp#
   path-cost stp-path-cost
```
- **Range:** 1 to 200000000
- **Default:** 10
- **Restore Default:** `no path-cost`

Spoke SDP Edge Port

The spoke SDP `edge-port` command is used to reduce the time it takes a spoke SDP to reach the forwarding state when the spoke SDP is on the edge of the network, and thus has no further STP bridge to handshake with.

The `edge-port` command is used to initialize the internal OPER_EDGE variable. At any time, when OPER_EDGE is false on a spoke SDP, the normal mechanisms are used to transition to the forwarding state (see Forward Delay on page 664). When OPER_EDGE is true, STP assumes that the remote end agrees to transition to the forwarding state without actually receiving a BPDU with an agreement flag set.

The OPER_EDGE variable will dynamically be set to false if the spoke SDP receives BPDUs (the configured edge-port value does not change). The OPER_EDGE variable will dynamically be set to true if auto-edge is enabled and STP concludes there is no bridge behind the spoke SDP.

When STP on the spoke SDP is administratively disabled and re-enabled, the OPER_EDGE is re-initialized to the spoke SDP configured for edge-port.

Valid values for spoke SDP edge-port are enabled and disabled with disabled being the default.

**CLI Syntax:**
```
config>service>vpls>spoke-sdp>stp#
   [no] edge-port
```
- **Default:** `no edge-port`
Spoke SDP Auto Edge

The spoke SDP edge-port command is used to instruct STP to dynamically decide whether the spoke SDP is connected to another bridge.

If auto-edge is enabled, and STP concludes there is no bridge behind the spoke SDP, the OPER_EDGE variable will dynamically be set to true. If auto-edge is enabled, and a BPDU is received, the OPER_EDGE variable will dynamically be set to true (see Spoke SDP Edge Port on page 685).

Valid values for spoke SDP auto-edge are enabled and disabled with enabled being the default.

CLI Syntax: config>service>vpls>spoke-sdp>stp#
            [no] auto-edge
            Default: auto-edge

Spoke SDP Link Type

The spoke SDP link-type command instructs STP on the maximum number of bridges behind this spoke SDP. If there is only a single bridge, transitioning to forwarding state will be based on handshaking (fast transitions). If more than two bridges are connected by a shared media, their spoke SDPs should all be configured as shared, and timer-based transitions are used.

Valid values for spoke SDP link-type are shared and pt-pt with pt-pt being the default.

CLI Syntax: config>service>vpls>spoke-sdp>stp#
            link-type {pt-pt|shared}
            Default: link-type pt-pt
            Restore Default: no link-type
Spoke SDP STP Operational States

The operational state of STP within a spoke SDP controls how BPDUs are transmitted and handled when received. Defined states are:

- Operationally Disabled on page 687
- Operationally Discarding on page 687
- Operationally Learning on page 687
- Operationally Forwarding on page 688

Operationally Disabled

Operationally disabled is the normal operational state for STP on a spoke SDP in a VPLS that has any of the following conditions:

- VPLS state administratively down
- Spoke SDP state administratively down
- Spoke SDP state operationally down

If the spoke SDP enters the operationally up state with the STP administratively up and the spoke SDP STP state is up, the spoke SDP will transition to the STP spoke SDP discarding state.

When, during normal operation, the router detects a downstream loop behind a spoke SDP, BPDUs can be received at a very high rate. To recover from this situation, STP will transition the spoke SDP to a disabled state for the configured forward-delay duration.

Operationally Discarding

A spoke SDP in the discarding state only receives and sends BPDUs, building the local proper STP state for each spoke SDP while not forwarding actual user traffic. The duration of the discarding state is explained in section Forward Delay on page 664.

Note: in previous versions of the STP standard, the discarding state was called a blocked state.

Operationally Learning

The learning state allows population of the MAC forwarding table before entering the forwarding state. In this state no user traffic is forwarded.
Operationally Forwarding

Configuration BPDUs are sent out a spoke SDP in the forwarding state. Layer 2 frames received on the spoke SDP are source learned and destination forwarded according to the FIB. Layer 2 frames received on other forwarding interfaces and destined for the spoke SDP are also forwarded.

Spoke SDP BPDU Encapsulation States

IEEE 802.1D (referred as dot1d) and Cisco’s per VLAN Spanning Tree (PVST) BPDU encapsulations are supported on a per spoke SDP basis. STP is associated with a VPLS service like PVST is per VLAN. The main difference resides in the Ethernet and LLC framing and a type-length-value (TLV) field trailing the BPDU.

Table 10 shows differences between dot1D and PVST Ethernet BPDU encapsulations based on the interface encap-type field:

Table 10: Spoke SDP BPDU Encapsulation States

<table>
<thead>
<tr>
<th>Field</th>
<th>dot1d encap-type null</th>
<th>dot1d encap-type dot1q</th>
<th>PVST encap-type null</th>
<th>PVST encap-type dot1q</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination MAC</td>
<td>01:80:c2:00:00:00</td>
<td>01:80:c2:00:00:00</td>
<td>N/A</td>
<td>01:00:0c:cc:cc:ed</td>
</tr>
<tr>
<td>Source MAC</td>
<td>Sending Port MAC</td>
<td>Sending Port MAC</td>
<td>N/A</td>
<td>Sending Port MAC</td>
</tr>
<tr>
<td>EtherType</td>
<td>N/A</td>
<td>0x81 00</td>
<td>N/A</td>
<td>0x81 00</td>
</tr>
<tr>
<td>Dot1p and CFI</td>
<td>N/A</td>
<td>0xe</td>
<td>N/A</td>
<td>0xe</td>
</tr>
<tr>
<td>Dot1q</td>
<td>N/A</td>
<td>VPLS spoke SDP ID</td>
<td>N/A</td>
<td>VPLS spoke SDP encap value</td>
</tr>
<tr>
<td>Length</td>
<td>LLC Length</td>
<td>LLC Length</td>
<td>N/A</td>
<td>LLC Length</td>
</tr>
<tr>
<td>LLC DSAP SSAP</td>
<td>0x4242</td>
<td>0x4242</td>
<td>N/A</td>
<td>0xaaaa (SNAP)</td>
</tr>
<tr>
<td>LLC CNTL</td>
<td>0x03</td>
<td>0x03</td>
<td>N/A</td>
<td>0x03</td>
</tr>
<tr>
<td>SNAP OUI</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>00 00 0c (Cisco OUI)</td>
</tr>
<tr>
<td>SNAP PID</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>01 0b</td>
</tr>
<tr>
<td>CONFIG or TCN BPDU</td>
<td>Standard 802.1d</td>
<td>Standard 802.1d</td>
<td>N/A</td>
<td>Standard 802.1d</td>
</tr>
<tr>
<td>TLV: Type &amp; Len</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>58 00 00 00 02</td>
</tr>
<tr>
<td>TLV: VLAN</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>VPLS spoke SDP encap value</td>
</tr>
<tr>
<td>Padding</td>
<td>As Required</td>
<td>As Required</td>
<td>N/A</td>
<td>As Required</td>
</tr>
</tbody>
</table>
Each spoke SDP has a Read Only operational state that shows which BPDU encapsulation is currently active on the spoke SDP. The following states apply:

- **Dot1d** specifies that the switch is currently sending IEEE 802.1D standard BPDUs. The BPDUs will be tagged or non-tagged based on the encapsulation type of the egress interface and the encapsulation value defined in the spoke SDP. A spoke SDP defined on an interface with encapsulation type dot1q will continue in the dot1d BPDU encapsulation state until a PVST encapsulated BPDU is received, after which the spoke SDP will convert to the PVST encapsulation state. Each received BPDU must be properly IEEE 802.1q tagged if the interface encapsulation type is defined to dot1q.

- **PVST** specifies that the switch is currently sending proprietary encapsulated BPDUs. PVST BPDUs are only supported on Ethernet interfaces with the encapsulation type set to dot1q. The spoke SDP continues in the PVST BPDU encapsulation state until a dot1d encapsulated BPDU is received, in which case the spoke SDP reverts to the dot1d encapsulation state. Each received BPDU must be properly IEEE 802.1q tagged with the encapsulation value defined for the spoke SDP.

Dot1d is the initial and only spoke SDP BPDU encapsulation state for spoke SDPs defined on Ethernet interface with encapsulation type set to null.

Each transition between encapsulation types optionally generates an alarm that can be logged and optionally transmitted as an SNMP trap.
Configuring VPLS Spoke SDPs with Split Horizon

To configure spoke SDPs with a split horizon group, add the `split-horizon-group` parameter when creating the spoke SDP. Traffic arriving on a SAP or spoke SDP within a split horizon group will not be copied to other SAPs or spoke SDPs in the same split horizon group.

The following example displays a VPLS configuration with split horizon enabled:

```
*A:ALA-1>config>service# info
----------------------------------------------
... vpls 800 customer 6001 vpn 700 create
description "VPLS with split horizon for DSL"
  stp
    shutdown
  exit
spoke-sdp 51:15 split-horizon-group DSL-group1 create
  exit
split-horizon-group DSL-group1
description "Split horizon group for DSL"
  exit
no shutdown
exit
...----------------------------------------------
*A:ALA-1>config>service#
```
Configuring VPLS Redundancy

This section discusses the following service management tasks:

- Creating a Management VPLS for SAP Protection on page 691
- Creating a Management VPLS for Spoke SDP Protection on page 692

Creating a Management VPLS for SAP Protection

This section provides a brief overview of the tasks that must be performed to configure a management VPLS for SAP protection and provides the CLI commands, see Figure 109. The tasks below should be performed on both nodes providing the protected VPLS service.

Before configuring a management VPLS, first read VPLS Redundancy on page 581 for an introduction to the concept of management VPLS and SAP redundancy.

1. Create an SDP to the peer node.
2. Create a management VPLS.
3. Define a SAP in the m-vpls on the port towards the MTU. Note that the port must be dot1q or qinq tagged. The SAP corresponds to the (stacked) VLAN on the MTU in which STP is active.
4. Optionally modify STP parameters for load balancing.
5. Create a mesh SDP in the m-vpls using the SDP defined in Step 1. Ensure that this mesh SDP runs over a protected LSP (see note below).
6. Enable the management VPLS service and verify that it is operationally up.
7. Create a list of VLANs on the port that are to be managed by this management VPLS.
8. Create one or more user VPLS services with SAPs on VLANs in the range defined by Step 6.

Note: The mesh SDP should be protected by a backup LSP or Fast Reroute. If the mesh SDP were to go down, STP on both nodes would go to “forwarding” state and a loop would occur.

Figure 109: Example Configuration for Protected VPLS SAP
Creating a Management VPLS for Spoke SDP Protection

This section provides a brief overview of the tasks that must be performed to configure a management VPLS for spoke SDP protection and provides the CLI commands, see Figure 110. The tasks below should be performed on all four nodes providing the protected VPLS service. Before configuring a management VPLS, first read Configuring a VPLS SAP on page 668 for an introduction to the concept of management VPLS and spoke SDP redundancy.

1. Create an SDP to the local peer node (node ALA-A2 in the example below).
2. Create an SDP to the remote peer node (node ALA-B1 in the example below).
3. Create a management VPLS.
4. Create a spoke SDP in the m-vpls using the SDP defined in Step 1. Ensure that this mesh SDP runs over a protected LSP (see note below).
5. Enable the management VPLS service and verify that it is operationally up.
6. Create a spoke SDP in the m-vpls using the SDP defined in Step 2. Optionally, modify STP parameters for load balancing (see Configuring Load Balancing with Management VPLS on page 695).
7. Create one or more user VPLS services with spoke SDPs on the tunnel SDP defined by Step 2.

As long as the user spoke SDPs created in step 7 are in this same tunnel SDP with the management spoke SDP created in step 6, the management VPLS will protect them.

The SDP should be protected by, for example, a backup LSP or Fast Reroute. If the SDP were to go down, STP on both nodes would go to “forwarding” state and a loop would occur.
Use the following CLI syntax to create a management VPLS for spoke SDP protection:

**CLI Syntax:**
```
config>service# sdp sdp-id mpls create
    far-end ip-address
    lsp lsp-name
    no shutdown
```

**CLI Syntax:**
```
vpls service-id customer customer-id [m-vpls] create
description description-string
mesh-sdp sdp-id:vc-id create
spoke-sdp sdp-id:vc-id create
stp
    no shutdown
```
The following example displays a VPLS configuration:

*A:ALA-A1>config>service# info
----------------------------------------------
... snip ...
----------------------------------------------
*A:ALA-A1>config>service#
Configuring Load Balancing with Management VPLS

With the concept of management VPLS, it is possible to load balance the user VPLS services across the two protecting nodes. This is done by creating two management VPLS instances, where both instances have different active QinQ spokes (by changing the STP path-cost). When different user VPLS services are associated with either the two management VPLS services, the traffic will be split across the two QinQ spokes. Load balancing can be achieved in both the SAP protection and spoke SDP protection scenarios.

![Diagram showing the configuration for load balancing across two protected VPLS spoke SDPs.]

Figure 111: Example Configuration for Load Balancing Across Two Protected VPLS Spoke SDPs

Use the following CLI syntax to create a load balancing across two management VPLS instances:

**CLI Syntax:**

```
config>service# sdp sdp-id mpls create
  far-end ip-address
  lsp lsp-name
  no shutdown

vpls service-id customer customer-id [m-vpls] create
  description description-string
  mesh-sdp sdp-id:vc-id create
  spoke-sdp sdp-id:vc-id create
  stp
  path-cost
  stp
  no shutdown
```
Note: the STP path costs in each peer node should be reversed.

The following example displays the VPLS configuration on ALA-A1 (top left, IP address 10.0.0.10):

*A:ALA-A1>config>service# info
----------------------------------------------
...  
sdp 101 mpls create  
    far-end 10.0.0.30  
    lsp "1toALA-B1"  
    no shutdown  
exit
sdp 102 mpls create  
    far-end 10.0.0.30  
    lsp "2toALA-B1"  
    no shutdown  
exit
...

vpls 101 customer 1 m-vpls create  
    spoke-sdp 101:1 create  
    stp  
        path-cost 1  
        exit  
exit
mesh-sdp 300:1 create  
exit
stp  
exit
no shutdown  
exit
vpls 102 customer 1 m-vpls create  
    spoke-sdp 102:2 create  
    stp  
        path-cost 1000  
        exit  
exit
mesh-sdp 300:2 create  
exit
stp  
exit
no shutdown  
exit
...
----------------------------------------------
*A:ALA-A1>config>service#
The following example displays the VPLS configuration on ALA-A2 (bottom left, IP address 10.0.0.20):

*AL-A2>config>service# info
----------------------------------------------
...  
sdp 101 mpls create
    far-end 10.0.0.40
    lsp "1toALA-B2"
    no shutdown
    exit
sdp 102 mpls create
    far-end 10.0.0.40
    lsp "2toALA-B2"
    no shutdown
    exit
...  
  vpls 101 customer 1 m-vpls create
      spoke-sdp 101:1 create
          stp
              path-cost 1000
              exit
          exit
      mesh-sdp 300:1 create
          exit
      stp
      exit
    no shutdown
    exit
  vpls 102 customer 1 m-vpls create
      spoke-sdp 102:2 create
          stp
              path-cost 1
              exit
          exit
      mesh-sdp 300:2 create
          exit
      stp
      exit
    no shutdown
    exit
...  
----------------------------------------------
*AL-A2>config>service#
The following example displays the VPLS configuration on ALA-A3 (top right, IP address 10.0.0.30):

*A:ALA-A1>config>service# info
-----------------------------------------------
... 
sdp 101 mpls create
   far-end 10.0.0.10
   lsp "1toALA-A1"
   no shutdown
exit
sdp 102 mpls create
   far-end 10.0.0.10
   lsp "2toALA-A1"
   no shutdown
exit
...
vpls 101 customer 1 m-vpls create
   spoke-sdp 101:1 create
      stp
         path-cost 1
      exit
      exit
   mesh-sdp 300:1 create
   exit
   stp
   exit
   no shutdown
exit
vpls 102 customer 1 m-vpls create
   spoke-sdp 102:2 create
      stp
         path-cost 1000
      exit
      exit
   mesh-sdp 300:2 create
   exit
   stp
   exit
   no shutdown
exit
...
-----------------------------------------------
*A:ALA-A1>config>service#
The following example displays the VPLS configuration on ALA-A4 (bottom right, IP address 10.0.0.40):

*A:ALA-A2>config>service# info
----------------------------------------------
...
  sdp 101 mpls create
    far-end 10.0.0.20
    lsp "1toALA-B2"
    no shutdown
  exit
  sdp 102 mpls create
    far-end 10.0.0.20
    lsp "2toALA-B2"
    no shutdown
  exit
...
  vpls 101 customer 1 m-vpls create
    spoke-sdp 101:1 create
    stp
    path-cost 1000
    exit
  exit
  mesh-sdp 300:1 create
  exit
  stp
  exit
  no shutdown
  exit
  vpls 102 customer 1 m-vpls create
    spoke-sdp 102:2 create
    stp
    path-cost 1
    exit
  exit
  mesh-sdp 300:2 create
  exit
  stp
  exit
  no shutdown
  exit
...
----------------------------------------------
*A:ALA-A2>config>service#
Configuring Selective MAC Flush

Use the following CLI syntax to enable selective MAC Flush in a VPLS.

**CLI Syntax:**  config>service# vpls service-id  
send-flush-on-failure

Use the following CLI syntax to disable selective MAC Flush in a VPLS.

**CLI Syntax:**  config>service# vpls service-id  
no send-flush-on-failure
Configuring Multi-Chassis Endpoints

The following output displays configuration examples of multi-chassis redundancy and the VPLS configuration. The configurations in the graphics depicted in Inter-Domain VPLS Resiliency Using Multi-Chassis Endpoints on page 584 are expressed in this output.

Node Mapping to figures the document:

- PE3 = Dut-B
- PE3' = Dut-C
- PE1 = Dut-D
- PE2 = Dut-E

PE3

```
*A:Dut-B>config>redundancy>multi-chassis# info
---------------------------------------------------------
  peer 3.1.1.3 create
    peer-name "Dut-C"
    description "mcep-basic-tests"
    source-address 2.1.1.2
    mc-endpoint
      no shutdown
      bfd-enable
      system-priority 50
    exit
    no shutdown
  exit
---------------------------------------------------------
*A:Dut-B>config>redundancy>multi-chassis#

*A:Dut-B>config>service>vpls# info
----------------------------------------
    fdb-table-size 20000
    send-flush-on-failure
    stp
      shutdown
    exit
    endpoint "mcep-t1" create
      no suppress-standby-signaling
      block-on-mesh-failure
      mc-endpoint 1
      mc-ep-peer Dut-C
    exit
    exit
    mesh-sdp 201:1 vc-type vlan create
    exit
    mesh-sdp 211:1 vc-type vlan create
    exit
    spoke-sdp 221:1 vc-type vlan endpoint "mcep-t1" create
    stp
```
shutdown
exit
block-on-mesh-failure
precedence 1
exit
spoke-sdp 231:1 vc-type vlan endpoint "mcep-t1" create
stp
shutdown
exit
block-on-mesh-failure
precedence 2
exit
no shutdown
----------------------------------------------
*A:Dut-B>config>service>vpls#

PE3’ Dut-C

:A:Dut-C>config>redundancy>multi-chassis# info
----------------------------------------------
peer 2.1.1.2 create
  peer-name "Dut-B"
  description "mcep-basic-tests"
  source-address 3.1.1.3
  mc-endpoint
    no shutdown
    bfd-enable
    system-priority 21
  exit
  no shutdown
  exit
----------------------------------------------
*A:Dut-C>config>redundancy>multi-chassis#
*A:Dut-C>config>service>vpls# info
----------------------------------------------
fdb-table-size 20000
send-flush-on-failure
stp
  shutdown
exit
endpoint "mcep-t1" create
  no suppress-standby-signaling
  block-on-mesh-failure
  mc-endpoint 1
    mc-ep-peer Dut-B
  exit
  exit
mesh-sdp 301:1 vc-type vlan create
exit
mesh-sdp 311:1 vc-type vlan create
exit
spoke-sdp 321:1 vc-type vlan endpoint "mcep-t1" create
stp
  shutdown
exit
  block-on-mesh-failure
  precedence 3
exit
spoke-sdp 331:1 vc-type vlan endpoint "mcep-t1" create
  stp
  shutdown
  exit
  block-on-mesh-failure
  exit
  no shutdown

*A:Dut-C>config>service>vpls#

**PE1 Dut-D**

*A:Dut-D>config>redundancy>multi-chassis# info

peer 5.1.1.5 create
  peer-name "Dut-E"
  description "mcep-basic-tests"
  source-address 4.1.1.4
  mc-endpoint
    no shutdown
    bfd-enable
    system-priority 50
    passive-mode
    exit
  no shutdown
  exit

*A:Dut-D>config>redundancy>multi-chassis#

*A:Dut-D>config>service>vpls# info

fdb-table-size 20000
propagate-mac-flush
stp
  shutdown
  exit
endpoint "mcep-t1" create
  block-on-mesh-failure
  mc-endpoint 1
  mc-ep-peer Dut-E
  exit
exit
mesh-sdp 401:1 vc-type vlan create
exit
spoke-sdp 411:1 vc-type vlan endpoint "mcep-t1" create
  stp
  shutdown
  exit
  block-on-mesh-failure
  precedence 2
  exit
spoke-sdp 421:1 vc-type vlan endpoint "mcep-t1" create
  stp
  shutdown
  exit
  block-on-mesh-failure
  precedence 1
exit
  mesh-sdp 431:1 vc-type vlan create
exit
  no shutdown
----------------------------------------------
*A:Dut-D>config>service>vpls# 

PE2  Dut-E

*A:Dut-E>config>redundancy>multi-chassis# info
----------------------------------------------
  peer 4.1.1.4 create
    peer-name "Dut-D"
    description "mcep-basic-tests"
    source-address 5.1.1.5
    mc-endpoint
      no shutdown
      bfd-enable
      system.priority 22
      passive-mode
    exit
    no shutdown
  exit
----------------------------------------------
*A:Dut-E>config>redundancy>multi-chassis#

*A:Dut-E>config>service>vpls# info
----------------------------------------------
  fdb-table-size 20000
  propagate-mac-flush
  stp
  shutdown
  exit
  endpoint "mcep-t1" create
    block-on-mesh-failure
    mc-endpoint 1
    mc-ep-peer Dut-D
  exit
  exit
  spoke-sdp 501:1 vc-type vlan endpoint "mcep-t1" create
    stp
    shutdown
    exit
    block-on-mesh-failure
    precedence 3
  exit
  spoke-sdp 511:1 vc-type vlan endpoint "mcep-t1" create
    stp
    shutdown
    exit
    block-on-mesh-failure
  exit
  spoke-sdp 521:1 vc-type vlan create
  exit
  spoke-sdp 531:1 vc-type vlan create
  exit
  no shutdown
----------------------------------------------
*A:Dut-E>config>service>vpls#
Service Management Tasks

This section discusses the following service management tasks:

- Modifying VPLS Service Parameters on page 705
- Modifying Management VPLS Parameters on page 706
- Deleting a Management VPLS on page 706
- Disabling a Management VPLS on page 707
- Deleting a VPLS Service on page 708

Modifying VPLS Service Parameters

You can change existing service parameters. The changes are applied immediately. To display a list of services, use the `show service service-using vpls` command. Enter the parameter such as description, SAP, and then enter the new information.

The following displays a modified VPLS configuration.

```
*A:ALA-1>config>service>vpls# info
----------------------------------------------
description "This is a different description."
disable-learning
disable-aging
discard-unknown
local-age 500
stp
  shutdown
exit
sap 1/1/5:22 create
description "VPLS SAP"
extit
exit
no shutdown
----------------------------------------------
*A:ALA-1>config>service>vpls#
```
Modifying Management VPLS Parameters

To modify the range of VLANs on an access port that are to be managed by an existing management VPLS, first the new range should be entered and afterwards the old range removed. If the old range is removed before a new range is defined, all customer VPLS services in the old range will become unprotected and may be disabled.

**CLI Syntax:**
```
config>service# vpls service-id
    sap sap-id
    managed-vlan-list
    [no] range vlan-range
```

Deleting a Management VPLS

As with normal VPLS service, a management VPLS cannot be deleted until SAPs and SDPs are unbound (deleted), interfaces are shutdown, and the service is shutdown on the service level.

Use the following CLI syntax to delete a management VPLS service:

**CLI Syntax:**
```
config>service
    [no] vpls service-id
    shutdown
    [no] spoke-sdp sdp-id
    [no] mesh-sdp sdp-id
    shutdown
    [no] sap sap-id
    shutdown
```
Disabling a Management VPLS

You can shut down a management VPLS without deleting the service parameters.

When a management VPLS is disabled, all associated user VPLS services are also disabled (to prevent loops). If this is not desired, first un-manage the user’s VPLS service by removing them from the managed-vlan-list or moving the spoke SDPs on to another tunnel SDP.

**CLI Syntax:**
```
config>service
  vpls service-id
  shutdown
```

**Example:**
```
config>service# vpls 1
config>service>vpls# shutdown
config>service>vpls# exit
```
Deleting a VPLS Service

A VPLS service cannot be deleted until SAPs and SDPs are unbound (deleted), interfaces are shutdown, and the service is shutdown on the service level.

Use the following CLI syntax to delete a VPLS service:

CLI Syntax:  
```
config>service
[no] vpls service-id
    shutdown
[no] mesh-sdp sdp-id
    shutdown
    sap sap-id [split-horizon-group group-name]
    no sap sap-id
    shutdown
```

Disabling a VPLS Service

You can shut down a VPLS service without deleting the service parameters.

CLI Syntax:  
```
config>service> vpls service-id
[no] shutdown
```

Example:  
```
config>service# vpls 1
config>service>vpls# shutdown
config>service>vpls# exit
```
Re-Enabling a VPLS Service

To re-enable a VPLS service that was shut down.

**CLI Syntax:**
```
config>service> vpls service-id
[no] shutdown
```

**Example:**
```
config>service# vpls 1
config>service>vpls# no shutdown
config>service>vpls# exit
```
VPLS Services Command Reference

Command Hierarchies

- Global Commands on page 712
- SAP Commands on page 718
- Mesh SDP Commands on page 728
- Spoke SDP Commands on page 731
- Provider Tunnel Commands on page 735
- Show Commands on page 738
- Clear Commands on page 740
- Debug Commands on page 741
VPLS Service Configuration Commands

Global Commands

```
config
  service
    vpls service-id [customer customer-id] [vpn vpn-id] [m-vpls | b-vpls | i-vpls] [create]
    no vpls service-id
    backbone-smac ieee-address
    no backbone-smac
    backbone-vpls service-id[:isid]
    no backbone-vpls
      [no] stp
    bgp
      pw-template-binding policy-id [split-horizon-group group-name]
        [import rt {ext-community...(up to 5 max)}]
      no pw-template-binding policy-id
        [no] bfd-enable
        bfd-template [256 chars max]
        no bfd-template
        monitor-oper-group group-name
        no monitor-oper-group
        oper-group group-name
        no oper-group
      route-target {ext-community | [[export ext-community] [import ext-community]]}
      no route-target
      route-distinguisher [ip-addr:comm-val | as-number:ext-comm-val]
      no route-distinguisher
      vsi-export policy-name [policy-name...(up to 5 max)]
      no vsi-export
      vsi-import policy-name [policy-name...(up to 5 max)]
      no vsi-import
    [no] bgp-ad
      [no] shutdown
      vpls-id vpls-id
      vsi-id
        prefix low-order-vsi-id
        no prefix
    bgp-evpn
      [no] mac-advertisement
      mac-duplication
        detect num-moves num-moves window minutes
        [no] retry minutes
      [no] unknown-mac-route
      vxlan
      [no] shutdown
    bgp-vpls
      max-ve-id value
      no max-ve-id
      ve-name name
      no ve-name
        ve-id ve-id-value
        no ve-id
      [no] shutdown
```
Virtual Private LAN Services

- [no] def-mesh-vc-id vc-id
- default-gtw
  - ip ip-address
  - no ip
  - mac ieve-address
  - no mac
- description description-string
  - no description
- [no] disable-aging
- [no] disable-learning
- [no] discard-unknown
- endpoint endpoint-name [create]
  - no endpoint
    - [no] auto-learn-mac-protect
    - [no] block-on-mesh-failure
    - description description-string
    - no description
    - [no] ignore-standby-signaling
    - [no] mac-pinning
    - max-nbr-mac-addr table-size
    - no max-nbr-mac-addr
    - [no] mc-endpoint
      - mc-ep-peer name
      - mc-ep-peer ip-address
      - no mc-ep-peer
    - restrict-protected-src alarm-only
    - restrict-protected-src [discard-frame]
    - no restrict-protected-src
    - revert-time revert-time | infinite
    - no revert-time
    - static-mac ieve-address [create]
    - no static-mac
    - [no] suppress-standby-signaling
  - eth-cfm
    - [no] mep mep-id domain md-index association ma-index
      - [no] ccm-enable
      - ccm-ltm-priority priority
      - no ccm-ltm-priority
      - [no] description
      - [no] eth-test-enable
        - [no] test-pattern {all-zeros | all-ones} [crc-enable]
        - low-priority-defect {allDef | macRemErrXcon | remErrXcon}
        - mac-address ma-address
        - no mac-address
        - one-way-delay-threshold seconds
        - [no] shutdown
    - tunnel-fault [accept | ignore]
    - [no] fdb-table-high-wmark high-water-mark
    - [no] fdb-table-low-wmark low-water-mark
    - fdb-table-size table-size
    - no fdb-table-size [table-size]
    - igmp-snooping
      - mvr
VPLS Services Command Reference

— description description-string
— no description
— group-policy policy-name
— no group-policy
— [no] shutdown
— query-interval seconds
— no query-interval
— query-src-ip ip-address
— no query-src-ip
— report-src-ip ip-address
— no report-src-ip
— robust-count robust-count
— no robust-count
— [no] shutdown
— [no] interface ip-int-name
— address ip-address[/mask] [netmask]
— no address
— arp-timeout seconds
— no arp-timeout
— description description-string
— no description
— mac ieee-address
— no mac
— [no] shutdown
— static-arp ieee-addr unnumbered
— no static-arp unnumbered
— unnumbered [ip-int-name | ip-address]
— no unnumbered
— isid-policy
— no isid-policy
— entry
— advertise-local
— range isid [to isid]
— [no] use-def-mcast
— local-age aging-timer
— no local-age
— [no] mac-move
— move-frequency frequency
— no move-frequency
— number-retries number-retries
— no number-retries
— primary-ports
— cumulative-factor cumulative-factor
— no cumulative-factor
— [no] sap sap-id
— [no] spoke-sdp spoke-id
— [no] cumulative-factor factor
— retry-timeout timeout
— no retry-timeout
— secondary-ports
— cumulative-factor cumulative-factor
— no cumulative-factor
— [no] sap sap-id
— [no] spoke-sdp spoke-id
— [no] cumulative-factor factor
— [no] shutdown
— mac-protect
  — [no] mac ieee-address
— mac-subnet-length subnet-length
— no mac-subnet-length
— mfib-table-high-wmark high-water-mark
— no mfib-table-high-wmark
— mfib-table-low-wmark low-water-mark
— no mfib-table-low-wmark
— mfib-table-size table-size
— no mfib-table-size
— mld-snooping
  — mvr
    — description description-string
    — no description
    — group-policy policy-name
    — no group-policy
    — [no] shutdown
— query-interval seconds
— no query-interval
— query-src-ip ipv-address
— no query-src-ip
— report-src-ip ipv6-address
— no report-src-ip
— robust-count robust-count
— no robust-count
— [no] shutdown
— mrp
  — [no] attribute-table-size
  — [no] attribute-table-high-wmark
  — [no] attribute-table-low-wmark
  — flood-time flood-time
— no flood-time
— [no] shutdown
— mrp
  — [no] attribute-table-size
  — [no] attribute-table-high-wmark
  — [no] attribute-table-low-wmark
  — flood-time flood-time
— no flood-time
— flood-time
— [no] hold-time value
— [no] shutdown
— multicast-info-policy policy-name
— no multicast-info-policy
— [no] per-service-hashing
— [no] pim-snooping
  — group-policy grp-policy-name [.. grp-policy-name]
  — no group-policy
  — oper-group seconds
  — no oper-group
  — mode mode
— [no] shutdown
— [no] propagate-mac-flush
— [no] propagate-mac-flush-from-bvpls
— remote-age aging-timer
— no remote-age
— send-bvpls-flush {[all-but-mine] [all-from-me]}
— no send-bvpls-flush
— [no] send-flush-on-bvpls-failure
— [no] send-flush-on-failure
— service-mtu octets
— no service-mtu
— service-name service-name
— no service-name
— [no] shutdown
— site name [create]
— no site name
  — boot-timer seconds
  — no boot-timer
  — failed-threshold [1..1000]
  — failed-threshold all
  — [no] mesh-sdp-binding
  — monitor-oper-group name
  — no monitor-oper-group
  — sap sap-id
  — no sap
  — [no] shutdown
  — site-activation-timer seconds
  — no site-activation-timer
  — site-id value
  — no site-id
  — split-horizon-group group-name
  — no split-horizon-group
  — spoke-sdp sdp-id:vc-id
  — no spoke-sdp
— spb [create]
— no spb
  — level [1..1]
    — hello-interval seconds
    — no hello-interval
    — hello-multiplier multiplier
    — no hello-multiplier
    — metric ipv4-metric
    — no metric
    — lsp-pacing-interval milli-seconds
    — no lsp-pacing-interval
    — retransmit-interval seconds
    — no retransmit-interval
    — [no] shutdown
— [no] split-horizon-group group-name [residential-group]
  — [no] auto-learn-mac-protect
  — description description-string
  — no description
  — restrict-protected-src alarm-only
  — restrict-protected-src alarm-only
  — restrict-protected-src [discard-frame]
  — no restrict-protected-src
— static-mac
— mac ieee-address [create ] sap sap-id [monitor fwd-status]
— mac ieee-address [create ] spoke-sdp sd-id:vc-id [monitor fwd-status]
— [no] mac ieee-address

— stp
— forward-delay forward-delay
— no forward-delay
— hello-time hello-time
— no hello-time
— hold-count BDPU tx hold count
— no hold-count
— max-age max-info-age
— no max-age
— mode [rstp | comp-dot1w | dot1w | mstp | pmstp]
— no mode
— [no] mst-instance mst-inst-number
   — mst-priority bridge-priority
   — no mst-priority
   — [no] vlan-range vlan-range
— mst-max-hops hops-count
— no mst-max-hops
— mst-name region-name
— no mst-name
— mst-revision revision-number
— no mst-revision
— priority bridge-priority
— no priority
— [no] shutdown

— vpls-group id
— service-range startid-endid [vlan-id startvid]
— vpls-template-binding name/id
— vpls-sap-template-binding name/id
— [no] mvrp-control

— vxlan vni vni-id create
— no vxlan vni
SAP Commands

```
config
  service
    vpls service-id [customer customer-id] [vpn vpn-id] [m-vpls] [b-vpls | i-vpls] [create]
    no vpls service-id
      sap sap-id [split-horizon-group group-name] [create]
      no sap sap-id
        accounting-policy acct-policy-id
        no accounting-policy
        [no] auto-learn-mac-protect
        app-profile app-profile-name
        no app-profile
        arp-host
          host-limit max-num-hosts
          no host-limit
          min-auth-interval min-auth-interval
          no min-auth-interval
          [no] shutdown
        [no] auto-learn-mac-protect
        [no] app-profile
        arp-reply-agent [sub-ident]
        no arp-reply-agent
        atm
          egress
            traffic-desc traffic-desc-profile-id
            no traffic-desc
          encapsulation atm-encap-type
          ingress
            traffic-desc traffic-desc-profile-id
            no traffic-desc
        [no] atm
        [no] alarm-cells
        bpdu-translation {auto | pvst | stp}
        no bpdu-translation
        [no] cflowd
        [no] collect-stats
        description description-string
        no description
        [no] disable-aging
        [no] disable-learning
        [no] discard-unknown
        egress
          [no] agg-rate
          [no] limit-unused-bandwidth
          [no] queue-frame-based-accounting
          rate {max | rate}
          no rate
        encap-defined-qos
          encap-group group-name [type group-type] [qos-per-member] [create]
          no encap-group group-name
            [no] agg-rate
            [no] limit-unused-bandwidth
            [no] queue-frame-based-accounting
            rate {max | rate}
            no rate
```
— [no] member encap-id [to encap-id]
— qos policy-id
— no qos
— scheduler-policy scheduler-policy-name
— no scheduler-policy

— filter ip ip-filter-id
— filter ipv6 ipv6-filter-id
— filter mac mac-filter-id
— no filter

— no filter [ip ip-filter-id] [mac mac-filter-id] [ipv6 ipv6-filter-id]
— [no] hsmda-queue-override
— secondary-shaper secondary-shaper-name
— no secondary-shaper
— wrr-policy hsmda-wrr-policy-name
— no wrr-policy
— packet-byte-offset {add add-bytes | subtract sub-bytes}
— no packet-byte-offset
— queue queue-id
— no queue queue-id
— wrr-weight weight
— no wrr-weight
— mbs size [bytes | kilobytes] [default]
— no mbs
— rate pir-rate
— no rate
— slope-policy hsmda-slope-policy-name allowable
— no slope-policy

— multicast-group group-name
— no multicast-group
— policer-control-override [create]
— no policer-control-override
— max-rate {rate | max}
— priority-mbs-thresholds
— min-thresh-separation size [bytes | kilobytes]
— [no] priority level
— mbs-contribution size [bytes | kilobytes]

— policer-control-policy policy-name
— no policer-control-policy
— [no] policer-override
— policer policer-id [create]
— no policer policer-id
— cbs size [bytes | kilobytes]
— no cbs
— mbs size [bytes | kilobytes]
— no mbs
— packet-byte-offset {add add-bytes | subtract sub-bytes}
— rate {rate | max} [cir {max | rate}]
— stat-mode stat-mode
— no stat-mode

— [no] qinq-mark-top-only
— qos policy-id [port-redirect-group queue-group-name instance instance-id]
— no qos
— [no] queue OVERRIDE
  — [no] queue queue-id
    — adaptation-rule [pir adaptation-rule] [cir adaptation-rule]
    — no adaptation-rule
    — avg-frame-overhead percentage
    — no avg-frame-overhead
    — cbs size-in-kbytes
    — no cbs
    — high-prio-only percent
    — no high-prio-only
    — mbs size-in-kbytes
    — no mbs
    — rate pir-rate [cir cir-rate]
    — no rate
    — wred-queue-policy slope-policy-name
    — no wred-queue-policy
  — [no] scheduler OVERRIDE
    — [no] scheduler scheduler-name
    — rate pir-rate [cir cir-rate]
    — no rate
    — scheduler-policy scheduler-policy-name
    — no scheduler-policy
— eth-cfm
  — mep mep-id domain md-index association ma-index [direction {up | down}] primary-vlan-enable [vlan vlan-id]
  — no mep mep-id domain md-index association ma-index
    — [no] ais-enable
      — [no] interface-support-enable
    — [no] interface-support-enable
    — ccm-padding-size ccm-padding
    — no ccm-padding-size ccm-padding
    — [no] csf-enable
      — multiplier multiplier-value
      — no multiplier
    — client-meg-level [level [level...]]
    — no client-meg-level
    — [no] description
    — interval {1 | 60}
    — no interval
    — priority priority-value
    — no priority
    — [no] ccm-enable
    — ccm-ltm-priority priority
    — no ccm-ltm-priority
    — [no] eth-test-enable
      — test-pattern {all-zeros | all-ones} [crc-enable]
      — no test-pattern
    — fault-propagation-enable {use-if-tlv | suspend-ccm}
    — no fault-propagation-enable
  — low-priority-defect {allDef | macRemErrXcon | remErrXcon | errXcon | xcon | noXcon}
    — mac-address mac-address
— no mac-address
— one-way-delay-threshold seconds
— [no] shutdown
— [no] squelch-ingress-levels [md-level [md-level...]]
— [no] mip [{mac mac-address | default-mac}]
— tunnel-fault [accept | ignore]
— vmeq-extensions
— vmeq-filter

— eth-tunnel
  — path path-index tag qtag[.qtag]
  — no path path-index
  — [no] mip
— fault-propagation-bmac [mac-name | ieee-address] [create]
— no fault-propagation-bmac [mac-name | ieee-address]
— [no] feature
— [no] force-l2pt-boundary
— frame-relay
  — [no] frf-12
  — ete-fragment-threshold threshold
  — no ete-fragment-threshold
  — [no] interleave
  — scheduling-class class-id
  — no scheduling-class
— host-connectivity-verify source-ip ip-address [source-mac ieee-address]
  [interval interval] [action {remove | alarm}]
— igmp-host-tracking
  — expiry-time expiry-time
  — no expiry-time
  — import policy-name
  — no import
— max-num-groups max-num-groups
— no max-num-groups
— max-num-sources max-num-sources
— no max-num-sources
— max-num-grp-sources [1..32000]
— no max-num-grp-sources
— igmp-snooping
  — [no] fast-leave
  — import policy-name
  — no import
  — last-member-query-interval interval
  — no last-member-query-interval
— max-num-groups max-num-groups
— no max-num-groups
— max-num-sources max-num-sources
— no max-num-sources
— max-num-grp-sources [1..32000]
— no max-num-grp-sources
— mcac
  — mc-constraints
    — level level-id bw bandwidth
    — no level level-id
VPLS Services Command Reference

— number-down number-lag-port-down level level-
id
— no number-down
— policy policy-name
— no policy
— unconstrained-bw bandwidth mandatory-bw mandatory-bw
— no unconstrained-bw
— [no] mrouter-port
— mvr
  — from-vpls vpls-id
  — no from-vpls
  — to-sap sap-id
  — no to-sap
— query-interval interval
— no query-interval
— query-response-interval interval
— no query-response-interval
— robust-count count
— no robust-count
— [no] send-queries
— static
  — [no] group group-address
  — [no] source ip-address
  — [no] starg
— version version
— no version
— ingress
  — filter ip ip-filter-id
  — filter ipv6 ipv6-filter-id
  — filter mac mac-filter-id
  — no filter [ip ip-filter-id] [mac mac-filter-id] [ipv6 ipv6-filter-id]
  — match-qinq-dot1p {top | bottom}
  — no match-qinq-dot1p de
  — policer-control-override [create]
  — no policer-control-override
    — max-rate {rate | max}
    — priority-mbs-thresholds
      — min-thresh-separation size [bytes | kilobytes]
      — [no] priority level
      — mbs-contribution size [bytes | kilobytes]
  — policer-control-policy policy-name
  — no policer-control-policy
  — [no] policer-override
    — policer policer-id [create]
    — no policer policer-id
      — cbs size [bytes | kilobytes]
      — no cbs
      — mbs size [bytes | kilobytes]
      — no mbs
      — packet-byte-offset {add add-bytes | subtract sub-bytes}
      — rate {rate | max} [cir {max | rate}]
      — stat-mode stat-mode
      — no stat-mode
— qos policy-id [shared-queuing | multipoint-shared] [fp-redirect-group queue-group-name instance instance-id]
— no qos
— [no] queue-override
— [no] queue queue-id
— adaptation-rule [pir {max|min|closest}] [cir {max | min | closest}]
— no adaptation-rule
— cbs size-in-kbytes
— no cbs
— high-prio-only percent
— no high-prio-only
— mbs size-in-kbytes
— no mbs
— rate pir-rate [cir cir-rate]
— no rate
— [no] scheduler-override
— [no] scheduler scheduler-name
— rate pir-rate [cir cir-rate]
— no rate
— scheduler-policy scheduler-policy-name
— no scheduler-policy
— vlan-translation {vlan-id | copy-outer}
— no vlan-translation
— 12pt-termination [cdp] [dtp] [pagp] [stp] [udld] [vtp]
— no 12pt-termination
— lag-link-map-profile link-map-profile-id
— no lag-link-map-profile
— limit-mac-move [blockable | non-blockable]
— no limit-mac-move
— [no] mac-pinning
— managed-vlan-list
— [no] default-sap
— [no] range vlan-range
— max-nbr-mac-addr table-size
— no max-nbr-mac-addr
— mld-snooping
— [no] fast-leave
— import policy-name
— no import
— last-member-query-interval interval
— no last-member-query-interval
— max-num-groups max-num-groups
— no max-num-groups
— mvr
— fast-leave
— no fast-leave
— to-sap sap-id
— no to-sap
— query-interval seconds
— no query-interval
— query-response-interval seconds
— no query-response-interval
— robust-count robust-count
— no robust-count
— [no] send-queries
— mrp
— [no] join-time value
— [no] leave-all-time value
— [no] leave-time value
— [no] mrp-policy policy-name
— [no] periodic-time value
— [no] periodic-time
— mvrp
— endstation-vid-group id vlan-id startvid-endvid
— [no] shutdown
— monitor-oper-group group-name
— no monitor-oper-group
— oper-group group-name
— no oper-group
— multi-service-site customer-site-name
— no multi-service-site
— pim-snooping
— max-num-groups num-groups
— [no] monitor-oper-group name
— [no] oper-group name
— restrict-protected-src alarm-only
— restrict-protected-src [discard-frame]
— no restrict-protected-src
— restrict-unprotected-dst alarm-only
— no restrict-unprotected-dst
— [no] shutdown
— [no] static-isid range entry-id isid [to isid] [create]
— [no] static-mac ieee-address
— stp
— [no] auto-edge
— [no] edge-port
— link-type {pt-pt | shared}
— no link-type [pt-pt | shared]
— mst-instance mst-inst-number
— mst-path-cost inst-path-cost
— no mst-path-cost
— mst-priority bridge-priority
— no mst-priority
— path-cost sap-path-cost
— no path-cost
— [no] port-num virtual-port-number
— priority stp-priority
— no priority
— [no] vpls-group
— [no] shutdown
— tod-suite tod-suite-name
— no tod-suite
Template Commands

```
config
    service
        template
            vpls-template name/id create
                [no] temp-flooding flood-time
                [no] disable-aging
                [no] disable-learning
                [no] discard-unknown
                [no] fdb-table-high-wmark high-water-mark
                [no] fdb-table-low-wmark low-water-mark
                fdb-table-size table-size
                no fdb-table-size [table-size]
                local-age aging-timer
                no local-age
                [no] mac-move
                    move-frequency frequency
                    [no] move-frequency
                    number-retries number-retries
                    [no] number-retries
                    primary-ports
                        cumulative-factor cumulative-factor
                        [no] cumulative-factor
                    retry-timeout timeout
                    [no] retry-timeout
                    secondary-ports
                        cumulative-factor cumulative-factor
                        [no] cumulative-factor
                    [no] shutdown
                [no] per-service-hashing
                remote-age aging-timer
                [no] remote-age
                service-mtu octets
                [no] service-mtu
                stp
                    forward-delay forward-delay
                    [no] forward-delay
                    hello-time hello-time
                    [no] hello-time
                    hold-count BDPU tx hold count
                    [no] hold-count
                    max-age max-info-age
                    [no] max-age
                    mode [rstp | comp-dot1w | dot1w | mstp | pmstp]
                    [no] mode
                    priority bridge-priority
                    [no] priority
                    [no] shutdown
            vpls-sap-template name/id create
                12pt-termination [cdp] [dtp] [pagp] [stp] [udld] [vtp]
                [no] 12pt-termination
                bpdu-translation {auto | pvst | stp}
                [no] bpdu-translation
```
— [no] collect-stats
— eth-cfm
  — [no] mip primary-vlan-enable [vlan vlan-id]
  — [no] squelch-ingress-levels [md-level [md-level...]]
— [no] disable-aging
— [no] disable-learning
— [no] discard-unknown
— ingress
  — agg-rate-limit agg-rate [queue-frame-based-accounting]
  — no agg-rate-limit
  — [no] agg-rate
    — rate {max | rate}
    — no rate
    — [no] limit-unused-bandwidth
    — [no] queue-frame-based-accounting
  — filter ip ip-filter-id
  — filter ipv6 ipv6-filter-id
  — filter mac mac-filter-id
  — no filter
  — no filter [ip ip-filter-id] [mac mac-filter-id] [ipv6 ipv6-filter-id]
  — policer-control-policy policy-name
  — no policer-control-policy
  — [no] qinq-mark-top-only
  — qos policy-id
  — no qos
  — scheduler-policy scheduler-policy-name
  — no scheduler-policy
— egress
  — agg-rate-limit agg-rate [queue-frame-based-accounting]
  — no agg-rate-limit
  — [no] agg-rate
    — rate {max | rate}
    — no rate
    — [no] limit-unused-bandwidth
    — [no] queue-frame-based-accounting
  — filter ip ip-filter-id
  — filter ipv6 ipv6-filter-id
  — filter mac mac-filter-id
  — no filter
  — no filter [ip ip-filter-id] [mac mac-filter-id] [ipv6 ipv6-filter-id]
  — policer-control-policy policy-name
  — no policer-control-policy
  — [no] qinq-mark-top-only
  — qos policy-id
  — no qos
  — scheduler-policy scheduler-policy-name
  — no scheduler-policy
— limit-mac-move [blockable | non-blockable]
— no limit-mac-move
— max-nbr-mac-addr table-size
— no max-nbr-mac-addr
— stp
  — [no] auto-edge
  — [no] edge-port
  — link-type {pt-pt | shared}
  — no link-type {pt-pt | shared}
  — path-cost sap-path-cost
  — no path-cost
  — priority stp-priority
  — no priority
— [no] vpls-group
— [no] shutdown
— [no] mac-move-level
Mesh SDP Commands

```text
config
    — service
        — [no] vpls service-id [customer customer-id] [vpn vpn-id] [mvpls] [b-vpls|vpls] [create]
        — mesh-sdp sdp-id:[vc-id] [vc-type {ether | vlan}]
        — no mesh-sdp sdp-id:[vc-id]
            — accounting-policy acct-policy-id
            — no accounting-policy
            — [no] auto-learn-mac-protect
            — [no] collect-stats
            — [no] control-word
            — description description-string
            — no description
            — egress
                — filter ip ip-filter-id
                — filter ipv6 ipv6-filter-id
                — filter mac mac-filter-id
                — no filter [ip ip-filter-id] [mac mac-filter-id] [ipv6 ipv6-filter-id]
                — qos network-policy-id port-redirect-group queue-group-name
                    [instance instance-id]
                — no qos
                — mfib-allowed-mda-destinations
                    — [no] mda mda-id
                — vc-label egress-vc-label
                — no vc-label [egress-vc-label]
                — eth-cfm
                    — mep mep-id domain md-index association ma-index [direction {up | down}]
                    — no mep mep-id domain md-index association ma-index primary-vlan-enable [vlan vlan-id]
                        — [no] ais-enable
                            — [no] interface-support-enable
                                — client-meg-level [[level [level...]]]
                                — no client-meg-level
                                — interval {1 | 60}
                                — no interval
                                — priority priority-value
                                — no priority
                        — [no] ccm-enable
                        — ccm-padding-size ccm-padding
                        — no ccm-padding-size ccm-padding
                        — ccm-ltm-priority priority
                        — no ccm-ltm-priority
                        — [no] csf-enable
                            — multiplier multiplier-value
                            — no multiplier
                        — [no] description
                        — [no] eth-test-enable
                            — test-pattern {all-zeros | all-ones} [cre-enable]
                            — no test-pattern
                        — fault-propagation-enable {use-ff-tlv | suspend-ccm}
                        — no fault-propagation-enable
```
— low-priority-defect (allDef | macRemErrXcon | remErrXcon | errXcon | xcon | noXcon)
— mac-address mac-address
— no mac-address
— [no] description
— [no] shutdown
— [no] squelch-ingress-levels [md-level [md-level...]]
— vmep-filter
— fault-propagation-bmac [mac-name | ieee-address] [create]
— no fault-propagation-bmac [mac-name | ieee-address]
— [no] force-vc-forwarding
— [no] hash-label
— igmp-snooping
— [no] disable-router-alert-check
— [no] fast-leave
— import policy-name
— no import
— last-member-query-interval interval
— no last-member-query-interval
— max-num-groups max-num-groups
— no max-num-groups
— max-num-grp-sources [1..32000]
— no max-num-grp-sources
— macac
— policy policy-name
— no policy
— unconstrained-bw bandwidth mandatory-bw mandatory-bw
— no unconstrained-bw
— [no] mrouter-port
— query-interval interval
— no query-interval
— query-response-interval interval
— no query-response-interval
— robust-count count
— no robust-count
— [no] send-queries
— static
— [no] group group-address
— [no] source ip-address
— [no] starg
— version version
— no version
— ingress
— filter ip ip-filter-id
— filter ipv6 ipv6-filter-id
— filter mac mac-filter-id
— no filter [ip ip-filter-id] [mac mac-filter-id] [ipv6 ipv6-filter-id]
— mfib-allowed-uda-destinations
— [no] mda mda-id
— vc-label egress-vc-label
— no vc-label [egress-vc-label]
— [no] mac-pinning
— mld-snooping
— [no] fast-leave
— import policy-name
— no import
— last-member-query-interval interval
— no last-member-query-interval
— max-num-groups max-num-groups
— no max-num-groups
— mvr
  — [no] fast-leave
  — to-sap sap-id
  — no to-sap
  — query-interval seconds
— no query-interval
— query-response-interval seconds
— no query-response-interval
— robust-count robust-count
— no robust-count
— [no] send-queries
— mrp
  — [no] join-time value
  — [no] leave-all-time value
  — [no] leave-time value
  — [no] mrp-policy policy-name
  — [no] periodic-time value
  — [no] periodic-time
— restrict-protected-src alarm-only
— restrict-protected-src [discard-frame]
— no restrict-protected-src
— [no] shutdown
— [no] static-mac ieee-address
— vlan-vc-tag 0..4094
— no vlan-vc-tag [0..4094]
Spoke SDP Commands

```plaintext
config
  service
    — [no] vpls service-id [customer customer-id] [vpn vpn-id] [mvpls] [b-vpls] [vpls] [create]
    — spoke-sdp sdp-id [vc-id] [vc-type {ether | vlan}] [split-horizon-group group-name]
    — no spoke-sdp sdp-id [vc-id]
      — accounting-policy acct-policy-id
      — no accounting-policies
      — app-profile app-profile-name
      — no app-profile
      — [no] auto-learn-mac-protect
      — [no] block-on-mesh-failure
      — bpdu-translation {auto | pvst | stp}
      — no bpdu-translation
      — [no] collect-stats
      — [no] control-word
      — description description-string
      — no description
      — [no] disable-aging
      — [no] disable-learning
      — [no] discard-unknown-source
      — eth-cfm
        — mep mep-id domain md-index association ma-index [direction {up | down}]
        — no mep mep-id domain md-index association ma-index
          — [no] ais-enable
            — [no] interface-support-enable
            — client-meg-level [{level | level...}]
            — no client-meg-level
            — interval {1 | 60}
            — no interval
            — priority priority-value
            — no priority
            — [no] ccm-enable
            — ccm-ltm-priority priority
            — no ccm-ltm-priority
            — ccm-padding-size ccm-padding
            — noccm-padding-size ccm-padding
            — [no] csf-enable
              — multiplier multiplier-value
              — no multiplier
            — [no] description
            — [no] eth-test-enable
              — test-pattern {all-zeros | all-ones} [crc-enable]
              — no test-pattern
            — fault-propagation-enable {use-if-tlv | suspend-ccm}
            — no fault-propagation-enable
            — low-priority-defect {allDef | macRemErrXcon | remErrXcon | errXcon | xcon | noXcon}
            — mac-address mac-address
            — no mac-address
```
— [no] description
— [no] shutdown
— [no] mip [{mac mac-address | default-mac}]
— [no] squelch-ingress-levels [md-level [md-level...]]
— vmep-filter
  — egress
  — filter ip ip-filter-id
  — filter ipv6 ipv6-filter-id
  — filter mac mac-filter-id
  — [no filter [ip ip-filter-id] [mac mac-filter-id] [ipv6 ipv6-filter-id]]
  — qos network-policy-id port-redirect-group queue-group-name [instance instance-id]
  — [no] qos
  — mfib-allowed-mda-destinations
    — [no] mda mda-id
  — vc-label egress-vc-label
  — [no vc-label [egress-vc-label]]
  — fault-propagation-bmac [mac-name | ieee-address] [create]
  — [no] fault-propagation-bmac [mac-name | ieee-address]
  — [no] force-vlan-vc-forwarding
  — hash-label
  — [no] hash-label
  — igmp-snooping
    — [no] fast-leave
    — import policy-name
    — [no import]
    — last-member-query-interval interval
    — [no last-member-query-interval]
    — max-num-groups max-num-groups
    — [no max-num-groups]
    — max-num-grp-sources [1..32000]
    — [no max-num-grp-sources]
    — mcac
      — policy policy-name
      — [no policy]
      — unconstrained-bw bandwidth mandatory-bw mandatory-bw
      — [no unconstrained-bw]
      — [no] mrouter-port
      — query-interval interval
      — [no query-interval]
      — query-response-interval interval
      — [no query-response-interval]
      — robust-count count
      — [no robust-count]
      — [no] send-queries
      — static
        — [no] group group-address
        — [no] source ip-address
        — [no] starg
        — version version
        — [no version]
    — [no] ignore-standby-signaling
    — ingress
      — filter ip ip-filter-id
— filter ipv6 ipv6-filter-id
— filter mac mac-filter-id
— no filter [ip ip-filter-id] [mac mac-filter-id] [ipv6 ipv6-filter-id]
— mfib-allowed-mda-destinations
    — no mda mda-id
— vc-label egress-vc-label
— no vc-label [egress-vc-label]
— [no] l2pt-termination
— limit-mac-move [blockable | non-blockable]
— no limit-mac-move
— [no] mac-pinning
— max-nbr-mac-addr table-size
— no max-nbr-mac-addr
— mid-snooping
    — [no] fast-leave
    — import policy-name
    — no import
— last-member-query-interval interval
— no last-member-query-interval
— max-num-groups max-num-groups
— no max-num-groups
— query-interval seconds
— no query-interval
— query-response-interval seconds
— no query-response-interval
— robust-count robust-count
— no robust-count
— [no] send-queries
— monitor-oper-group group-name
— no monitor-oper-group
— oper-group group-name
— no oper-group
— mrg
    — [no] join-time value
    — [no] leave-all-time value
    — [no] leave-time value
— no mrp-policy policy-name
— [no] periodic-time value
— oper-group group-name
— no oper-group
— pim-snooping
    — max-num-groups num-groups
— no monitor-oper-group name
— [no] oper-group name
— precedence precedence-value | primary
— no precedence
— [no] pw-status-signaling
— propagate-mac-flush [precedence-value | primary]
— no propagate-mac-flush
— [no] shutdown
— [no] static-isid range entry-id isid [to isid] [create]
— [no] static-mac lee-address
— stp
    — [no] auto-edge
— [no] edge-port
— link-type {pt-pt | shared}
— no link-type [pt-pt | shared]
— path-cost sap-path-cost
— no path-cost
— [no] port-num virtual-port-number
— priority stp-priority
— no priority
— [no] vpls-group
— [no] shutdown
  — transit-policy prefix prefix-aasub-policy-id
— no transit-policy
— vlan-vc-tag 0..4094
— no vlan-vc-tag [0..4094]
Provider Tunnel Commands

```
config
  service
    [no] vpls service-id [customer customer-id] [vpn vpn-id] [mvpls] [b-vpls|i-vpls] [create]
    provider-tunnel
      inclusive
        data-delay-interval seconds
        no data-delay-interval
        mldp
        [no] mldp
        [no] root-and-leaf
        [no] rsvp
          lsp-template p2mp-lsp-template-name
          no lsp-template
        [no] shutdown
```
Egress Multicast Group Commands

```
config
  service
    egress-multicast-group group-name [create]
    no egress-multicast-group group-name
      description description-string
      no description
      dest-chain-limit destinations per pass
      no dest-chain-limit
      sap-common-requirements
        dot1q-etype 0x0600..0xffff
        no dot1q-etype
        egress-filter [ip ip-filter-id]
        egress-filter [ipv6 ipv6-filter-id]
        egress-filter [mac mac-filter-id]
        no egress-filter [ip ip-filter-id] [ipv6 ipv6-filter-id] [mac mac-filter-id]
        encap-type {dot1q | null}
        no encap-type
        qinq-etype [0x0600..0xffff]
        no qinq-etype
        qinq-fixed-tag-value tag-value
        no qinq-fixed-tag-value

config
  service
    [no] vpls service-id [customer customer-id] [vpn vpn-id] [mvpls] [b-vpls|i-vpls] [create]
    sap sap-id [split-horizon-group group-name]
    no sap sap-id
      egress
        multicast-group group-name
        no multicast-group
```
Provider Edge Discovery Policy Commands

config
  — service
    — [no] pe-discovery-policy name
    — password password
    — no password
    — polling-interval minutes
    — no polling-interval
    — server server-index address ip-address secret key [hash | hash2] [port port-num]
    — no server server-index
    — timeout seconds
    — no timeout

Routed VPLS Commands

config
  — service
    — vpls service-id [customer customer-id] [vpn vpn-id] [m-vpls] [b-vpls | i-vpls] [create]
      — service-name service-name
      — no service-name
      — [no] allow-ip-int-binding
Show Commands

show
  — service
    — egress-label egress-label1 [egress-label2]
    — fdb-info
    — fdb-mac ieee-address [expiry]
    — id service-id
      — all
      — base
      — bgp-evpn
      — fdb [sap sap-id] [expiry] | [sdp sdp-id [expiry]] | [mac ieee-address [expiry]] | endpoint endpoint | [detail] [expiry] | pbb
    — igmp-snooping
      — all
      — base
      — mrouters [detail]
      — proxy-db [detail]
      — proxy-db [group grp-ip-address]
      — querier
      — static [sap sap-id | sdp sdp-id:vc-id]
    — isid-policy
    — labels
    — l2pt disabled
    — l2pt [detail]
    — mac-move
    — mac-protect
    — mfib [brief | statistics] [ip | mac] brief
    — mfib [group grp-address | *) [statistics]
    — proxy-arp [ip-address ip-address]
    — sap [sap-id [detail]]
    — sdp [sdp-id | far-end ip-addr] [detail]
    — sdp sdp-id:vc-id [mrp | mmrp]
    — site [detail]
    — site name
    — split-horizon-group [group-name]
    — stp mst-instance mst-inst-number
    — stp [detail]
    — vxlan
      — ingress-label start-label [end-label]
      — isid-using [ISID]
      — sap-using [sap sap-id]
      — sap-using interface [ip-address | ip-int-name]
      — sap-using [ingress | egress] atm-td-profile id-profile-id
      — sap-using [ingress | egress] filter filter-id
      — sap-using [ingress | egress] qos-policy qos-policy-id
      — sap-using authentication-policy policy-name
      — sdp [sdp-id | far-end ip-address] [detail | keep-alive-history]
      — sdp [sdp-id:vc-id] | far-end ip-address]
      — sdp [sdp-id | far-end ip-addr] [detail | keep-alive-history]
      — sdp-using [sdp-id:vc-id] | far-end ip-address]
      — service-using [vpls][b-vpls] [l-vpls] [m-vpls]
      — vxlan
Clear Commands

clear
   — service
      — id service-id
         — fdb {all | mac ieee-address | sap sap-id | mesh-sdp sdp-id[:vc-id] | spoke-sdp sdp-id[:vc-id]}
         — igmp-snooping
            — port-db sap sap-id [group grp-address [source ip-address]]
            — port-db sdp sdp-id[:vc-id] [group grp-address [source ip-address]]
            — querier
         — mesh-sdp sdp-id[:vc-id] ingress-vc-label
         — spoke-sdp sdp-id[:vc-id] ingress-vc-label
         — stp
            — detected-protocols [all | sap sap-id | spoke-sdp [sdp-id[:vc-id]]]
   — statistics
      — id service-id
         — counters
         — l2pt
         — mesh-sdp sdp-id[:vc-id] {all | counters | stp | mrp}
         — spoke-sdp sdp-id[:vc-id] {all | counters | stp | l2pt | mrp}
         — stp
      — sap sap-id {all | cem | counters | l2pt | stp | mrp}
      — sdp sap-id {keep alive}
Debug Commands

debug
  — service
    — id service-id
      — [no] arp-host
      — igmp-snooping
        — detail-level {low | medium | high}
        — no detail-level
        — [no] mac ieee-address
        — mode {dropped-only | ingr-and-dropped | egr-ingr-and-dropped}
        — no mode
        — [no] sap sap-id
        — [no] sdp sdp-id:vc-id
      — mld-snooping
        — detail-level {low | medium | high}
        — no detail-level
        — [no] mac ieee-address
        — mode {dropped-only | ingr-and-dropped | egr-ingr-and-dropped}
        — no mode
        — [no] sap sap-id
        — [no] sdp sdp-id:vc-id
      — [no] mrp
        — all-events
        — [no] applicant-sm
        — [no] leave-all-sm
        — [no] mmrp-mac ieee-address
        — [no] mrpdu
        — [no] periodic-sm
        — [no] registrant-sm
        — [no] sap sap-id
        — [no] sdp sdp-id:vc-id
      — [no] event-type {config-change | svc-oper-status-change | sap-oper-status-change | sdpbind-oper-status-change}
        — [no] host-connectivity-verify
          — [no] ip ip-address
          — [no] mac ieee-address
          — [no] sap sap-id
      — [no] sap sap-id
      — stp
        — all-events
        — [no] bpdu
        — [no] core-connectivity
        — [no] exception
        — [no] fsm-state-changes
        — [no] fsm-timers
        — [no] port-role
        — [no] port-state
        — [no] sap sap-id
        — [no] sdp sdp-id:vc-id

Tools Commands

tools
Refer to the 7950 OS OAM and Diagnostic Guide for information about CLI commands and syntax for OAM and diagnostics commands.
Virtual Private LAN Services

VPLS Service Configuration Commands

Generic Commands

shutdown

Syntax  [no] shutdown

Context  config>service>vpls
        config>service>vpls>snooping
        config>service>vpls>igmp-snooping
        config>service>vpls>mac-move
        config>service>vpls>gsmp
        config>service>vpls>gsmp>group
        config>service>vpls>gsmp>group>neighbor
        config>service>vpls>interface
        config>service>vpls>split-horizon-group
        config>service>vpls>sap
        config>service>vpls>sap>stp
        config>service>vpls>sap>arp-host
        config>service>vpls>sap>sub-sla-mgmt
        config>service>vpls>mesh-sdp
        config>service>vpls>spoke-sdp
        config>service>vpls>spoke-sdp>stp
        config>service>vpls>stp
        config>service>vpls>spoke-sdp>stp
        config>service>vpls>mrp
        config>service>vpls>mesh-sdp>eth-cfm>mep
        config>service>vpls>sap>eth-cfm>mep
        config>service>vpls>>spoke-sdp>eth-cfm>mep
        config>service>vpls>bgp-ad
        config>service>vpls>eth-cfm>mep
        config>service>vpls>mesh-sdp>eth-cfm>mep
        config>service>vpls>>spoke-sdp>eth-cfm>mep

Description  This command administratively disables an entity. When disabled, an entity does not change, reset, or remove any configuration settings or statistics.

The operational state of the entity is disabled as well as the operational state of any entities contained within. Many objects must be shut down before they may be deleted.

Services are created in the administratively down (shutdown) state. When a no shutdown command is entered, the service becomes administratively up and then tries to enter the operationally up state. Default administrative states for services and service entities is described below in Special Cases.

The no form of this command places the entity into an administratively enabled state.
### Special Cases

**Service Admin State** — Bindings to an SDP within the service will be put into the out-of-service state when the service is shutdown. While the service is shutdown, all customer packets are dropped and counted as discards for billing and debugging purposes.

**Service Operational State** — A service is regarded as operational providing that two SAPs or if one SDP are operational.

**SDP (global)** — When an SDP is shutdown at the global service level, all bindings to that SDP are put into the out-of-service state and the SDP itself is put into the administratively and operationally down states. Packets that would normally be transmitted using this SDP binding will be discarded and counted as dropped packets.

**SDP (service level)** — Shutting down an SDP within a service only affects traffic on that service from entering or being received from the SDP. The SDP itself may still be operationally up for other services.

**SDP Keepalives** — Enables SDP connectivity monitoring keepalive messages for the SDP ID. Default state is disabled (shutdown) in which case the operational state of the SDP-ID is not affected by the keepalive message state.

**VPLS SAPs and SDPs** — SAPs are created in a VPLS and SDPs are bound to a VPLS in the administratively up default state. The created SAP will attempt to enter the operationally up state. An SDP will attempt to go into the in-service state once bound to the VPLS.

### description

**Syntax**

```
description description-string
no description
```

**Context**

```
config>service>vpls
config>service>vpls>gsmp>group
config>service>vpls>gsmp>group>neighbor
config>service>vpls>igmp-snooping>mvr
config>service>vpls>interface
config>service>vpls>split-horizon-group
config>service>vpls>sap
config>service>vpls>spoke-sdp
config>service>vpls>sap>dhcp
config>service>vpls>mld-snooping>mvr
```

**Description**

This command creates a text description stored in the configuration file for a configuration context. The `description` command associates a text string with a configuration context to help identify the content in the configuration file.

The `no` form of this command removes the string from the configuration.

**Default**

No description associated with the configuration context.

**Parameters**

`string` — The description character string. Allowed values are any string up to 80 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.
VPLS Service Commands

vpls

Syntax

vpls service-id customer customer-id vpn vpn-id [m-vpls] [bvpls | i-vpls] [create]
no vpls service-id

Context

config>service

Description

This command creates or edits a Virtual Private LAN Services (VPLS) instance. The vpls command is used to create or maintain a VPLS service. If the service-id does not exist, a context for the service is created. If the service-id exists, the context for editing the service is entered.

A VPLS service connects multiple customer sites together acting like a zero-hop, Layer 2 switched domain. A VPLS is always a logical full mesh.

When a service is created, the create keyword must be specified if the create command is enabled in the environment context. When a service is created, the customer keyword and customer-id must be specified and associates the service with a customer. The customer-id must already exist having been created using the customer command in the service context. Once a service has been created with a customer association, it is not possible to edit the customer association. The service must be deleted and recreated with a new customer association.

Once a service is created, the use of the customer customer-id is optional for navigating into the service configuration context. Attempting to edit a service with the incorrect customer-id specified will result in an error.

More than one VPLS service may be created for a single customer ID.

By default, no VPLS instances exist until they are explicitly created.

The no form of this command deletes the VPLS service instance with the specified service-id. The service cannot be deleted until all SAPs and SDPs defined within the service ID have been shutdown and deleted, and the service has been shutdown.

Parameters

service-id — The unique service identification number identifying the service in the service domain. This ID must be unique to this service and may not be used for any other service of any type. The service-id must be the same number used for every router on which this service is defined.

Values

service-id: 1 — 2147483648
svc-name: 64 characters maximum

customer customer-id — Specifies the customer ID number to be associated with the service. This parameter is required on service creation and optional for service editing or deleting.

Values

1 — 2147483647

vpn vpn-id — Specifies the VPN ID number which allows you to identify virtual private networks (VPNs) by a VPN identification number.

Values

1 — 2147483647

Default

null (0)
m-vpls — Specifies a management VPLS.

b-vpls | i-vpls — Creates a backbone-vpls or ISID-vpls.

**backbone-smac**

**Syntax**
```
backbone-smac ieee-address
```

**Context**
```
config>service>vpls
```

**Description**
This command configures the backbone source MAC address used for PBB. This command allows a per B-VPLS control of the B-SMAC and the B-Mcast MAC. All I-VPLS provisioned under this B-VPLS will share the provisioned value.

**Default**
backbone-smac address is chassis MAC address

**Parameters**
```
ieee-address — Specifies the backbone source MAC address.
```

**backbone-vpls**

**Syntax**
```
backbone-vpls vpls-id[:isid]
```

**Context**
```
config>service>vpls
```

**Description**
This command associated the I-VPLS with the B-VPLS service. The ISID value is used to mux/demux packets for the VPLS flowing through the B-VPLS.

**Parameters**
```
vpls-id — This value represents the VPLS ID value associated with the B-VPLS.
```

```
isid — Defines ISID associated with the I-VPLS.
```

**Default**
The default is the service-id.

**Values**
```
0 — 16777215
```

**stp**

**Syntax**
```
[no] stp
```

**Context**
```
config>service>vpls>backbone-vpls
```

**Description**
This command enables STP on the backbone VPLS service.

The **no** form of the command disables STP on the backbone VPLS service.
block-on-mesh-failure

**Syntax**  
`[no] block-on-mesh-failure`

**Context**  
`config>service>vpls>spoke-sdp`
`config>service>vpls>endpoint`

**Description**  
This command enables blocking (brings the entity to an operationally down state) after all configured SDPs or endpoints are in operationally down state. This event is signalled to corresponding T-LDP peer by withdrawing service label (status-bit-signaling non-capable peer) or by setting “PW not forwarding” status bit in T-LDP message (status-bit-signaling capable peer).

**Default**  
disabled

bpdu-translation

**Syntax**  
`bpdu-translation {auto | pvst | stp}
no bpdu-translation`

**Context**  
`config>service>vpls>spoke-sdp`
`config>service>vpls>sap`

**Description**  
This command enables the translation of BPDUs to a given format, meaning that all BPDUs transmitted on a given SAP or spoke SDP will have a specified format.

The **no** form of this command reverts to the default setting.

**Default**  
no bpdu-translation

**Parameters**

- **auto** — Specifies that appropriate format will be detected automatically, based on type of bpdus received on such port.
- **pvst** — Specifies the BPDU-format as PVST. Note that the correct VLAN tag is included in the payload (depending on encapsulation value of outgoing SAP).
- **stp** — Specifies the BPDU-format as STP.

cflowd

**Syntax**  
`[no] cflowd`

**Context**  
`config>service>vpls>sap`

**Description**  
This command enables cflowd to collect traffic flow samples through a service interface (SAP) for analysis. When cflowd is enabled on an ethernet service SAP, the ethernet traffic can be sampled and processed by the system’s cflowd engine and exported to IPFIX collectors with the I2-ip template enabled.

cflowd is used for network planning and traffic engineering, capacity planning, security, application and user profiling, performance monitoring, usage-based billing, and SLA measurement. When cflowd is enabled at the SAP level, all packets forwarded by the interface are subjected to analysis according to the cflowd configuration.
For L2 services, only ingress sampling is supported.

**Default**  
no cflowd

### lag-link-map-profile

**Syntax**  
lag-link-map-profile link-map-profile-id  
nolag-link-map-profile

**Context**  
config>service>vpls>sap

**Description**  
This command assigns a pre-configured lag link map profile to a SAP/network interface configured on a LAG or a PW port that exists on a LAG. Once assigned/de-assigned, the SAP/network interface egress traffic will be re-hashed over LAG as required by the new configuration.  
The no form of this command reverts the SAP/network interface to use per-flow, service or link hash as configured for the service/LAG.

**Default**  
nolag-link-map-profile

**Parameters**  
link-map-profile-id — An integer from 1 to 64 that defines a unique lag link map profile on which the LAG the SAP/network interface exist.

### l2pt-termination

**Syntax**  
l2pt-termination [cdp] [dtp] [pagp] [stp] [udld] [vtp]  
nol2pt-termination

**Context**  
config>service>vpls>spoke-sdp  
config>service>vpls>sap

**Description**  
This command enables Layer 2 Protocol Tunneling (L2PT) termination on a given SAP or spoke SDP. L2PT termination will be supported only for STP BPDUs. PDUs of other protocols will be discarded.  
This feature can be enabled only if STP is disabled in the context of the given VPLS service.

**Default**  
nol2pt-termination

**Parameters**  
cdp — Specifies the Cisco discovery protocol.  
dtp — Specifies the dynamic trunking protocol.  
pagp — Specifies the port aggregation protocol.  
stp — Specifies all spanning tree protocols: stp, rstp, mstp, pvst (default).  
uddl — Specifies unidirectional link detection.  
vtp — Specifies the virtual trunk protocol.
def-mesh-vc-id

**Syntax**  
[no] def-mesh-vc-id vc-id

**Context**  
config>service>vpls

**Description**  
This command configures the value used by each end of a tunnel to identify the VC. If this command is not configured, then the service ID value is used as the VC-ID. This VC-ID is used instead of a label to identify a virtual circuit. The VC-ID is significant between peer nodes on the same hierarchical level. The value of a VC-ID is conceptually independent from the value of the label or any other datalink specific information of the VC.

The no form of this command disables the VC-ID.

**Default**  
none

**Parameters**  
vc-id — Specifies the default mesh vc-id.

**Values**  
1 — 4294967295

default-gtw

**Syntax**  
default-gtw

**Context**  
config>service>vpls

**Description**  
This command configures a service default gateway.

ip

**Syntax**  
ip ip-address  
no ip

**Context**  
config>service>vpls>defgw

**Description**  
This command configures the default gateway IP address.

mac

**Syntax**  
mac ieee-address

**Context**  
config>service>vpls>defgw

**Description**  
This command configures the default gateway MAC address.

disable-aging

**Syntax**  
[no] disable-aging
VPLS Service Commands

**Context**
- config>service>vpls
- config>service>vpls>spoke-sdp
- config>service>vpls>sap
- config>template>vpls-template

**Description**
This command disables MAC address aging across a VPLS service or on a VPLS service SAP or spoke SDP.

Like in a Layer 2 switch, learned MACs can be aged out if no packets are sourced from the MAC address for a period of time (the aging time). In each VPLS service instance, there are independent aging timers for local learned MAC and remote learned MAC entries in the VPLS forwarding database (FDB). The `disable-aging` command turns off aging for local and remote learned MAC addresses.

When **no disable-aging** is specified for a VPLS, it is possible to disable aging for specific SAPs and/or spoke SDPs by entering the `disable-aging` command at the appropriate level.

When the `disable-aging` command is entered at the VPLS level, the `disable-aging` state of individual SAPs or SDPs will be ignored.

The **no** form of this command enables aging on the VPLS service.

**Default**
no disable-aging

**disable-learning**

**Syntax**
- **[no]** disable-learning

**Context**
- config>service>vpls
- config>service>vpls>sap
- config>service>vpls>spoke-sdp
- config>template>vpls-template

**Description**
This command disables learning of new MAC addresses in the VPLS forwarding database (FDB) for the service instance, SAP instance or spoke SDP instance.

When **disable-learning** is enabled, new source MAC addresses will not be entered in the VPLS service forwarding database. This is true for both local and remote MAC addresses.

When **disable-learning** is disabled, new source MAC addresses will be learned and entered into the VPLS forwarding database.

This parameter is mainly used in conjunction with the `discard-unknown` command.

The **no** form of this command enables learning of MAC addresses.

**Default**
no disable-learning (Normal MAC learning is enabled)

**discard-unknown**

**Syntax**
- **[no]** discard-unknown

**Context**
- config>service>vpls
- config>template>vpls-template

**Page 750**
Virtual Private LAN Services

**Description**

By default, packets with unknown destination MAC addresses are flooded. If discard-unknown is enabled at the VPLS level, packets with unknown destination MAC address will be dropped instead (even when configured FIB size limits for VPLS or SAP are not yet reached).

The **no** form of this command allows flooding of packets with unknown destination MAC addresses in the VPLS.

**Default**

*no discard-unknown* — Packets with unknown destination MAC addresses are flooded.

---

**endpoint**

**Syntax**

```
endpoint endpoint-name [create]
no endpoint
```

**Context**

```
config>service>vpls
```

**Description**

This command configures a service endpoint.

**Parameters**

- `endpoint-name` — Specifies an endpoint name up to 32 characters in length.
- `create` — This keyword is mandatory while creating a service endpoint.

---

**description**

**Syntax**

```
description description-string
no description
```

**Context**

```
config>service>vpls>endpoint
```

**Description**

This command creates a text description stored in the configuration file for a configuration context.

The **description** command associates a text string with a configuration context to help identify the content in the configuration file.

The **no** form of this command removes the string from the configuration.

**Default**

No description associated with the configuration context.

**Parameters**

- `string` — The description character string. Allowed values are any string up to 80 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

---

**auto-learn-mac-protect**

**Syntax**

```
[no] auto-learn-mac-protect
```

**Context**

```
config>service>vpls>endpoint
config>service>vpls>mesh-sdp
config>service>vpls>sap
config>service>vpls>split-horizon-group
config>service>vpls>spoke-sdp
```
**VPLS Service Commands**

**Description**  This command specifies whether to enable automatic population of the MAC protect list with source MAC addresses learned on the associated with this SHG. For more information, refer to Auto-Learn MAC Protect on page 555.

The no form of the command disables the automatic population of the MAC protect list.

**Default**  auto-learn-mac-protect

**ignore-standby-signaling**

**Syntax**  [no] ignore-standby-signaling

**Context**  config>service>vpls>endpoint
              config>service>vpls>spoke-sdp

**Description**  When this command is enabled, the node will ignore standby-bit received from TLDP peers for the given spoke SDP and performs internal tasks without taking it into account.

This command is present at endpoint level as well as spoke SDP level. If the spoke SDP is part of the explicit-endpoint, it is not possible to change this setting at the spoke SDP level. The existing spoke SDP will become part of the explicit-endpoint only if the setting is not conflicting. The newly created spoke SDP which is a part of the given explicit-endpoint will inherit this setting from the endpoint configuration.

**Default**  enabled

**restrict-protected-src**

**Syntax**  restrict-protected-src alarm-only
             restrict-protected-src [discard-frame]
             no restrict-protected-src

**Context**  config>service>vpls>endpoint
              config>service>vpls>mesh-sdp
              config>service>vpls>sap
              config>service>vpls>split-horizon-group
              config>service>vpls>spoke-sdp

This command indicates the action to take whenever a relearn request for a protected MAC is received on a restricted SAP belonging to this SHG.

When enabled, the agent will protect the MAC from being learned or re-learned on a SAP that has restricted learning enabled.

**Default**  restrict-protected-src

**Parameters**

- **alarm-only** — Specifies that the SAP will be left up and only a notification, sapReceivedProtSrcMac, will be generated.

- **discard-frame** — Specifies that the SAP will start discarding the frame in addition to generating sapReceivedProtSrcMac notification.
revert-time

Syntax revert-time revert-time | infinite
no revert-time

Context config>service>vpls>endpoint

Description This command configures the time to wait before reverting to primary spoke SDP.

In a regular endpoint the revert-time setting affects just the pseudowire defined as primary (precedence 0). For a failure of the primary pseudowire followed by restoration the revert-timer is started. After it expires the primary pseudowire takes the active role in the endpoint. This behavior does not apply for the case when both pseudowires are defined as secondary. For example, if the active secondary pseudowire fails and is restored it will stay in standby until a configuration change or a force command occurs.

Parameters revert-time — Specifies the time to wait, in seconds, before reverting back to the primary spoke SDP defined on this service endpoint, after having failed over to a backup spoke SDP.

Values 0 — 600

infinite — Specifying this keyword makes endpoint non-revertive.

static-mac

Syntax static-mac ieee-address [create]
no static-mac

Context config>service>vpls>endpoint

Description This command assigns a static MAC address to the endpoint. In the FDB, the static MAC is then associated with the active spoke SDP.

Default none

Parameters ieee-address — Specifies the static MAC address to the endpoint.


create — This keyword is mandatory while creating a static MAC.

suppress-standby-signaling

Syntax [no] suppress-standby-signaling

Context config>service>vpls>endpoint

Description When this command is enabled, the pseudowire standby bit (value 0x00000020) will not be sent to T-LDP peer when the given spoke is selected as a standby. This allows faster switchover as the traffic will be sent over this SDP and discarded at the blocking side of the connection. This is particularly applicable to multicast traffic.
propagate-mac-flush

Syntax     [no] propagate-mac-flush
Context     config>service>vpls
Description This command enabled propagation of mac-flush messages received from the given T-LDP on all spoke and mesh-sdps within the context of the VPLS service. The propagation will follow split-horizon principles and any data-path blocking in order to avoid looping of these messages.
Default     disabled

fdb-table-high-wmark

Syntax     [no] fdb-table-high-wmark high-water-mark
Context     config>service>vpls
                         config>template>vpls-template
Description This command specifies the value to send logs and traps when the threshold is reached.
Parameters  high-water-mark — Specify the value to send logs and traps when the threshold is reached.
            Values          0— 100
            Default         95%

fdb-table-low-wmark

Syntax     [no] fdb-table-low-wmark low-water-mark
Context     config>service>vpls
                         config>template>vpls-template
Description This command specifies the value to send logs and traps when the threshold is reached.
Parameters  low-water-mark — Specify the value to send logs and traps when the threshold is reached.
            Values     0— 100
            Default   90%
Virtual Private LAN Services

**fdb-table-size**

**Syntax**

```
fdb-table-size table-size
no fdb-table-size [table-size]
```

**Context**

```
config>service>vpls
config>template>vpls-template
```

**Description**

This command specifies the maximum number of MAC entries in the forwarding database (FDB) for the VPLS instance on this node.

The `fdb-table-size` specifies the maximum number of forwarding database entries for both learned and static MAC addresses for the VPLS instance.

The `no` form of this command returns the maximum FDB table size to default.

**Default**

250 — Forwarding table of 250 MAC entries.

**Parameters**

`table-size` — Specifies the maximum number of MAC entries in the FDB.

**Values**

1 — 511999

Chassis-mode A or B limit: 131071

Chassis-mode C limit: 196607

Chassis-mode D limit: 511999

---

**interface**

**Syntax**

```
[no] interface ip-int-name
```

**Context**

```
config>service>vpls
```

**Description**

This command creates an IP interface.

---

**address**

**Syntax**

```
address ip-address[/mask]> [netmask]
no address
```

**Context**

```
config>service>vpls>interface
```

**Description**

This command assigns an IP address, IP subnet, and broadcast address format to an IES IP router interface. Only one IP address can be associated with an IP interface.

An IP address must be assigned to each IES IP interface. An IP address and a mask are used together to create a local IP prefix. The defined IP prefix must be unique within the context of the routing instance. It cannot overlap with other existing IP prefixes defined as local subnets on other IP interfaces in the same routing context within the router.

The local subnet that the `address` command defines must be part of the services address space within the routing context using the `config router service-prefix` command. The default is to disallow the complete address space to services. Once a portion of the address space is allocated as a service prefix, that portion can be made unavailable for IP interfaces defined within the `config router`
interface CLI context for network core connectivity with the exclude option in the config router service-prefix command.

The IP address for the interface can be entered in either CIDR (Classless Inter-Domain Routing) or traditional dotted decimal notation. The show commands display CIDR notation and is stored in configuration files.

By default, no IP address or subnet association exists on an IP interface until it is explicitly created. Use the no form of this command to remove the IP address assignment from the IP interface. When the no address command is entered, the interface becomes operationally down.

<table>
<thead>
<tr>
<th>Address</th>
<th>Admin State</th>
<th>Oper State</th>
</tr>
</thead>
<tbody>
<tr>
<td>No address</td>
<td>up</td>
<td>down</td>
</tr>
<tr>
<td>No address</td>
<td>down</td>
<td>down</td>
</tr>
<tr>
<td>1.1.1.1</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>1.1.1.1</td>
<td>down</td>
<td>down</td>
</tr>
</tbody>
</table>

The operational state is a read-only variable and the only controlling variables are the address and admin states. The address and admin states are independent and can be set independently. If an interface is in an administratively up state and an address is assigned, it becomes operationally up and the protocol interfaces and the MPLS LSPs associated with that IP interface will be reinitialized.

ip-address — The IP address of the IP interface. The ip-address portion of the address command specifies the IP host address that will be used by the IP interface within the subnet. This address must be unique within the subnet and specified in dotted decimal notation. Allowed values are IP netmask.

The subnet mask in dotted decimal notation. When the IP prefix is not specified in CIDR notation, a space separates the ip-address from a traditional dotted decimal mask. The mask parameter indicates the complete mask that will be used in a logical ‘AND’ function to derive the local subnet of the IP address. Allowed values are dotted decimal addresses in the range 128.0.0.0 – 255.255.255.252. Note that a mask of 255.255.255.255 is reserved for system IP addresses.

arp-timeout

Syntax         arp-timeout seconds
               no arp-timeout

Context        config>service>vpls>interface

Description    This command configures the minimum time in seconds an ARP entry learned on the IP interface will be stored in the ARP table. ARP entries are automatically refreshed when an ARP request or gratuitous ARP is seen from an IP host, otherwise, the ARP entry is aged from the ARP table. If arp-timeout is set to a value of zero seconds, ARP aging is disabled.

The default value for arp-timeout is 14400 seconds (4 hours).

The no form of this command restores arp-timeout to the default value.
Virtual Private LAN Services

### Default

14400 seconds

### Parameters

*seconds* — The minimum number of seconds a learned ARP entry will be stored in the ARP table, expressed as a decimal integer. A value of zero specifies that the timer is inoperative and learned ARP entries will not be aged.

*Values*

0 — 65535

### mac

**Syntax**

mac *ieee-address*

no mac

**Context**

config>service>vpls>interface

**Description**

This command assigns a specific MAC address to a VPLS IP interface.

For Routed Central Office (CO), a group interface has no IP address explicitly configured but inherits an address from the parent subscriber interface when needed. For example, a MAC will respond to an ARP request when an ARP is requested for one of the IPs associated with the subscriber interface through the group interface.

The `no` form of the command returns the MAC address of the IP interface to the default value.

*Default*

The system chassis MAC address.

*Parameters*

*ieee-address* — Specifies the 48-bit MAC address for the static ARP in the form aa:bb:cc:dd:ee:ff or aa-bb-cc-dd-ee-ff where aa, bb, cc, dd, ee, and ff are hexadecimal numbers. Allowed values are any non-broadcast, non-multicast MAC and non-IEEE reserved MAC addresses.

### static-arp

**Syntax**

static-arp *ieee-mac-addr unnumbered*

no static-arp unnumbered

**Context**

config>service>vpls>interface

**Description**

This command configures a static address resolution protocol (ARP) entry associating a subscriber IP address with a MAC address for the core router instance. A static ARP can only be configured if it exists on the network attached to the IP interface.

If an entry for a particular IP address already exists and a new MAC address is configured for the IP address, the existing MAC address will be replaced with the new MAC address.

The `no` form of the command removes a static ARP entry.

*Default*

None

*Parameters*

*ip-address* — Specifies the IP address for the static ARP in dotted decimal notation.

*ieee-mac-address* — Specifies the 48-bit MAC address for the static ARP in the form aa:bb:cc:dd:ee:ff or aa-bb-cc-dd-ee-ff where aa, bb, cc, dd, ee and ff are hexadecimal numbers. Allowed values are any non-broadcast, non-multicast MAC and non-IEEE reserved MAC addresses.
**unnumbered** — Specifies the static ARP MAC for an unnumbered interface. Unnumbered interfaces support dynamic ARP. Once this command is configured, it overrides any dynamic ARP.

### static-mac

**Syntax**

static-mac

**Context**

cfg>service>vpls

**Description**

A set of conditional static MAC addresses can be created within a VPLS supporting bgp-evpn. Conditional static macs are also supported in B-VPLS with SPBM. Conditional Static MACs are dependent on the SAP/SDP state.

This command allows assignment of a set of conditional static MAC addresses to a SAP/spoke-SDP. In the FDB, the static MAC is then associated with the active SAP or spoke SDP.

Static MACs are used for PBB Epipe and I-VPLS services that may terminate external to SPBM. If this is configured under a Control B-VPLS the interface referenced will not use IS-IS for this neighbor. This may also be configured under a User B-VPLS where the corresponding interface is not supported under the Control B-VPLS.

Static MACs configured in a bgp-evpn service are advertised as protected (EVPN will signal the mac as protected).

### mac

**Syntax**

mac ieee-address [create] sap sap-id [monitor fwd-status]
mac ieee-address [create] spoke-sdp sdp-id:vc-id [monitor fwd-status]
[no] mac ieee-address

**Context**

cfg>service>vpls>static-mac

**Description**

This command assigns a conditional static MAC address entry to an SPBM B-VPLS SAP/spoke-SDP allowing external MACs for single and multi-homed operation.

Static MACs are used for PBB Epipe and I-VPLS services that may terminate external to SPBM. If this is configured under a Control B-VPLS the interface referenced will not use IS-IS for this neighbor. This may also be configured under a User B-VPLS where the corresponding interface is not supported under the Control B-VPLS.

**Default**

none

**Parameters**

**ieee-address** — Specifies the static MAC address to an SPBM/sdp-binding interface.

**Values**


**create** — This keyword is mandatory while creating a static MAC.

**monitor fwd-status** — Specifies that this static mac is based on the forwarding status of the SAP or spoke SDP for multi-homed operation. Monitoring is optional but is required for multi-homing.
unnumbered

Syntax  
unnumbered [ip-int-name | ip-address]  
no unnumbered  

Context  
config>service>ies>if  
config>service>vpls>if  
config>service>vprn>if  

Description  
This command configures the interface as an unnumbered interface. Unnumbered IP interface is supported on a Sonet/SDH access port with the PPP, ATM, or Frame Relay encapsulation. It is also supported on an Ethernet port. It is not supported on a TDM port or channel.

Parameters  

ip-int-name — Specifies the name of the IP interface. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

ip-address — Specifies an IP address which must be a valid address of another interface.

isid-policy

Syntax  
isid-policy  
no isid-policy  

Context  
config>service>vpls  

Description  
This command configures isid-policies for individual ISIDs or ISID ranges in a B-VPLS using SPBM. The ISIDs may belong to I-VPLS services or may be static-isids defined on this node. Multiple entry statements are allowed under a isid-policy. ISIDs that are declared as static do not require and isid-policy unless the ISIDs are not to be advertised.

isid-policy allows finer control of ISID multicast but is not typically required for SPBM operation. Use of ISID policies can cause additional flooding of multicast traffic.

Default  
no default

entry

entry id create  
no entry  

Context  
config>service>vpls>isid-policy  

Description  
This command creates or edits an isid-policy entry. Multiple entries can be created using unique entry-id numbers within the isid-policy.

Default: No entry

text id — An entry-id uniquely identifies a ISID range and the corresponding actions. This allows users to insert a new entry in an existing policy without requiring renumbering of all the existing entries.

The following rules govern the usage of multiple entry statements:
• overlapping values are allowed:
  – isid from 301 to 310
  – isid from 305 to 315
  – isid 316
• the minimum and maximum values from overlapping ranges are considered and displayed. The
  above entries will be equivalent with “isid from 301 to 316” statement.
• there is no consistency check with the content of ISID statements from other entries. The entries
  will be evaluated in the order of their IDs and the first match will cause the implementation to
  execute the associated action for that entry.

no isid - removes all the previous statements under one entry.
no isid value | from value to higher-value - removes a specific ISID value or range. Must match a
previously used positive statement: for example, if the command “isid 16 to 100” was used using “no
isid 16 to 50”, it will not work but “no isid 16 to 100 will be successful.

Values 1-65535

create — Required when first creating the configuration context. Once the context is created, one can
navigate into the context without the create keyword.

advertise-local

Syntax  [no] advertise-local

Context  config>service>vpls>isid-policy>entry

Description  The no advertise-local option prevents the advertisement of any locally defined I-VPLS ISIDs or
static-isids in the range in a B-VPLS. For I-VPLS services or static-isids that are primarily unicast
traffic, the use-def-mcast and no advertise-local options allows the forwarding of ISID based
multicast frames locally using the default multicast. The no advertise-local option also suppresses
this range of ISIDs from being advertised in ISIS. When using the use-def-mcast and no advertise-
local policies, the ISIDs configured under this static-isid declarations SPBM treats the ISIDs as
belonging to the default tree.

Default  advertise-local

range

Syntax  range isid [to isid]

Context  config>service>vpls>isid-policy>entry

Description  This command specifies an ISID or a Range of ISIDs in a B-VPLS. One range is allowed per entry.

Default  no range

Parameters  isid — Specifies the ISID value in 24 bits. When singular, ISID identifies a particular ISID to be used
for matching.
Values 0..16777215
to isid — Identifies upper value in a range of ISIDs to be used as matching criteria.

use-def-mcast

Syntax  [no] use-def-mcast
Context config>service>vpls>isid-policy>entry
Description The use-def-mcast option prevents local installation of the ISIDs in the range in the MFIB and uses the default multicast tree instead for a B-VPLS. In a node that does not have I-VPLS or static-isids, this command prevents the building of an MFIB entry for this ISID when received in a SPBM TLV and allows the broadcast of ISID based traffic on the default multicast tree. If an isid-policy exists, the core nodes can have this policy to prevent connectivity problems when some nodes are advertising an ISID and others are not. In a I-VPLS service if the customer MAC (C-MAC) is unknown, a frame will have the Multicast DA for an ISID (PBB-OUI + ISID) flooded on the default multicast tree and not pruned.

Default no use-def-mcast

local-age

Syntax  local-age aging-timer
no local-age
Context config>service>vpls
config>template>vpls-template
Description Specifies the aging time for locally learned MAC addresses in the forwarding database (FDB) for the Virtual Private LAN Service (VPLS) instance. In a VPLS service, MAC addresses are associated with a Service Access Point (SAP) or with a Service Distribution Point (SDP). MACs associated with a SAP are classified as local MACs, and MACs associated with an SDP are remote MACs.

Like in a Layer 2 switch, learned MACs can be aged out if no packets are sourced from the MAC address for a period of time (the aging time). In each VPLS service instance, there are independent aging timers for local learned MAC and remote learned MAC entries in the FDB. The local-age timer specifies the aging time for local learned MAC addresses.

The no form of this command returns the local aging timer to the default value.

Default local age 300 — Local MACs aged after 300 seconds.

Parameters aging-timer — The aging time for local MACs expressed in seconds.

Values 60 — 86400
mac-move

Syntax  
[no] mac-move

Context  
config>service>vpls
config>template>vpls-template

Description  
This command enables the context to configure MAC move attributes. A sustained high re-learn rate can be a sign of a loop somewhere in the VPLS topology. Typically, STP detects loops in the topology, but for those networks that do not run STP, the mac-move feature is an alternative way to protect your network against loops.

When enabled in a VPLS, mac-move monitors the re-learn rate of each MAC. If the rate exceeds the configured maximum allowed limit, it disables the SAP where the source MAC was last seen. The SAP can be disabled permanently (until a shutdown/no shutdown command is executed) or for a length of time that grows linearly with the number of times the given SAP was disabled. You have the option of marking a SAP as non-blockable in the config>service>vpls>sap>limit-mac-move or config>service>vpls>spoke-sdp>limit-mac-move contexts. This means that when the re-learn rate has exceeded the limit, another (blockable) SAP will be disabled instead.

The mac-move command enables the feature at the service level for SAPs and spoke SDPs, as only those objects can be blocked by this feature. Mesh SDPs are never blocked, but their re-learn rates (sap-to-mesh/spoke-to-mesh or vice versa) are still measured.

The operation of this feature is the same on the SAP and spoke SDP. For example, if a MAC address moves from SAP to SAP, from SAP to spoke SDP, or between spoke SDPs, one will be blocked to prevent thrashing. If the MAC address moves between a SAP and mesh SDP or spoke SDP and mesh SDP combinations, the respective SAP or spoke SDP will be blocked.

mac-move will disable a VPLS port when the number of relearns detected has reached the number of relearns needed to reach the move-frequency in the 5-second interval. For example, when the move-frequency is configured to 1 (relearn per second) mac-move will disable one of the VPLS ports when 5 relearns were detected during the 5-second interval because then the average move-frequency of 1 relearn per second has been reached. This can already occur in the first second if the real relearn rate is 5 relearns per second or higher.

The no form of this command disables MAC move.

mac-protect

Syntax  
mac-protect

Context  
config>service>vpls

Description  
This command indicates whether or not this MAC is protected on the MAC protect list. When enabled, the agent will protect the MAC from being learned or re-learned on a SAP, spoke SDP or mesh-SDP that has restricted learning enabled. The MAC protect list is used in conjunction with restrict-protected-src, restrict-unprotected-dst and auto-learn-mac-protect.

Default  
disabled
mac

**Syntax**  
[no] mac ieee-address

**Context**  
config>service>vpls>mac-protect

**Description**  
This command adds a protected MAC address entry.

**Parameters**

- **ieee-address** — Specifies the 48-bit MAC address in the form aa:bb:cc:dd:ee:ff or aa-bb-cc-dd-ee-ff where aa, bb, cc, dd, ee, and ff are hexadecimal numbers.

mac-subnet-length

**Syntax**  
mac-subnet-length subnet-length

**Context**  
config>service>vpls

**Description**  
This command specifies the number of bits to be considered when performing MAC learning (MAC source) and MAC switching (MAC destination). Specifically, this value identifies how many bits, starting from the beginning of the MAC address are used. For example, if the mask-value of 28 is used, MAC learning will only do a lookup for the first 28 bits of the source MAC address when comparing with existing FIB entries. Then, it will install the first 28 bits in the FIB while zeroing out the last 20 bits of the MAC address. When performing switching in the reverse direction, only the first 28 bits of the destination MAC address will be used to perform a FIB lookup to determine the next hop.

The **no** form of this command switches back to full MAC lookup.

**Parameters**

- **subnet-length** — Specifies the number of bits to be considered when performing MAC learning or MAC switching.

  **Values**  
  24 — 48

move-frequency

**Syntax**  
move-frequency frequency

**Context**  
config>service>vpls>mac-move  
config>template>vpls-template>mac-move

**Description**  
This command indicates the maximum rate at which MAC's can be re-learned in the VPLS service, before the SAP where the moving MAC was last seen is automatically disabled in order to protect the system against undetected loops or duplicate MAC's.

The **no** form of the command reverts to the default value.

**Default**  
2 (when mac-move is enabled). For example, 10 relearns in a 5 second period.

**Parameters**

- **frequency** — Specifies the rate, in 5-second intervals for the maximum number of relearns.
number-retries

**Syntax**
number-retries *number-retries*
no number-retries

**Context**
cfg-service>vpls>mac-move
cfg-template>vpls-template>mac-move

**Description**
This command configures the number of times retries are performed for reenabling the SAP/SDP.

**Parameters**

*number-retries*

Specifies number of retries for reenabling the SAP/SDP. A zero (0) value indicates unlimited number of retries.

**Values**
0 — 255

primary-ports

**Syntax**
primary-ports

**Context**
cfg-service>vpls>mac-move
cfg-template>vpls-template>mac-move

**Description**
This command enables the context to define primary VPLS ports. VPLS ports that were declared as secondary prior to the execution of this command will be moved from secondary port-level to primary port-level. Changing a port to the tertiary level can only be done by first removing it from the secondary port-level.

cumulative-factor

**Syntax**
cumulative-factor *cumulative-factor*
no cumulative-factor

**Context**
cfg-service>vpls>mac-move>primary-ports
cfg-service>vpls>mac-move>secondary-ports
cfg-template>vpls-template>mac-move>primary-ports
cfg-template>vpls-template>mac-move>secondary-ports

**Description**
This command configures a factor for the primary or secondary ports defining how many MAC relearn periods should be used to measure the MAC relearn rate. This rate must be exceeded during consecutive periods before the corresponding ports (SAP and/or spoke-SDP) are blocked by the MAC-move feature.

**Parameters**

*cumulative-factor* — Specifies a MAC relearn period to be used for MAC relearn rate.

**Values**
3 — 10
sap

Syntax  sap [split-horizon-group group-name] [create]
        no sap sap-id

Context  config>service>vpls>mac-move>primary-ports
         config>service>vpls>mac-move>secondary-ports

Description  This command declares a given SAP as a primary (or secondary) VPLS port.

Parameters  sap-id — Specifies the physical port identifier portion of the SAP definition. See Common CLI
              Command Descriptions on page 1783 for command syntax.

spoke-sdp

Syntax  [no] spoke-sdp spoke-id

Context  config>service>vpls>mac-move>primary-ports
         config>service>vpls>mac-move>secondary-ports

Description  This command declares a given spoke SDP as a primary (or secondary) VPLS port.

Parameters  spoke-id — Specifies the SDP ID to configure as the primary VPLS port.

Values  1 — 17407

vc-id — The virtual circuit identifier.

Values  1 — 4294967295

cumulative-factor

Syntax  [no] cumulative-factor factor

Context  config>service>vpls>mac-move>primary-ports
         config>service>vpls>mac-move>secondary-ports

Description  This command defines a factor defining how many mac-relearn measurement periods can be used to
              measure mac-relearn rate. The rate must be exceeded during the defined number of consecutive
              periods before the corresponding port is blocked by the mac-move feature. The cumulative-factor of
              primary ports must be higher than cumulative-factor of secondary ports.

Default  2 — secondary ports
         3 — primary ports

Parameters  factor — Specifies the factor defining the number of mac-relearn measurement periods can be used to
              measure mac-relearn rate.

Values  2 — 10
secondary-ports

Syntax  secondary-ports

Context  config>service>vpls>mac-move
          config>template>vpls-template>mac-move

Description  This command opens configuration context for defining secondary vpls-ports. VPLS ports that were declared as primary prior to the execution of this command will be moved from primary port-level to secondary port-level. Changing a port to the tertiary level can only be done by first removing it from the primary port-level.

retry-timeout

Syntax  retry-timeout timeout
        no retry-timeout

Context  config>service>vpls>mac-move
          config>template>vpls-template>mac-move

Description  This indicates the time in seconds to wait before a SAP that has been disabled after exceeding the maximum relearn rate is reenabled.

  It is recommended that the retry-timeout value is larger or equal to 5s * cumulative factor of the highest priority port so that the sequential order of port blocking will not be disturbed by re-initializing lower priority ports.

  A zero value indicates that the SAP will not be automatically re-enabled after being disabled.

  If, after the SAP is reenabled it is disabled again, the effective retry timeout is doubled in order to avoid thrashing.

  The no form of the command reverts to the default value.

Default  10 (when mac-move is enabled)

Parameters  timeout — Specifies the time, in seconds, to wait before a SAP that has been disabled after exceeding the maximum relearn rate is reenabled.

  Values  0 — 120

mfib-table-high-wmark

Syntax  [no] mfib-table-high-wmark high-water-mark

Context  config>service>vpls

Description  This command specifies the multicast FIB high watermark. When the percentage filling level of the multicast FIB exceeds the configured value, a trap is generated and/or a log entry is added.

Parameters  high-water-mark — Specifies the multicast FIB high watermark as a percentage.
Values 1 — 100
Default 95%

mfib-table-low-wmark

Syntax [no] mfib-table-low-wmark low-water-mark
Context config>service>vpls
Description This command specifies the multicast FIB low watermark. When the percentage filling level of the Multicast FIB drops below the configured value, the corresponding trap is cleared and/or a log entry is added.
Parameters low-water-mark — Specifies the multicast FIB low watermark as a percentage.
Values 1 — 100
Default 90%

mfib-table-size

Syntax mfib-table-size size
no mfib-table-size
Context config>service>vpls
Description This command specifies the maximum number of (s,g) entries in the multicast forwarding database (MFIB) for this VPLS instance.

The mfib-table-size parameter specifies the maximum number of multicast database entries for both learned and static multicast addresses for the VPLS instance. When a table-size limit is set on the mfib of a service which is lower than the current number of dynamic entries present in the mfib then the number of entries remains above the limit.

The no form of this command removes the configured maximum MFIB table size.

Default none
Parameters size — The maximum number of (s,g) entries allowed in the Multicast FIB.
Values 1 — 16383

mld-snooping

Syntax mld-snooping
Context config>service>vpls
config>service>vpls>sap
Description This command configures MLD snooping parameters.
remote-age

Syntax
remote-age seconds
no remote-age

Context
config>service>vpls
config>template>vpls-template

Description
Specifies the aging time for remotely learned MAC addresses in the forwarding database (FDB) for the Virtual Private LAN Service (VPLS) instance. In a VPLS service, MAC addresses are associated with a Service Access Point (SAP) or with a Service Distribution Point (SDP). MACs associated with a SAP are classified as local MACs, and MACs associated with an SDP are remote MACs.

Like in a layer 2 switch, learned MACs can be aged out if no packets are sourced from the MAC address for a period of time (the aging time). In each VPLS service instance, there are independent aging timers for local learned MAC and remote learned MAC entries in the FDB. The remote-age timer specifies the aging time for remote learned MAC addresses. To reduce the amount of signaling required between switches configure this timer larger than the local-age timer.

The no form of this command returns the remote aging timer to the default value.

Default
remote age 900 — Remote MACs aged after 900 seconds

Parameters
seconds — The aging time for remote MACs expressed in seconds.

Values
60 — 86400

send-bvpls-flush

Syntax
send-bvpls-flush {all-but-mine} [all-from-me]
no send-bvpls-flush

Context
config>service>vpls

Description
This command enables generation of LDP MAC withdrawl “flush-all-from-me” in the B-VPLS domain when the following triggers occur in the related IVPLS:

• MC-LAG failure
• Failure of a local SAP
• Failure of a local pseudowire/SDP binding

Note that failure means transition of link SAP/pseudowire to either down or standby status.

This command does not require send-flush-on-failure in B-VPLS to be enabled on an IVPLS trigger to send an MAC flush into the BVPLS.

Default
no send-bvpls-flush

Parameters
all-but-mine — Specifies to send an LDP flush all-but-mine and also sent into the B-VPLS. Note that both parameters can be set together.

all-from-me — Specifies to send an LDP flush-all-from and when STP initiates a flush, it is sent into the B-VPLS using LDP MAC flush all-from-me. Note that both parameters can be set together.
send-flush-on-bvpls-failure

**Syntax**

```
[no] send-flush-on-bvpls-failure
```

**Context**

```
config>service>vpls ivpls
```

**Description**

This command enables the generation in the local I-VPLS of a LDP MAC flush-all-from-me following a failure of SAP/the whole endpoint/spoke-SDP in the related B-VPLS. Note that the failure of mesh-SDP in B-VPLS does not generate the I-VPLS MAC flush.

The **no** form of this command disables the generation of LDP MAC flush in I-VPLS on failure of SAP/endpoint/spoke-SDP in the related B-VPLS.

**Default**

```
no send-flush-on-bvpls-failure
```

propagate-mac-flush-from-bvpls

**Syntax**

```
[no] propagate-mac-flush-from-bvpls
```

**Context**

```
config>service>vpls ivpls
```

**Description**

This command enables the propagation in the local I-VPLS of any regular LDP MAC Flush received in the related B-VPLS. If an LDP MAC flush-all-but-mine is received in the B-VPLS context, the command controls also whether a flush is performed for all the customer MACs in the associated I-VPLS FIB. The command does not have any effect on a PBB MAC Flush (LDP MAC flush with PBB TLV) received in the related B-VPLS context.

The **no** form of this command disables the propagation of LDP MAC Flush in I-VPLS from the related B-VPLS.

**Default**

```
no propagate-mac-flush-from-bvpls
```

send-flush-on-failure

**Syntax**

```
[no] send-flush-on-failure
```

**Context**

```
config>service>vpls
```

**Description**

This command enables sending out “flush-all-from-ME” messages to all LDP peers included in affected VPLS, in the event of physical port failures or “oper-down” events of individual SAPs. This feature provides an LDP-based mechanism for recovering a physical link failure in a dual-homed connection to a VPLS service. This method provides an alternative to RSTP solutions where dual homing redundancy and recovery, in the case of link failure, is resolved by RSTP running between a PE router and CE devices. If the endpoint is configured within the VPLS and send-flush-on-failure is enabled, flush-all-from-me messages will be sent out only when all spoke SDPs associated with the endpoint go down.

This feature cannot be enabled on management VPLS.

**Default**

```
no send-flush-on-failure
```
service-mtu

**Syntax**

```
service-mtu octets
no service-mtu
```

**Context**

```
config>service>vpls
config>template>vpls-template
```

**Description**

This command configures the service payload (Maximum Transmission Unit – MTU), in bytes, for the service. This MTU value overrides the service-type default MTU. The *service-mtu* defines the payload capabilities of the service. It is used by the system to validate the SAP and SDP binding’s operational state within the service.

The service MTU and a SAP’s service delineation encapsulation overhead (4 bytes for a dot1q tag) is used to derive the required MTU of the physical port or channel on which the SAP was created. If the required payload is larger than the port or channel MTU, then the SAP will be placed in an inoperative state. If the required MTU is equal to or less than the port or channel MTU, the SAP will be able to transition to the operative state.

When binding an SDP to a service, the service MTU is compared to the path MTU associated with the SDP. The path MTU can be administratively defined in the context of the SDP. The default or administrative path MTU can be dynamically reduced due to the MTU capabilities discovered by the tunneling mechanism of the SDP or the egress interface MTU capabilities based on the next hop in the tunnel path. If the service MTU is larger than the path MTU, the SDP binding for the service will be placed in an inoperative state. If the service MTU is equal to or less than the path MTU, then the SDP binding will be placed in an operational state.

In the event that a service MTU, port or channel MTU, or path MTU is dynamically or administratively modified, then all associated SAP and SDP binding operational states are automatically re-evaluated.

For i-VPLS and Epipes bound to a b-VPLS, the service-mtu must be at least 18 bytes smaller than the b-VPLS service MTU to accommodate the PBB header.

The *no* form of this command returns the default *service-mtu* for the indicated service type to the default value.

**Default**

VPLS: 1514

The following table displays MTU values for specific VC types.

<table>
<thead>
<tr>
<th>VC-Type</th>
<th>Service MTU</th>
<th>Advertised MTU</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet</td>
<td>1514</td>
<td>1500</td>
</tr>
<tr>
<td>Ethernet (with preserved dot1q)</td>
<td>1518</td>
<td>1504</td>
</tr>
<tr>
<td>VPLS</td>
<td>1514</td>
<td>1500</td>
</tr>
<tr>
<td>VPLS (with preserved dot1q)</td>
<td>1518</td>
<td>1504</td>
</tr>
<tr>
<td>VLAN (dot1p transparent to MTU value)</td>
<td>1514</td>
<td>1500</td>
</tr>
<tr>
<td>VLAN (QinQ with preserved bottom Qtag)</td>
<td>1518</td>
<td>1504</td>
</tr>
</tbody>
</table>

The size of the MTU in octets, expressed as a decimal integer.

**Values**

1 — 9194
service-name

Syntax

```
service-name service-name
no service-name
```

Context

`config>service>vpls`

Description

This command configures an optional service name, up to 64 characters in length, which adds a name identifier to a given service to then use that service name in configuration references as well as display and use service names in show commands throughout the system. This helps the service provider/administrator to identify and manage services within the 7950 XRSplatforms.

All services are required to assign a service ID to initially create a service. However, either the service ID or the service name can be used to identify and reference a given service once it is initially created.

Parameters

- `service-name` — Specifies a unique service name to identify the service. Service names may not begin with an integer (0-9).

allow-ip-int-binding

Syntax

```
[no] allow-ip-int-binding
```

Context

`config>service>vpls`

Description

The `allow-ip-int-binding` command sets a flag on the VPLS or I-VPLS service that enables the ability to attach an IES or VPRN IP interface to the VPLS service in order to make the VPLS service routable. When the `allow-ip-int-binding` command is not enabled, the VPLS service cannot be attached to an IP interface.

VPLS Configuration Constraints for Enabling allow-ip-int-binding

When attempting to set the `allow-ip-int-binding` VPLS flag, the system first checks to see if the correct configuration constraints exist for the VPLS service and the network ports. In Release 8.0 the following VPLS features must be disabled or not configured for the `allow-ip-int-binding` flag to set:

- SAP ingress QoS policies applied to the VPLS SAPs cannot have MAC match criteria defined
- SDPs used in spoke or mesh SDP bindings cannot be configured as GRE
- The VPLS service type cannot be B-VPLS or M-VPLS, and it cannot be an I-VPLS service bound to a B-VPLS context
- MVR from Routed VPLS and to another SAP is not supported
- Enhanced and Basic Subscriber Management (ESM and BSM) features
- Network domain on SDP bindings

Once the VPLS allow-ip-int-binding flag is set on a VPLS service, the above features cannot be enabled on the VPLS service.

NETWORK PORT HARDWARE CONSTRAINTS

The system also checks to ensure that all ports configured in network mode are associated with FlexPath2 forwarding planes. If a port is currently in network mode and the port is associated with a FlexPath1 forwarding plane, the allow-ip-int-binding command will fail. Once the allow-ip-int-
binding flag is set on any VPLS service, attempting to enable network mode on a port associated with a FlexPath1 forwarding plane will fail.

**VPLS SAP HARDWARE CONSTRAINTS**
Besides VPLS configuration and network port hardware association, the system also checks to that all SAPs within the VPLS are created on Ethernet ports and the ports are associated with FlexPath2 forwarding planes. Certain Ethernet ports and virtual Ethernet ports are not supported which include HSMDA ports and CCAG virtual ports (VSM based). If a SAP in the VPLS exists on an unsupported port type or is associated with a FlexPath1 forwarding plane, the allow-ip-int-binding command will fail. Once the allow-ip-int-binding flag is set on the VPLS service, attempting to create a VPLS SAP on the wrong port type or associated with a FlexPath1 forwarding plane will fail.

**VPLS SERVICE NAME BOUND TO IP INTERFACE WITHOUT ALLOW-IP-INT-BINDING FLAG SET**
In the event that a service name is applied to a VPLS service and that service name is also bound to an IP interface but the allow-ip-int-binding flag has not been set on the VPLS service context, the system attempt to resolve the service name between the VPLS service and the IP interface will fail. After the allow-ip-int-binding flag is successfully set on the VPLS service, either the service name on the VPLS service must be removed and reapplied or the IP interface must be re-initialized using the shutdown / no shutdown commands. This will cause the system to reattempt the name resolution process between the IP interface and the VPLS service.

The **no** form of the command resets the allow-ip-int-binding flag on the VPLS service. If the VPLS service currently has an IP interface from an IES or VPRN service attached, the **no** allow-ip-int-binding command will fail. Once the allow-ip-int-binding flag is reset on the VPLS service, the configuration and hardware restrictions associated with setting the flag are removed. The port network mode hardware restrictions are also removed.

### site

**Syntax**

```plaintext
site name [create]
no site name
```

**Context**

`config>service>vpls`

**Description**

This command configures a VPLS site.

The **no** form of the command removes the name from the configuration.

**Parameters**

- `name` — Specifies a site name up to 32 characters in length.
- `create` — This keyword is mandatory while creating a VPLS service.

### boot-timer

**Syntax**

```plaintext
boot-timer seconds
no boot-timer
```

**Context**

`config>service>vpls>site`
Virtual Private LAN Services

Description
This command configures for how long the service manager waits after a node reboot before running the DF election algorithm. The boot-timer value should be configured to allow for the BGP sessions to come up and for the NLRI information to be refreshed/exchanged.

The no form of the command reverts the default.

Default
10

Parameters
seconds — Specifies the site boot-timer in seconds.

Values
0 — 100

failed-threshold

Syntax
failed-threshold [1..1000]
failed-threshold all

Context
config>service>vpls>site

Description
This command defines the number of objects should be down for the site to be declared down. Both administrative and operational status must be evaluated and if at least one is down, the related object is declared down.

Default
failed-threshold all

Parameters
1 .. 1000 — Specifies the threshold for the site to be declared down.

mesh-sdp-binding

Syntax
[no] mesh-sdp-binding

Context
config>service>vpls>site

Description
This command enables applications to all mesh SDPs.

The no form of reverts the default.

Default
no mesh-sdp-binding

monitor-oper-group

Syntax
monitor-oper-group group-name
no monitor-oper-group

Context
config>service>vpls>site
cfg>service>vpls>spoke-sdp
cfg>service>vpls>sap
cfg>service>vpls>bgp>pw-template-binding
VPLS Service Commands

Description
This command specifies the operational group to be monitored by the object under which it is configured. The `oper-group name` must be already configured under the `config>service` context before its name is referenced in this command.

The `no` form of the command removes the association.

sap

Syntax
```
sap sap-id
no sap
```

Context `config>service>vpls>site`

Description
This command configures a SAP for the site.

The `no` form of the command removes the SAP ID from the configuration.

Parameters
- `sap-id` — Specifies the physical port identifier portion of the SAP definition. See Common CLI Command Descriptions on page 1783 for command syntax.

site-activation-timer

Syntax
```
site-activation-timer seconds
no site-activation-timer
```

Context `config>service>vpls>site`

Description
This command configures the time-period the system keeps the local sites in standby status, waiting for BGP updates from remote PEs before running the DF (designated-forwarder) election algorithm to decide whether the site should be unblocked. This timer if terminated if an update is received for which the remote PE has transitioned from DF to non-DF.

The `no` form of the command removes the value from the configuration.

Default 2

Parameters
- `seconds` — Specifies the site activation timer in seconds.
  - Values 0 — 100

site-id

Syntax
```
site-id value
no site-id
```

Context `config>service>vpls>site`

Description
This command configures the identifier for the site in this service.

Parameters
- `value` — Specifies the site identifier.
  - Values 1 — 65535
split-horizon-group

Syntax
split-horizon-group group-name
no split-horizon-group

Context config>service>vpls>site

Description This command configures the value of split-horizon group associated with this site.
The no form of the command reverts the default.

Default no split-horizon-group

Parameters group-name — Specifies a split-horizon group name.

spoke-sdp

Syntax spoke-sdp sdp-id:vc-id
no spoke-sdp

Context config>service>vpls>site

Description This command binds a service to an existing Service Distribution Point (SDP).
The no form of the command removes the parameter from the configuration.

split-horizon-group

Syntax [no] split-horizon-group [group-name] [residential-group]

Context config>service>vpls

Description This command creates a new split horizon group for the VPLS instance. Traffic arriving on a SAP or spoke SDP within this split horizon group will not be copied to other SAPs or spoke SDPs in the same split horizon group.

A split horizon group must be created before SAPs and spoke SDPs can be assigned to the group.
The split horizon group is defined within the context of a single VPLS. The same group-name can be re-used in different VPLS instances.

Up to 30 split horizon groups can be defined per VPLS instance. Half are supported in i-VPLS.
The no form of the command removes the group name from the configuration.

Parameters group-name — Specifies the name of the split horizon group to which the SDP belongs.

residential-group — Defines a split horizon group as a residential split horizon group (RSHG). Doing so entails that:

a) SAPs which are members of this Residential Split Horizon Group will have:

- Double-pass queuing at ingress as default setting (can be disabled)
- STP disabled (cannot be enabled)
VPLS Service Commands

- ARP reply agent enabled per default (can be disabled)
- MAC pinning enabled per default (can be disabled)
- Downstream broadcast packets are discarded thus also blocking the unknown, flooded traffic
- Downstream multicast packets are allowed when IGMP snooping is enabled

b) Spoke SDPs which are members of this Residential Split Horizon Group will have:
- Downstream multicast traffic supported
- Double-pass queuing is not applicable
- STP is disabled (can be enabled)
- ARP reply agent is not applicable (dhcp-lease-states are not supported on spoke SDPs)
- MAC pinning enabled per default (can be disabled)

Default A split horizon group is by default not created as a residential-group.

auto-learn-mac-protect

Syntax  [no] auto-learn-mac-protect

Context  config>service>vpls>sap
         config>service>vpls>spoke-sdp
         config>service>vpls >mesh-sdp
         config>service>vpls>split-horizon-group
         config>service>vpls>endpoint
         config>service>pw-template
         config>service>pw-template>split-horizon-group

Description This command enables the automatic protection of source MAC addresses learned on the associated object. MAC protection is used in conjunction with restrict-protected-src, restrict-unprotected-dst and mac-protect. When this command is applied or removed, the MAC addresses are cleared from the related object.

When the auto-learn-mac-protect is enabled on an SHG the action only applies to the associated SAPs (no action is taken by default for spoke SDPs in the SHG). In order to enable this function for spoke SDPs within a SHG, the auto-learn-mac-protect must be enabled explicitly under the spoke-SDP. If required, auto-learn-mac-protect can also be enabled explicitly under specific SAPs within the SHG.

Default  no auto-learn-mac-protect

restrict-protected-src

Syntax  restrict-protected-src [alarm-only | discard-frame]
no restrict-protected-src

Context  config>service>vpls>sap
         config>service>vpls>spoke-sdp
         config>service>vpls >mesh-sdp
         config>service>vpls>split-horizon-group
This command indicates how the agent will handle relearn requests for protected MAC addresses, either manually added using the mac-protect command or automatically added using the auto-learn-mac-protect command. While enabled all packets entering the configured SAP, spoke-SDP, mesh-SDP, or any SAP that is part of the configured split horizon group (SHG) will be verified not to contain a protected source MAC address. If the packet is found to contain such an address, the action taken depends on the parameter specified on the restrict-protected-src command, namely:

- **No parameter**
  
The packet will be discarded, an alarm will be generated and the SAP, spoke-SDP or mesh-SDP will be set operationally down. The SAP, spoke-SDP or mesh-SDP must be shutdown and enabled (no shutdown) for this state to be cleared.

- **alarm-only**
  
The packet will be forwarded, an alarm will be generated but the source MAC is not learned on the SAP/spoke-SDP/mesh-SDP.

- **discard-frame**
  
The packet will be discarded and an alarm generated. The frequency of alarm generation is fixed to be at most one alarm per MAC address per FP2 per 10 minutes in a given VPLS service. This parameter is only applicable to automatically protected MAC addresses.

When the `restrict-protected-src` is enabled on an SHG the action only applies to the associated SAPs (no action is taken by default for spoke SDPs in the SHG). In order to enable this function for spoke SDPs within a SHG, the `restrict-protected-src` must be enabled explicitly under the spoke-SDP. If required, `restrict-protected-src` can also be enabled explicitly under specific SAPs within the SHG.

When this command is applied or removed, with either the alarm-only or discard-frame parameters, the MAC addresses are cleared from the related object.

The use of “`restrict-protected-src discard-frame`” is mutually exclusive with both the “`restrict-protected-src [alarm-only]`” command and with the configuration of manually protected MAC addresses within a given VPLS. “`restrict-protected-src discard-frame`” can only be enabled on SAPs on FP2 or later hardware or on SDPs where all network interfaces are on FP2 or later hardware.

### Parameters

- **alarm-only** — Specifies that the packet will be forwarded, an alarm will be generated but the source MAC is not learned on the SAP/spoke-SDP/mesh-SDP.
  
  **Default** no alarm-only

- **discard-frame** — Specifies that the packet will be discarded and an alarm generated. The frequency of alarm generation is fixed to be at most one alarm per FP2 per MAC address per 10 minutes within a given VPLS service.
  
  **Default** no discard-frame

**Default** no restrict-protected-src
restrict-unprotected-dst

Syntax:
- `restrict-unprotected-dst`
- `no restrict-unprotected-dst`

Context:
- `config>service>pw-template>split-horizon-group`
- `config>service>vpls>split-horizon-group`
- `config>service>vpls.sap`

Description:
This command indicates how the system will forward packets destined to an unprotected MAC address, either manually added using the mac-protect command or automatically added using the auto-learn-mac-protect command. While enabled all packets entering the configured SAP or SAPs within a split-horizon-group (but not spoke or mesh-SDPs) will be verified to contain a protected destination MAC address. If the packet is found to contain a non-protected destination MAC, it will be discarded. Detecting a non-protected destination MAC on the SAP will not cause the SAP to be placed in the operationally down state. No alarms are generated.

If the destination MAC address is unknown, even if the packet is entering a restricted SAP, with restrict-unprotected-dst enabled, it will be flooded.

Default:
`no restrict-unprotected-dst`

vpls-group

Syntax:
- `[no] vpls-group id`

Context:
`config>service>vpls`

Description:
This command defines a vpls-group index. Multiple vpls-group commands can be specified to allow the use of different VPLS and SAP templates for different ranges of service ids. A vpls-group can be deleted only in shutdown state. Multiple commands under different vpls-group ids can be issued and can be in progress at the same time.

Default:
`no vpls-group`

Parameters:
- `id` — Specifies the ID associated with the VPLS group.

Values:
- 1 — 4094

service-range

Syntax:
- `service-range startid-endid [start-vlan-id startvid]
- `no service-range startid-endid`

Context:
`config>service>vpls>vpls-group`

Description:
This command configures the service ID and implicitly the VLAN-ID ranges to be used as input variables for related VPLS and SAP templates to pre-provision “data” VPLS instances and related SAPs using the service ID specified in the command. If the start-vlan-id is not specified then the service-range values are used for vlan-ids. The data SAPs will be instantiated on all the ports used to specify SAP instances under the related control VPLS.
Modifications of the service id and vlan ranges are allowed with the following restrictions.

- **service-range increase can be achieved in two ways:**
  - Allowed when vpls-group is in shutdown state
  - By creating a new vpls-group

- **service-range decrease can be achieved in two ways:**
  - Allowed when vpls-group is in shutdown state; when shutdown command is executed the associated service instances are deleted.
  - Allowed when vpls-group is in no shutdown state and has completed successfully instantiating services.
  - Note that in both cases only the services that do not have user configured SAPs will be deleted. Otherwise the above commands are rejected. Existing declarations or registrations do not prevent service deletion.

- **start-vlan-id change can be achieved in two ways:**
  - Allowed when vpls-group is in shutdown state
  - At the time of range decrease by increasing the start-vlan-id which can be done when vpls-group is in no shutdown state and has completed successfully instantiating services

The **no** form of this command removes the specified ranges and deletes the pre-provisioned VPLS instances and related SAPs. The command will fail if any of the VPLS instances in the affected ranges have a provisioned SAP.

**Default**

**no service-range**

**Parameters**

- **startid-endid** — Specifies the range of service IDs.
  
  **Values**
  
  1—2147483647

- **startvid** — Specifies the starting VLAN ID; it provides a way to set aside a service ID range that is not the same as the VLAN range and allows for multiple MVRP control-VPLSes to control same VLAN range on different ports.
  
  **Values**
  
  1—4094

**vpls-template-binding**

**Syntax**

```
vpls-template-binding name/id
no vpls-template-binding
```

**Context**

```
config>service>vpls>vpls-group
```

**Description**

This command configures the binding to a VPLS template to be used to instantiate pre-provisioned data VPLS using as input variables the service IDs generated by the vid-range command.

The **no** form of this command removes the binding and deletes the related VPLS instances. The command will fail if any of the affected VPLS instances have either a provisioned SAP or an active MVRP declaration/registration or if the related vpls-group id is in no shutdown state. Any changes to the vpls-template-binding require the vpls-group to be in shutdown state.

**Default**

**no vpls-template-binding**
Parameters  name/id — Specifies the name or the ID of the VPLS template.

Values  1—1024
Virtual Private LAN Services

vpls-sap-template-binding

Syntax

vpls-sap-template-binding name/id
no vpls-sap-template-binding

Context

config>service>vpls>vpls-group

Description

This command configures the binding to a SAP template to be used to instantiate SAPs in the data VPLS using as input variables the VLAN IDs generated by the vid-range command.

The no form of this command removes the binding and deletes the related SAP instances. The command will fail if any of the affected VPLS instances have either a provisioned SAP or an active MVRP declaration/registration registration or if the related vpls-group is in no shutdown state. Any changes to the vpls-sap-template-binding require the vpls-group to be in shutdown state. New control SAP additions to the management VPLS are allowed as long as data VPLS instantiations/removals for vpls-groups are not in progress. Control SAPs can be removed at any time generating the removal of related data SAPs from the data VPLS. The shutdown or no shutdown state for the control SAPs does not have any effect on data SAPs instantiated with this command.

Default

no vpls-sap-template-binding

Parameters

name — Specifies the name of the VPLS template.

Values

ASCII character string

id — Specifies the ID of the VPLS template

Values

1—8196

mvrp-control

Syntax

[no] mvrp-control

Context

config>service>vpls>vpls-group

Description

This command enables MVRP control in the VPLS instances instantiated using the templates for the specified vpls-group. That means the flooding FIB will be created empty and will be populated with endpoints whenever MVRP receives a declaration and a registration on a specific endpoint. Also the VLAN ID associated by the control VPLS with the instantiated VPLS will be declared on service activation by MVRP on all virtual MVRP ports in the control VPLS. Service activation takes place when at least one other SAP is provisioned and brought up under the data VPLS. This is usually a customer facing SAP or a SAP leading outside of the MVRP controlled domain.

The no form of this command disallows MVRP control over this VPLS. The VPLS will be created with a regular FIB and will become as a result active upon creation time. Command change is allowed only when the related vpls-group is in shutdown state.

Default

no mvrp-control
**mvrp**

**Syntax**
```
mvrp
```

**Context**
```
config>service>vpls>mrp
config>service>vpls>sap>mrp
```

**Description**
This object consolidates the MVRP attributes. MVRP is only supported initially in the management VPLS so the object is not supported under BVPLS, IVPLS or regular VPLS not marked with the m-vpls tag.

**hold-time**

**Syntax**
```
hold-time value
no hold-time
```

**Context**
```
config>service>vpls>mrp>mvrp
```

**Description**
This command enables the dampening timer and applies to both types of provisioned SAPs – end-station and UNI. When a value is configured for the timer, it controls the delay between detecting that the last provisioned SAP in VPLS goes down and reporting it to the MVRP module. The CPM will wait for the time specified in the value parameter before reporting it to the MVRP module. If the SAP comes up before the hold-timer expires, the event will not be reported to MVRP module.

The non-zero hold-time does not apply for SAP transition from down to up. This kind of transition is reported immediately to MVRP module without waiting for hold-time expiration. Also this parameter applies only to the provisioned SAPs. It does NOT apply to the SAPs configured with the **vpls-sap-template** command. Also when endstation QinQ SAPs are present only the “no hold-time” configuration is allowed.

The no form of this command disables tracking of the operational status for the last active SAP in the VPLS. MVRP will stop declaring the VLAN only when the last provisioned customer (UNI) SAP associated locally with the service is deleted. Also MVRP will declare the associated VLAN attribute as soon as the first provisioned SAP is created in the associated VPLS instance, regardless of the operational state of the SAP.

**Default**
```
no hold-time
```

**Parameters**
```
value — Specifies the hold time in minutes
```

**Values**
```
1—30 minutes
```

**endstation-vid-group**

**Syntax**
```
endstation-vid-group id vlan-id startvid-endvid
no endstation-vid-group id
```

**Context**
```
config>service>vpls>mrp>mvrp
```
Description  This command specifies the range of VLAN IDs that are controlled by MVRP on the port associated with the parent SAP. When the command is present under a certain SAP, the MVRP will treat the associated virtual port as an endstation.

MVRP endstation behavior means that configuration of a new data SAP with the outer tag in the configured endstation-vid-group will generate down that virtual port a MVRP declaration for the new [outer] VLAN attribute. Also registration received for the VLAN attribute in the range will be accepted but not propagated in the rest of MVRP context.

Note that VPLS-groups are not allowed under the associated Management VPLS (MVPLS) once the endstation is configured under one SAP. VPLS-groups can be supported in the chassis using a different MVPLS.

The no form of the command removes the specified group id.

Default  no endstation-vid-group

Parameters  id — Specifies the range index.

Values  1—4094

starvid-endvid — Specifies the range of VLANs to be controlled by MVRP.

Values  1—4094

root-guard

Syntax  [no] root-guard

Context  config>service>vpls>sap>stp

Description  This command specifies whether this port is allowed to become an STP root port. It corresponds to the restrictedRole parameter in 802.1Q. If set, it can cause lack of spanning tree connectivity.

Default  no root-guard

tod-suite

Syntax  tod-suite tod-suite-name

no tod-suite

Context  config>service>vpls>sap

Description  This command applies a time-based policy (filter or QoS policy) to the service SAP. The suite name must already exist in the config>cron context.

Default  no tod-suite

Parameters  tod-suite-name — Specifies collection of policies (ACLs, QoS) including time-ranges that define the full or partial behavior of a SAP. The suite can be applied to more than one SAP.
vxlan

Syntax

vxlan vni vni-id create
no vxlan vni vni-id

Context

config>service>vpls

Description

This command enables the use of vxlan in the vpls service.

Default

none

Parameters

vni — Specifies the vxlan network identifier configured in the vpls service. All the EVPN advertisements (mac routes and inclusive multicast routes) for this service will encode the configured vni in the Ethernet Tag field of the NLRI.

Values

1 — 16777215
VPLS Interface Commands

interface

Syntax  [no] interface ip-int-name

Context  config>service>vpls

Description  This command creates a logical IP routing interface for a VPLS service. Once created, attributes such as IP address and service access points (SAP) can be associated with the IP interface.

The interface command, under the context of services, is used to create and maintain IP routing interfaces within the VPLS service IDs. The IP interface created is associated with the VPLS management routing instance. This instance does not support routing.

Interface names are case-sensitive and must be unique within the group of defined IP interfaces defined for the network core router instance. Interface names in the dotted decimal notation of an IP address are not allowed. For example, the name “1.1.1.1” is not allowed, but “int-1.1.1.1” is allowed.

Show commands for router interfaces use either interface names or the IP addresses. Use unique IP address values and IP address names to maintain clarity. Duplicate interface names can exist in different router instances.

Enter a new name to create a logical router interface. When an existing interface name is entered, the user enters the router interface context for editing and configuration.

By default, no default IP interface names are defined within the system. All VPLS IP interfaces must be explicitly defined in an enabled state.

The no form of this command removes the IP interface and the entire associated configuration. The interface must be administratively shutdown before issuing the no interface command.

For VPLS services, the IP interface must be shutdown before the SAP on that interface is removed. For VPLS service, ping and traceroute are the only applications supported.

Parameters  ip-int-name — Specifies the name of the IP interface. Interface names must be unique within the group of defined IP.

An interface name:

• Should not be in the form of an IP address.
• Can be from 1 to 32 alphanumeric characters.
• If the string contains special characters (such as #,$,spaces), the entire string must be enclosed within double quotes.

If ip-int-name already exists within the service ID, the context changes to maintain that IP interface. If ip-int-name already exists within another service ID, an error occurs and the context does not change to that IP interface. If ip-int-name does not exist, the interface is created and the context is changed to that interface for further command processing.
address

Syntax  
address (ip-address/mask | ip-address netmask)
address ip-address mask

Context  
config>service>vpls>interface

Description  
This command assigns an IP address and an IP subnet, to a VPLS IP router interface. Only one IP address can be associated with an IP interface. An IP address must be assigned to each VPLS IP interface. An IP address and a mask are used together to create a local IP prefix. The defined IP prefix must be unique within the context of the routing instance. It cannot overlap with other existing IP prefixes defined as local subnets on other IP interfaces in the same routing context.

The IP address for the interface can be entered in either CIDR (Classless Inter-Domain Routing) or traditional dotted decimal notation. The show commands display CIDR notation and is stored in configuration files.

By default, no IP address or subnet association exists on an IP interface until it is explicitly created. Use the no form of this command to remove the IP address assignment from the IP interface. When the no address command is entered, the interface becomes operationally down.

<table>
<thead>
<tr>
<th>Address</th>
<th>Admin State</th>
<th>Oper State</th>
</tr>
</thead>
<tbody>
<tr>
<td>No Address</td>
<td>Up</td>
<td>Down</td>
</tr>
<tr>
<td>No Address</td>
<td>Down</td>
<td>Down</td>
</tr>
<tr>
<td>1.1.1.1</td>
<td>Up</td>
<td>Up</td>
</tr>
<tr>
<td>1.1.1.1</td>
<td>Down</td>
<td>Down</td>
</tr>
</tbody>
</table>

The operational state is a read-only variable and the only controlling variables are the address and admin states. The address and admin states are independent and can be set independently. If an interface is in an administratively up state and an address is assigned, it becomes operationally up.

Parameters

ip-address  — The IP address of the IP interface. The ip-address portion of the address command specifies the IP host address that will be used by the IP interface within the subnet.

This address must be unique within the subnet and specified in dotted decimal notation. Allowed values are IP addresses in the range 1.0.0.0 – 223.255.255.255 (with support of /31 subnets).

/  — The forward slash is a parameter delimiter and separates the ip-address portion of the IP address from the mask that defines the scope of the local subnet. No spaces are allowed between the ip-address, the “/” and the mask-length parameter. If a forward slash is not immediately following the ip-address, a dotted decimal mask must follow the prefix.

mask-length  — The subnet mask length when the IP prefix is specified in CIDR notation. When the IP prefix is specified in CIDR notation, a forward slash (/) separates the ip-address from the mask-length parameter. The mask length parameter indicates the number of bits used for the network portion of the IP address; the remainder of the IP address is used to determine the host portion of the IP address. The values allowed are integers in the range 0 – 30. Note that a mask length of 32 is reserved for system IP addresses.

mask  — The subnet mask in dotted decimal notation. When the IP prefix is not specified in CIDR notation, a space separates the ip-address from a traditional dotted decimal mask. The mask
parameter indicates the complete mask that will be used in a logical ‘AND’ function to derive the local subnet of the IP address. Allowed values are dotted decimal addresses in the range 128.0.0.0 – 255.255.255.252. Note that a mask of 255.255.255.255 is reserved for system IP addresses.
General Switch Management Protocol Commands

gsmp

Syntax: gsmp
Context: config>service>vpls
Description: This command enables the context to configure General Switch Management Protocol (GSMP) connections maintained in this service.
Default: not enabled

group

Syntax: [no] group name
Context: config>service>vpls>gsmp
Description: This command specifies a GSMP name. A GSMP group name is unique only within the scope of the service in which it is defined.

ancp

Syntax: ancp
Context: config>service>vpls>gsmp>group
Description: This command configures Access Node Control Protocol (ANCP) parameters for this GSMP group.

dynamic-topology-discover

Syntax: [no] dynamic-topology-discover
Context: config>service>vpls>gsmp>group>ancp
Description: This command enables the ANCP dynamic topology discovery capability. The no form of this command disables the feature.

idle-filter

Syntax: [no] idle-filter
Context: config>service>vpls>gsmp
config>service>vprn>gsmp

**Description**
This command when applied will filter out new subscriber’s ANCP messages from subscriber with “DSL-line-state” IDLE

**Default**
no idle-filter

---

**line-configuration**

**Syntax**
\[[no\] line-configuration

**Context**
config>service>vpls>gsmp>group>ancp

**Description**
This command enables the ANCP line-configuration capability. The **no** form of this command disables the feature.

---

**oam**

**Syntax**
\[[no\] oam

**Context**
config>service>vpls>gsmp>group>ancp

**Description**
This command specifies whether or not the GSMP ANCP OAM capability should be negotiated at startup of the GSMP connection. The **no** form of this command disables the feature.

---

**hold-multiplier**

**Syntax**
hold-multiplier multiplier
\[no\] hold-multiplier

**Context**
config>service>vpls>gsmp>group

**Description**
This command configures the hold-multiplier for the GSMP connections in this group.

**Parameters**
- **multiplier** — Specifies the GSMP hold multiplier value.
  
  **Values**
  1 — 100

---

**keepalive**

**Syntax**
keepalive seconds
\[no\] keepalive

**Context**
config>service>vpls>gsmp>group

**Description**
This command configures keepalive values for the GSMP connections in this group.
Parameters  

*seconds* — Specifies the GSMP keepalive timer value in seconds.

**Values**  

1 — 25

---

**neighbor**

**Syntax**  

[no] neighbor *ip-address*

**Context**  

config>service>vpls>gsmp>group

**Description**  

This command configures a GSMP ANCP neighbor.

**Parameters**  

*ip-address* — Specifies the IP address of the GSMP ANCP neighbor.

---

**local-address**

**Syntax**  

local-address *ip-address*  
no local-address

**Context**  

config>service>vpls>gsmp>group>neighbor

**Description**  

This command configures the source ip-address used in the connection towards the neighbor. The local address is optional. If specified the node will accept connections only for that address in the service running ANCP. The address may be created after the reference but connections will not be accepted until it is created. If the local address is not used, the system accepts connections on any interface within the routing context.

**Parameters**  

*ip-address* — Specifies the source IP address to be used in the connection toward the neighbor.

---

**priority-marking**

**Syntax**  

priority-marking dscp *dscp-name*  
priority-marking prec *ip-prec-value*  
no priority-marking

**Context**  

config>service>vpls>gsmp>group>neighbor

**Description**  

This command configures the type of priority marking to be used.

**Parameters**  

dscp *dscp-name* — Specifies the DSCP code-point to be used.

**Values**  

be, cp1, cp2, cp3, cp4, cp5, cp6, cp7, cs1, cp9, af11, cp11, af12, cp13, af13, cp15, cs2, cp17, af21, cp19, af22, cp21, af23, cp23, cs3, cp25, af31, cp27, af32, cp29, af33, cp31, cs4, cp33, af41, cp35, af42, cp37, af43, cp39, cs5, cp41, cp42, cp43,
cp44, cp45, ef, cp47, nc1, cp49, cp50, cp51, cp52, cp53, cp54, cp55, nc2, cp57, cp58, cp59, cp60, cp61, cp62, cp63

prec ip-prec-value — Specifies the precedence value to be used.

Values 0 — 7

persistency-database

Syntax

```
persistency-database
no persistency-database
```

Context

```
config>service>vpls <service id>gsmp
config>service>vprn<service id>gsmp
```

Description

This command enables the system to store DSL line information in memory. If the GSMP connection terminates, the DSL line information will remain in memory and accessible for Radius authentication and accounting.

Default no persistency-database
**VPLS STP Commands**

**stp**

**Syntax**

stp

**Context**

config>service>vpls
config>service>vpls>sap
config>service>vpls>spoke-sdp
config>template>vpls-template

**Description**

This command enables the context to configure the Spanning Tree Protocol (STP) parameters. Alcatel-Lucent’s STP is simply the Spanning Tree Protocol (STP) with a few modifications to better suit the operational characteristics of VPLS services. The most evident change is to the root bridge election. Since the core network operating between Alcatel-Lucent’s service routers should not be blocked, the root path is calculated from the core perspective.

**auto-edge**

**Syntax**

auto-edge

no auto-edge

**Context**

config>service>vpls>sap>stp
config>service>vpls>spoke-sdp>stp

**Description**

This command configures automatic detection of the edge port characteristics of the SAP or spoke SDP.

If auto-edge is enabled, and STP concludes there is no bridge behind the spoke SDP, the OPER_EDGE variable will dynamically be set to true. If auto-edge is enabled, and a BPDU is received, the OPER_EDGE variable will dynamically be set to true (see edge-port on page 792).

The no form of this command returns the auto-detection setting to the default value.

**Default**

auto-edge

**edge-port**

**Syntax**

[no] edge-port

**Context**

config>service>vpls>sap>stp
config>service>vpls>spoke-sdp>stp

**Description**

This command configures the SAP or SDP as an edge or non-edge port. If auto-edge is enabled for the SAP, this value will be used only as the initial value.

NOTE: The function of the edge-port command is similar to the rapid-start command. It tells RSTP that it is on the edge of the network (for example, there are no other bridges connected to that port).
and, as a consequence, it can immediately transition to a forwarding state if the port becomes available.

RSTP, however, can detect that the actual situation is different from what edge-port may indicate. Initially, the value of the SAP or spoke SDP parameter is set to edge-port. This value will change if:

- A BPDU is received on that port. This means that after all there is another bridge connected to this port. Then the edge-port becomes disabled.
- If auto-edge is configured and no BPDU is received within a certain period of time, RSTP concludes that it is on an edge and enables the edge-port.

The no form of this command returns the edge port setting to the default value.

Default

no edge-port

forward-delay

Syntax

```
forward-delay seconds
no forward-delay
```

Context

```
config\>service\>vpls\>stp
config\>template\>vpls-template\>stp
```

Description

RSTP, as defined in the IEEE 802.1D-2004 standards, will normally transition to the forwarding state via a handshaking mechanism (rapid transition), without any waiting times. If handshaking fails (e.g. on shared links, see below), the system falls back to the timer-based mechanism defined in the original STP (802.1D-1998) standard.

A shared link is a link with more than two nodes (for example, a shared 10/100BaseT segment). The port-type command is used to configure a link as point-to-point or shared.

For timer-based transitions, the 802.1D-2004 standard defines an internal variable forward-delay, which is used in calculating the default number of seconds that a SAP or spoke SDP spends in the discarding and learning states when transitioning to the forwarding state.

The value of the forward-delay variable depends on the STP operating mode of the VPLS instance:

- in rstp or mstp mode, but only when the SAP or spoke SDP has not fallen back to legacy STP operation, the value configured by the hello-time command is used;
- in all other situations, the value configured by the forward-delay command is used.

Default

15 seconds

Parameters

```
seconds — The forward delay timer for the STP instance in seconds.
```

Values

```
4 — 30
```

hello-time

Syntax

```
hello-time hello-time
no hello-time
```

Context

```
config\>service\>vpls\>stp
```
**General Switch Management Protocol Commands**

```sh
cfg>template>vpls-template>stp
```

**Description**  
This command configures the Spanning Tree Protocol (STP) hello time for the Virtual Private LAN Service (VPLS) STP instance.

The hello time parameter defines the default timer value that controls the sending interval between BPDU configuration messages by this bridge, on ports where this bridge assumes the designated role.

The active hello time for the spanning tree is determined by the root bridge (except when the STP is running in RSTP mode, then the hello time is always taken from the locally configured parameter).

The configured hello-time can also be used to calculate the forward delay. See auto-edge on page 792.

The **no** form of this command returns the hello time to the default value.

**Default**  
2 seconds

**Parameters**  
`hello-time` — The hello time for the STP instance in seconds.

**Values**  
1 — 10

**hold-count**

```sh
hold-count
```

**Syntax**  
`hold-count BDPU tx hold count`

```sh
no hold-count
```

**Context**  
`config>service>vpls>stp`

```sh
config>template>vpls-template>stp
```

**Description**  
This command configures the peak number of BPDUs that can be transmitted in a period of one second.

The **no** form of this command returns the hold count to the default value.

**Default**  
6

**Parameters**  
`BDPU tx hold count` — The hold count for the STP instance in seconds.

**Values**  
1 — 10

**link-type**

```sh
link-type
```

**Syntax**  
`link-type {pt-pt | shared}`

```sh
no link-type
```

**Context**  
`config>service>vpls>sap>stp`

```sh
config>service>vpls>spoke-sdp>stp
```

**Description**  
This command instructs STP on the maximum number of bridges behind this SAP or spoke SDP. If there is only a single bridge, transitioning to forwarding state will be based on handshaking (fast transitions). If more than two bridges are connected via a shared media, their SAP or spoke SDPs should all be configured as shared, and timer-based transitions are used.

The **no** form of this command returns the link type to the default value.
mst-instance

Syntax  mst-instance mst-inst-number

Context  config>service>vpls>sap>stp

Description  This command enables the context to configure MSTI related parameters at SAP level. This context can be open only for existing mst-instances defined at the service level (see mst-instance).

Default  none

Parameters  mst-inst-number — Specifies an existing Multiple Spanning Tree Instance number.

Values  1 — 4094

mst-path-cost

Syntax  mst-path-cost inst-path-cost

no mst-path-cost

Context  config>service>vpls>sap>stp>mst-instance

Description  This commands specifies path-cost within a given instance, expressing probability that a given port will be put into the forwarding state in case a loop occurs (the highest value expresses lowest priority).

The no form of this command sets port-priority to its default value.

Default  The path-cost is proportional to link speed.

Parameters  inst-path-cost — Specifies the contribution of this port to the MSTI path cost of paths towards the spanning tree regional root which include this port.

Values  1 — 20000000

mst-priority

Syntax  mst-priority stp-priority

no mst-priority

Context  config>service>vpls>sap>stp>mst-instance

Description  This commands specifies the port priority within a given instance, expressing probability that a given port will be put into the forwarding state if a loop occurs.

The no form of this command sets port-priority to its default value.

Default  128

Parameters  stp-priority — Specifies the value of the port priority field.
General Switch Management Protocol Commands

max-age

Syntax  
max-age seconds  
no max-age  

Context config>service>vpls>stp  
config>template>vpls-template>stp  

Description  This command indicates how many hops a BPDU can traverse the network starting from the root bridge. The message age field in a BPDU transmitted by the root bridge is initialized to 0. Each other bridge will take the message_age value from BPDUs received on their root port and increment this value by 1. The message_age thus reflects the distance from the root bridge. BPDUs with a message_age exceeding max-age are ignored.  
STP uses the max-age value configured in the root bridge. This value is propagated to the other bridges via the BPDUs.  

The no form of this command returns the max-age to the default value.  

Default  20 seconds  

Parameters  
seconds — The max_info_age for the STP instance in seconds. Allowed values are integers in the range 6 to 40.  

mode

Syntax  
mode {rstp | comp-dot1w | dot1w | mstp | pmstp}  
no mode  

Context config>service>vpls>stp  
config>template>vpls-template>stp  

Description  This command specifies the version of Spanning Tree Protocol the bridge is currently running.  
See section Spanning Tree Operating Modes on page 561 for details on these modes.  
The no form of this command returns the STP variant to the default.  

Default rstp  

Parameters  
dot1w — Corresponds to the mode where the Rapid Spanning Tree is backward compatible with IEEE 802.1w.  
compdot1w — Corresponds to the Rapid Spanning Tree Protocol fully conformant to IEEE 802.1w.  
mstp — Sets MSTP as the STP mode of operation. Corresponds to the Multiple Spanning Tree Protocol specified in 802.1Q REV/D5.0-09/2005  
pmstp — The PMSTP mode is only supported in VPLS services where the mVPLS flag is configured.
mst-instance

**Syntax**

\[ \text{no} \] mst-instance \textit{mst-inst-number}  

**Context**

config>service>vpls>stp

**Description**

This command creates the context to configure MST instance (MSTI) related parameters. Up to 16 instances will be supported by MSTP. The instance 0 is mandatory by protocol and therefore, it cannot be created by the CLI. The software will maintain this instance automatically.

**Default**

none

**Parameters**

\textit{mst-inst-number} — Specifies the Multiple Spanning Tree instance.

\textbf{Values}\n
1 — 4094

mst-priority

**Syntax**

mst-priority \textit{bridge-priority}  

\[ \text{no} \] mst-priority

**Context**

config>service>vpls>stp>mst-instance

**Description**

This command specifies the bridge priority for this specific Multiple Spanning Tree Instance for this service. The \textit{bridge-priority} value reflects likelihood that the switch will be chosen as the regional root switch (65535 represents the least likely). It is used as the highest 4 bits of the Bridge ID included in the MSTP BPDU's generated by this bridge.

The priority can only take on values that are multiples of 4096 (4k). If a value is specified that is not a multiple of 4K, then the value will be replaced by the closest multiple of 4K, which is lower than the value entered.

The \texttt{no} form of this command sets the bridge-priority to its default value.

**Default**

32768 — All instances created by \texttt{vlan-range} command and not having explicit definition of bridge-priority will inherit default value.

**Parameters**

\textit{bridge-priority} — Specifies the priority of this specific Multiple Spanning Tree Instance for this service.

\textbf{Values}\n
0 — 65535

vlan-range

**Syntax**

\[ \text{no} \] vlan-range \textit{vlan-range}  

**Context**

config>service>vpls>stp>mst-instance

**Description**

This command specifies a range of VLANs associated with a certain MST-instance. This range applies to all SAPs of the mVPLS.

Every VLAN range that is not assigned within any of the created \texttt{mst-instance} is automatically assigned to mst-instance 0. This instance is automatically maintained by the software and cannot be
modified. Changing the VLAN range value can be performed only when the given mst-instance is shutdown.

The no form of this command removes the vlan-range from given mst-instance.

**Parameters**  
**vlan-range** — The first VLAN range specifies the left-bound (i.e., minimum value) of a range of VLANs that are associated with the mVPLS SAP. This value must be smaller than (or equal to) the second VLAN range value. The second VLAN range specifies the right-bound (i.e., maximum value) of a range of VLANs that are associated with the mVPLS SAP.

**Values**  
1 to 4094 — 1 to 4094

**mst-max-hops**

**Syntax**  
```plaintext
mst-max-hops hops-count  
no mst-max-hops
```

**Context**  
```plaintext
config>service>vpls>stp
```

**Description**  
This command specifies the number of hops in the region before BPDU is discarded and the information held for the port is aged out. The root bridge of the instance sends a BPDU (or M-record) with remaining-hop-count set to configured `<max-hops>`. When a bridge receives the BPDU (or M-record), it decrements the received remaining-hop-count by 1 and propagates it in BPDU (or M-record) it generates.

The no form of this command sets the hops-count to its default value.

**Default**  
20

**Parameters**  
**hops-count** — Specifies the maximum number of hops.

**Values**  
1 — 40

**mst-name**

**Syntax**  
```plaintext
mst-name region-name  
no mst-name
```

**Context**  
```plaintext
config>service>vpls>stp
```

**Description**  
This command defines an MST region name. Two bridges are considered as a part of the same MST region as soon as their configuration of the MST region name, the MST-revision and VLAN-to-instance assignment is identical.

The no form of this command removes region-name from the configuration.

**Default**  
no mst-name

**Parameters**  
**region-name** — Specifies an MST-region name up to 32 characters in length.
VPLS > sdp

**Syntax**

```
mst-revision revision-number
```

**Context**

```
config>service>vpls>stp
```

**Description**

This command defines the MST configuration revision number. Two bridges are considered as a part of the same MST region as soon as their configuration of MST-region name, MST-revision and VLAN-to-instance assignment is identical.

The `no` form of this command returns MST configuration revision to its default value.

**Default**

0

**Parameters**

- **revision-number** — Specifies the MSTP region revision number to define the MSTP region.
  - **Values**
    - 0 — 65535

---

VPLS > sap

**Syntax**

```
path-cost sap-path-cost
```

**no path-cost**

**Context**

```
config>service>vpls>sap>stp
config>service>vpls>spoke-sdp>stp
```

**Description**

This command configures the Spanning Tree Protocol (STP) path cost for the SAP or spoke SDP.

The path cost is used by STP to calculate the path cost to the root bridge. The path cost in BPDUs received on the root port is incremented with the configured path cost for that SAP or spoke SDP. When BPDUs are sent out other egress SAPs or spoke SDPs, the newly calculated root path cost is used. These are the values used for CIST when running MSTP.

STP suggests that the path cost is defined as a function of the link bandwidth. Since SAPs and spoke SDPs are controlled by complex queuing dynamics, in the SR-OS the STP path cost is a purely static configuration.

The `no` form of this command returns the path cost to the default value.

- **path-cost** — The path cost for the SAP or spoke SDP.
  - **Values**
    - 1 — 200000000 (1 is the lowest cost)
  - **Default**
    - 10

---

VPLS > sap

**Syntax**

```
port-num virtual-port-number
```

**Context**

```
config>service>vpls>sap>stp
config>service>vpls>spoke-sdp>stp
```

**Description**

This command configures the virtual port number which uniquely identifies a SAP within configuration bridge protocol data units (BPDUs). The internal representation of a SAP is unique to a
system and has a reference space much bigger than the 12 bits definable in a configuration BPDU. STP takes the internal representation value of a SAP and identifies it with its own virtual port number that is unique to every other SAP defined on the TLS. The virtual port number is assigned at the time that the SAP is added to the TLS. Since the order that the SAP was added to the TLS is not preserved between reboots of the system, the virtual port number may change between restarts of the STP instance.

The virtual port number cannot be administratively modified.

**priority**

**Syntax**

```
priority bridge-priority
no priority
```

**Context**

```
config>service>vpls>stp
config>template>vpls-template>stp
```

**Description**

The bridge-priority command is used to populate the priority portion of the bridge ID field within outbound BPDUs (the most significant 4 bits of the bridge ID). It is also used as part of the decision process when determining the best BPDUs between messages received and sent. All values will be truncated to multiples of 4096, conforming with IEEE 802.1t and 802.1D-2004.

The no form of this command returns the bridge priority to the default value.

**Default**

By default, the bridge priority is configured to 4096 which is the highest priority.

**Parameters**

- `bridge-priority` — The bridge priority for the STP instance.

  **Values**

  Allowed values are integers in the range of 4096 — 65535 with 4096 being the highest priority. The actual bridge priority value stored/used is the number entered with the lowest 12 bits masked off which means the actual range of values is 4096 to 61440 in increments of 4096.

**priority**

**Syntax**

```
priority stp-priority
no priority
```

**Context**

```
config>service>vpls>spoke-sdp
config>service>vpls>sap>stp
```

**Description**

This command configures the Alcatel-Lucent Spanning Tree Protocol (STP) priority for the SAP or spoke SDP.

STP priority is a configurable parameter associated with a SAP or spoke SDP. When configuration BPDUs are received, the priority is used in some circumstances as a tie breaking mechanism to determine whether the SAP or spoke SDP will be designated or blocked.

In traditional STP implementations (802.1D-1998), this field is called the port priority and has a value of 0 to 255. This field is coupled with the port number (0 to 255 also) to create a 16 bit value. In the latest STP standard (802.1D-2004) only the upper 4 bits of the port priority field are used to encode the SAP or spoke SDP priority. The remaining 4 bits are used to extend the port ID field into a 12 bit
virtual port number field. The virtual port number uniquely references a SAP or spoke SDP within the STP instance.

STP computes the actual priority by taking the input value and masking out the lower four bits. The result is the value that is stored in the SDP priority parameter. For instance, if a value of 0 is entered, masking out the lower 4 bits results in a parameter value of 0. If a value of 255 is entered, the result is 240.

The **no** form of this command returns the STP priority to the default value.

<table>
<thead>
<tr>
<th>Default</th>
<th>128</th>
</tr>
</thead>
</table>

**Parameters**

**stp-priority** — The STP priority value for the SAP or spoke SDP. Allowed values are integer in the range of 0 to 255, 0 being the highest priority. The actual value used for STP priority (and stored in the configuration) will be the result of masking out the lower 4 bits, thus the actual value range is 0 to 240 in increments of 16.

| Default | 128 |
### VPLS SAP Commands

**sap**

**Syntax**

```
sap sap-id [split-horizon-group group-name] [create] [eth-ring ring-index]
no sap sap-id
```

**Context**

`config>service>vpls`

**Description**

This command creates a Service Access Point (SAP) within a service. A SAP is a combination of port and encapsulation parameters which identifies the service access point on the interface and within the 7950 SR. Each SAP must be unique.

All SAPs must be explicitly created. If no SAPs are created within a service or on an IP interface, a SAP will not exist on that object.

Enter an existing SAP without the `create` keyword to edit SAP parameters. The SAP is owned by the service in which it was created.

A SAP can only be associated with a single service. A SAP can only be defined on a port that has been configured as an access port using the `config interface port-type port-id mode access` command. Channelized TDM ports are always access ports.

If a port is shutdown, all SAPs on that port become operationally down. When a service is shutdown, SAPs for the service are not displayed as operationally down although all traffic traversing the service will be discarded. The operational state of a SAP is relative to the operational state of the port on which the SAP is defined.

The `no` form of this command deletes the SAP with the specified port. When a SAP is deleted, all configuration parameters for the SAP will also be deleted. For Internet Enhanced Service (IES), the IP interface must be shutdown before the SAP on that interface may be removed.

**Default**

No SAPs are defined.

**Special Cases**

A VPLS SAP can be defined with Ethernet ports, SONET/SDH or TDM channels. The limits of the number of SAPs and SDPs supported in a VPLS service depends on the hardware used. Each SDP must have a unique destination or an error will be generated. Split horizon groups can only be created in the scope of a VPLS service.

A default SAP has the following format: `port-id:*`. This type of SAP is supported only on Ethernet MDAs and its creation is allowed only in the scope of Layer 2 services (Epipe and VPLS). This type of SAP is mutually exclusive with a SAP defined by explicit null encapsulation (for example, `1/1/1:0`).

**Parameters**

- `sap-id` — Specifies the physical port identifier portion of the SAP definition. See Common CLI Command Descriptions on page 1783 for command syntax.

- `create` — Keyword used to create a SAP instance. The `create` keyword requirement can be enabled/disabled in the `environment>create` context.
cflowd

**Syntax**

[no] cflowd

**Context**

`config>service>vpls>sap`

**Description**

This command enables cflowd to collect traffic flow samples through a service interface (SAP) for analysis. When cflowd is enabled on an ethernet service SAP, the ethernet traffic can be sampled and processed by the system's cflowd engine and exported to IPFIX collectors with the l2-ip template enabled.

cflowd is used for network planning and traffic engineering, capacity planning, security, application and user profiling, performance monitoring, usage-based billing, and SLA measurement. When cflowd is enabled at the SAP level, all packets forwarded by the interface are subjected to analysis according to the cflowd configuration.

For Layer 2 services, only ingress sampling is supported.

**Default**

no cflowd

discard-unknown-source

**Syntax**

[no] discard-unknown-source

**Context**

`config>service>vpls>sap`
`config>service>vpls>spoke-sdp`

**Description**

When this command is enabled, packets received on a SAP or a spoke SDP with an unknown source MAC address will be dropped only if the maximum number of MAC addresses for that SAP or spoke SDP (see `max-nbr-mac-addr on page 814`) has been reached. If max-nbr-mac-addr has not been set for the SAP or spoke SDP, enabling discard-unknown-source has no effect.

When disabled, the packets are forwarded based on the destination MAC addresses.

The no form of this command causes packets with an unknown source MAC addresses to be forwarded by destination MAC addresses in VPLS.

**Default**

no discard-unknown
ETH-CFM Service Commands

eth-cfm

Syntax

eth-cfm

Context

config>service>vpls
config>service>vpls>mesh-sdp
config>service>vpls>spoke-sdp
config>service>vpls>sap

Description
This command enables the context to configure ETH-CFM parameters.

eth-tunnel

Syntax

eth-tunnel

Context

config>service>vpls>sap

Description
The command enables the context to configure Ethernet Tunnel SAP parameters.

eth-ring

Syntax

eth-ring ring-id

no eth-ring

Context

config>service>vpls

Description
This command configures a VPLS Sap to be associated with an Ethernet ring. The Sap port-id is associated with the corresponding Ethernet ring path configured on the same port-id. The encapsulation type must be compatible with the Eth-ring path encapsulation.

The no form of this command removes eth-ring from this SAP

Default

no eth-ring

Parameters

ring-id — Specifies the ring ID.

Values

1-128

path

Syntax

path path-index tag qtag[,qtag]

no path path-index

Context

config>service>vpls>sap>eth-tunnel
Description
This command configures Ethernet tunnel SAP path parameters. The no form of the command removes the values from the configuration.

Default
none

Parameters

- **path-index** — Specifies the path index value.
  - **Values**
    - 1 — 16

- **tag qtag[qtag]** — Specifies the qtag value.
  - **Values**
    - 0 — 4094, *

mep

Syntax
```
mep mep-id domain md-index association ma-index [direction {up | down}] primary-vlan-enable [vlan vlan-id] 
no mep mep-id domain md-index association ma-index 
```

Context
```
config>service>vpls>mesh-sdp>eth-cfm 
config>service>vpls>spoke-sdp>eth-cfm 
config>service>vpls>eth-cfm 
config>service>vpls>sap>eth-cfm 
```

Description
This command configures the ETH-CFM maintenance endpoint (MEP). A MEP created at the VPLS service level vpls>eth-cfm creates a virtual MEP.
The no version of the command will remove the MEP.

Parameters

- **mep-id** — Specifies the maintenance association end point identifier.
  - **Values**
    - 1 — 8191

- **md-index** — Specifies the maintenance domain (MD) index value.
  - **Values**
    - 1 — 4294967295

- **ma-index** — Specifies the MA index value.
  - **Values**
    - 1 — 4294967295

- **direction up|down** — Indicates the direction in which the maintenance association (MEP) faces on the bridge port. Direction is not supported when a MEP is created directly under the vpls>eth-cfm construct (vMEP).
  - down — Sends ETH-CFM messages away from the MAC relay entity.
  - up — Sends ETH-CFM messages towards the MAC relay entity.

- **primary-vlan-enable** — Provides a method for linking the MEP with the primary VLAN configured under the bridge-identifier for the MA. MEPs can not be changed from or to primary vlan functions. This must be configured as part of the creation step and can only be changed by deleting the MEP and recreating it. Primary VLANs are only supported under Ethernet SAPs.

- **vlan** — A required parameter when including primary-vlan-enable. Provides a method for associating the VLAN under the bridge-identifier under the MA with the MEP.
**mip**

**Syntax**

- `mip [mac mac-address] primary-vlan-enable [vlan vlan-id]`
- `mip default-mac`
- `no mip`

**Context**

- `config>service>vpls>sap>eth-cfm`
- `config>service>vpls>spoke-sdp>eth-cfm`

**Description**

This command allows Maintenance Intermediate Points (MIPs). The creation rules of the MIP are dependant on the mhf-creation configuration for the MA. This MIP option is only available for default and static mhf-creation methods.

**Parameters**

- `mac-address` — Specifies the MAC address of the MEP.
  - **Values**
    - 6-byte mac-address in the form of xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx of the MIP. The MAC must be unicast. Using the all zeros address is equivalent to the no form of this command.

- `default-mac` — Using the no command deletes the MIP. If the operator wants to change the mac back to the default mac without having to delete the MIP and reconfiguring this command is useful.

- `primary-vlan-enable` — Provides a method for linking the MIP with the primary VLAN configured under the bridge-identifier for the MA. This is only allowed if the mhf-creation method is static. MIPs can not be changed from or to primary vlan functions without first being deleted. This must be configured as part of the creation step and can only be changed by deleting the MEP and recreating it. Primary VLANs are only supported under Ethernet SAPs.

- `vlan` — A required parameter when including primary-vlan-enable. Provides a method for associating the VLAN under the bridge-identifier under the MA with the MIP.

**Default**

`no mip`

---

**mip**

**Syntax**

- `mip primary-vlan-enable [vlan vlan-id]`
- `no mip`

**Context**

- `config>service>template>vpls-sap-template>eth-cfm`

**Description**

This command allows Maintenance Intermediate Points (MIPs). The creation rules of the MIP are dependant on the mhf-creation configuration for the MA. This MIP option is only available for default and static mhf-creation methods.
Parameters

**primary-vlan-enable** — Provides a method for linking the MIP with the primary VLAN configured under the bridge-identifier for the MA. This is only allowed if the mhf-creation method is static. MIPs can not be changed from or to primary vlan functions without first being deleted. This must be configured as part of the creation step and can only be changed by deleting the MEP and recreating it. Primary VLANS are only supported under Ethernet SAPs.

**vlan** — A required parameter when including primary-vlan-enable. Provides a method for associating the VLAN under the bride-identifier under the MA with the MIP.

**vlan-id** — Must match the vlan-id under the bridge-identifier for the MA that is appropriate for this service

**Values**

0 — 4094

**ais-enable**

**Syntax**

[no] ais-enable

**Context**

config>service>vpls>mesh-sdp>eth-cfm>mep
config>service>vpls>spoke-sdp>eth-cfm>mep

**Description**

This command enables the generation and the reception of AIS messages.

**interface-support-enable**

**Syntax**

[no] interface-support-enable

**Context**

config>service>vpls>mesh-sdp>eth-cfm>mep>ais
config>service>vpls>spoke-sdp>eth-cfm>mep>ais
config>service>vpls>mesh-sdp>eth-cfm>mep>ais

**Description**

This command enables the AIS function to consider the operational state of the entity on which it is configured. With this command, ETH-AIS on DOWN MEPs will be triggered and cleared based on the operational status of the entity on which it is configured. If CCM is also enabled then transmission of the AIS PDU will be based on either the non operational state of the entity or on ANY CCM defect condition. AIS generation will cease if BOTH operational state is UP and CCM has no defect conditions. If the MEP is not CCM enabled then the operational state of the entity is the only consideration assuming this command is present for the MEP.

**Default**

[no] interface-support-enabled (AIS will not be generated or stopped based on the state of the entity on) which the DOWN MEP is configured.

**client-meg-level**

**Syntax**

client-meg-level [[level [level ...]]
no client-meg-level

**Context**

config>service>vpls>mesh-sdp>eth-cfm>mep>ais-enable
config>service>vpls>spoke-sdp>eth-cfm>mep>ais-enable
Description  This command configures the client maintenance entity group (MEG) level(s) to use for AIS message generation. Up to 7 levels can be provisioned with the restriction that the client MEG level must be higher than the local MEG level.

Parameters  

- **level** — Specifies the client MEG level.
  - Values  1 — 7
  - Default  1

ccm-padding-size

**Syntax**  

```
ccm-padding-size ccm-padding
no ccm-padding-size ccm-padding
```

**Context**  

```
config>service>vpls>mesh-sdp>eth-cfm>mep
config>service>vpls>sap>eth-cfm>mep
config>service>vpls>spoke-sdp>eth-cfm>mep
```

**Description**  

Set the byte size of the optional Data TLV to be included in the ETH-CC PDU. This will increase the size of the ETH-CC PDU by the configured value. The base size of the ETH-CC PDU, including the Interface Status TLV and Port Status TLV, is 83 bytes not including the Layer Two encapsulation. CCM padding is not supported when the CCM-Interval is less than one second.

**Default**  

[no] ccm-padding-size

**Parameters**  

- **ccm-padding** — specifies the byte size of the Optional Data TLV
  - Values  3 — 1500

csf-enable

**Syntax**  

```
[no] csf-enable
```

**Context**  

```
config>service>vpls>mesh-sdp>eth-cfm>mep
config>service>vpls>sap>eth-cfm>mep
config>service>vpls>spoke-sdp>eth-cfm>mep
```

**Description**  

This command enables the reception and local processing of ETH-CSF frames.

multiplier

**Syntax**  

```
multiplier multiplier-value
no multiplier
```

**Context**  

```
config>service>vpls>mesh-sdp>eth-cfm>mep>cfs-enable
config>service>vpls>sap>eth-cfm>mep>cfs-enable
config>service>vpls>spoke-sdp>eth-cfm>mep>cfs-enable
```
Description
This command enables the multiplication factor applied to the receive time used to clear the CSF condition in increments of .5.

Default
3.5

Parameters
multiplier-value — Specifies the multiplier used for timing out CSF.

Values
0.0, 2.0 .. 30.0

interval

Syntax
interval {1 | 60}
no interval

Context
config>service>vpls>mesh-sdp>eth-cfm>mep>ais-enable
config>service>vpls>spoke-sdp>eth-cfm>mep>ais-enable

Description
This command specifies the transmission interval of AIS messages in seconds.

Parameters
1 | 60 — The transmission interval of AIS messages in seconds.

Default
1

priority

Syntax
priority priority-value
no priority

Context
config>service>vpls>mesh-sdp>eth-cfm>mep>ais-enable
config>service>vpls>spoke-sdp>eth-cfm>mep>ais-enable

Description
This command specifies the priority of AIS messages originated by the node.

Parameters
priority-value — Specify the priority value of the AIS messages originated by the node.

Values
0 — 7

Default
1

ccm-enable

Syntax
[no] ccm-enable

Context
config>service>vpls>eth-cfm>mep
config>service>vpls>sap>eth-cfm>mep
config>service>vpls>mesh-sdp>mep
config>service>vpls>spoke-sdp>eth-cfm>mep

Description
This command enables the generation of CCM messages.
The no form of the command disables the generation of CCM messages.
ccm-ltm-priority

Syntax:  
ccm-ltm-priority priority  
no ccm-ltm-priority

Context:  
config>service>vpls>eth-cfm>mep  
config>service>vpls>sap>eth-cfm>mep  
config>service>vpls>mesh-sdp>eth-cfm>mep  
config>service>vpls>spoke-sdp>eth-cfm>mep

Description:  
This command specifies the priority value for CCMs and LTMs transmitted by the MEP. The no form of the command removes the priority value from the configuration.

Default:  
The highest priority on the bridge-port.

Parameters:  
priority — Specifies the priority of CCM and LTM messages.

Values:  
0 — 7

eth-test-enable

Syntax:  
[no] eth-test-enable

Context:  
config>service>vpls>.sap>eth-cfm>mep  
config>service>vpls>spoke-sdp>eth-cfm>mep  
config>service>vpls>mesh-sdp>eth-cfm>mep

Description:  
For ETH-test to work, operators need to configure ETH-test parameters on both sender and receiver nodes. The ETH-test then can be done using the following OAM commands:

```
oam eth-cfm eth-test mac-address mep mep-id domain md-index association ma-index [priority priority] [data-length data-length]
```

A check is done for both the provisioning and test to ensure the MEP is an Y.1731 MEP (MEP provisioned with domain format none, association format icc-based). If not, the operation fails. An error message in the CLI and SNMP will indicate the problem.

test-pattern

Syntax:  
test-pattern {all-zeros | all-ones} [crc-enable]  
no test-pattern

Context:  
config>service>vpls>sap>eth-cfm>mep>eth-test-enable  
config>service>vpls>spoke-sdp>eth-cfm>mep>eth-test-enable  
config>service>vpls>mesh-sdp>eth-cfm>mep>eth-test-enable

Description:  
This command configures the test pattern for eth-test frames. The no form of the command removes the values from the configuration.

Parameters:  
all-zeros — Specifies to use all zeros in the test pattern.
all-ones — Specifies to use all ones in the test pattern.
crc-enable — Generates a CRC checksum.
  Default all-zeros

fault-propagation-enable

Syntax  fault-propagation-enable (use-if-tlv | suspend-ccm)
  no fault-propagation-enable

Context  config>service>vpls>mesh-sdp>eth-cfm>mep
  config>service>vpls>sap>eth-cfm>mep
  config>service>vpls>spoke-sdp>eth-cfm>mep

Description  This command configures the fault propagation for the MEP.

Parameters  use-if-tlv — Specifies to use the interface TLV.
  suspend-ccm — Specifies to suspend the continuity check messages.

low-priority-defect

Syntax  low-priority-defect {allDef|macRemErrXcon|remErrXcon|errXcon|xcon|noXcon}

Context  config>service>vpls>mesh-sdp>eth-cfm>mep
  config>service>vpls>sap>eth-cfm>mep
  config>service>vpls>spoke-sdp>eth-cfm>mep

Description  This command specifies the lowest priority defect that is allowed to generate a fault alarm.

Default  macRemErrXcon

Values  allDef  DefRDICCM, DefMACstatus, DefRemoteCCM, DefErrorCCM, and DefXconCCM
  macRemErrXcon  Only DefMACstatus, DefRemoteCCM, DefErrorCCM, and DefXconCCM
  remErrXcon  Only DefRemoteCCM, DefErrorCCM, and DefXconCCM
  errXcon  Only DefErrorCCM and DefXconCCM
  xcon  Only DefXconCCM; or
  noXcon  No defects DefXcon or lower are to be reported

mac-address

Syntax  mac-address mac-address
  no mac-address

Context  config>service>vpls>eth-cfm>mep
  config>service>vpls>sap>eth-cfm>mep
  config>service>vpls>spoke-sdp>eth-cfm>mep
config>service>vpls>mesh-sdp>eth-cfm>mep

**Description**
This command specifies the MAC address of the MEP. The `no` form of this command reverts the MAC address of the MEP back to that of the port (if the MEP is on a SAP) or the bridge (if the MEP is on a spoke).

**Parameters**
- `mac-address` — Specifies the MAC address of the MEP.
  - **Values**
    - 6-byte mac-address in the form of xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx of the MEP. Must be unicast. Using the all zeros address is equivalent to the `no` form of this command.

one-way-delay-threshold

**Syntax**
`one-way-delay-threshold seconds`

**Context**
`config>service>vpls>sap>eth-cfm>mep`

**Description**
This command enables/disables eth-test functionality on MEP.

**Parameters**
- `seconds` — Specifies the one way delay threshold, in seconds.
  - **Values**
    - 0..600
  - **Default**
    - 3

**tunnel-fault**

**Syntax**
tunnel-fault {accept | ignore}

**Context**
`config>service>vpls>eth-cfm`
`config>service>vpls>sap>eth-cfm`

**Description**
Allows the individual service SAPs to react to changes in the tunnel MEP state. When tunnel-fault accept is configured at the service level, the SAP will react according to the service type, Epipe will set the operational flag and VPLS, IES and VPRN SAP operational state will become down on failure or up on clear. This command triggers the OAM mapping functions to mate SAPs and bindings in an Epipe service as well as setting the operational flag. If AIS generation is the requirement for the Epipe services this command is not required. See the command ais-enable under epipe>sap>eth-cfm>ais-enable for more details. This works in conjunction with the tunnel-fault accept on the individual SAPs. Both must be set to accept to react to the tunnel MEP state. By default the service level command is “ignore” and the sap level command is “accept”. This means simply changing the service level command to “accept” will enable the feature for all SAPs. This is not required for Epipe services that only wish to generate AIS on failure.

**Parameters**
- `accept` — Share fate with the facility tunnel MEP
- `ignore` — Do not share fate with the facility tunnel MEP

**Default**
- `ignore` (Service Level)
- `accept` (SAP Level for Epipe and VPLS)
vmep-extensions

Syntax
vmep-extensions
[no] vmep-extensions

Context
config>service>vpls>eth-cfm

Description
This command enables and disables enhanced Virtual Maintenance Endpoints functionality. This must manually be configured for a B-VPLS to change the legacy behavior and cannot be disable for VPLS contexts that are not BVPLS based.

The no form of the command reverts to the default values. This is not applicable to a VPLS contexts that is not B-VPLS based.

Default
no vmep-extensions (for B-VPLS)
vmep-extensions (for VPLS contexts not B-VPLS based)

vmep-filter

Syntax
vmep-filter
[no] vmep-filter

Context
config>service>vpls>eth-cfm>sap
config>service>vpls>eth-cfm>spoke-sdp
config>service>vpls>eth-cfm>mesh-sdp

Description
Suppress eth-cfm PDUs based on level lower than or equal to configured Virtual MEP. This command is not supported under a B-VPLS context. This will also delete any MIP configured on the SAP or Spoke-SDP.

The no form of the command reverts to the default values.

Default
no vmep-filter

limit-mac-move

Syntax
limit-mac-move [blockable | non-blockable]
no limit-mac-move

Context
config>service>vpls>spoke-sdp
config>service>vpls>sap

Description
This command indicates whether or not the mac-move agent, when enabled using config>service>vpls>mac-move or config>service>epipe>mac-move, will limit the MAC re-learn (move) rate on this SAP.

Default
blockable

Parameters
blockable — The agent will monitor the MAC re-learn rate on the SAP, and it will block it when the re-learn rate is exceeded.
non-blockable — When specified, this SAP will not be blocked, and another blockable SAP will be blocked instead.

mac-pinning

Syntax

```
[no] mac-pinning
```

Context

```
config>service>vpls>spoke-sdp
config>service>vpls>mesh-sdp
config>service>vpls>sap
config>service>vpls>endpoint
```

Description

Enabling this command will disable re-learning of MAC addresses on other SAPs within the VPLS. The MAC address will remain attached to a given SAP for duration of its age-timer. The age of the MAC address entry in the FIB is set by the age timer. If mac-aging is disabled on a given VPLS service, any MAC address learned on a SAP/SDP with mac-pinning enabled will remain in the FIB on this SAP/SDP forever. Every event that would otherwise result in re-learning will be logged (MAC address; original-SAP; new-SAP).

Default

When a SAP or spoke SDP is part of a Residential Split Horizon Group (RSHG), MAC pinning is activated at creation of the SAP. Otherwise, MAC pinning is not enabled by default.

max-nbr-mac-addr

Syntax

```
max-nbr-mac-addr table-size
```

```
no max-nbr-mac-addr
```

Context

```
config>service>vpls>sap
config>service>vpls>spoke-sdp
config>service>vpls>endpoint
```

Description

This command specifies the maximum number of FDB entries for both learned and static MAC addresses for this SAP, spoke SDP or endpoint.

When the configured limit has been reached, and discard-unknown-source has been enabled for this SAP or spoke SDP (see discard-unknown-source on page 803), packets with unknown source MAC addresses will be discarded.

The no form of the command restores the global MAC learning limitations for the SAP or spoke SDP.

Default

no max-nbr-mac-addr

Parameters

```
table-size — Specifies the maximum number of learned and static entries allowed in the FDB of this service.
```

Values

```
1 — 511999
```

Chassis-mode C limit: 196607
Chassis-mode D limit: 511999
mc-endpoint

Syntax  
mc-endpoint mc-ep-id
mc-endpoint

Context  
config>service>vpls>endpoint

Description  
This command specifies the identifier associated with the multi-chassis endpoint. This value should be the same on both MC-EP peers for the pseudowires that must be part of the same group.

The no form of this command removes the endpoint from the MC-EP. Single chassis behavior applies.

Default  
no mc-endpoint

Parameters  
mc-ep-id — Specifies a multi-chassis endpoint ID.

Values  
1 — 4294967295

mc-ep-peer

Syntax  
mc-ep-peer name
mc-ep-peer ip-address
no mc-ep-peer

Context  
config>service>vpls>endpoint>mc-ep

Description  
This command adds multi-chassis endpoint object.

The no form of this command removes the MC-Endpoint object.

Default  
mc-endpoint is not provisioned.

Parameters  
name — Specifies the name of the multi-chassis end-point peer.

ip-address — Specifies the IP address of multi-chassis end-point peer.

multi-service-site

Syntax  
multi-service-site customer-site-name
no multi-service-site

Context  
config>service>vpls>sap

Description  
This command associates the SAP with a customer-site-name. If the specified customer-site-name does not exist in the context of the service customer ID an error occurs and the command will not execute. If customer-site-name exists, the current and future defined queues on the SAP (ingress and egress) will attempt to use the scheduler hierarchies created within customer-site-name as parent schedulers.

This command is mutually exclusive with the SAP ingress and egress scheduler-policy commands. If a scheduler-policy has been applied to either the ingress or egress nodes on the SAP, the multi-
service-site command will fail without executing. The locally applied scheduler policies must be removed prior to executing the multi-service-site command.

The **no** form of the command removes the SAP from any multi-service customer site the SAP belongs to. Removing the site can cause existing or future queues to enter an orphaned state.

**Default**

None

customer-site-name — The customer-site-name must exist in the context of the customer-id defined as the service owner. If customer-site-name exists and local scheduler policies have not been applied to the SAP, the current and future queues defined on the SAP will look for their parent schedulers within the scheduler hierarchies defined on customer-site-name.

**Values**

Any valid customer-site-name created within the context of the customer-id.

**precedence**

**Syntax**

```plaintext
precedence [precedence-value | primary]
no precedence
```

**Context**

`config>service>vpls>spoke-sdp`

**Description**

This command configures the precedence of this SDP bind when there are multiple SDP binds attached to one service endpoint. When an SDP bind goes down, the next highest precedence SDP bind begins forwarding traffic.

**Parameters**

`precedence-value` — Specifies the precedence of this SDP bind.

**Values**

1 — 4

`primary` — Assigns this as the primary spoke-sdp.

**static-isid**

**Syntax**

```plaintext
[no] static-isid range entry-id isid [to isid] [create]
```

**Context**

`config>service>vpls><instance> b-vpls>sap`

`config>service>vpls><instance> b-vpls>spokeSdp`

**Description**

This command identifies a set of ISIDs for I-VPLS services that are external to SPBM. These ISIDs are advertised as supported locally on this node unless an altered by an isid-policy. This allows communication from I-VPLS services external to SPBM through this node. The SAP may be a regular SAP or MC-LAG SAP. The spoke SDP may be a active/standby spoke. When used with MC-Lag or active/stand-by PWs the conditional static-mac must be configured. ISIDs declared this way become part of the ISID multicast and consume MFIBs. Multiple SPBM static-isid ranges are allowed under a SAP/spoke SDP.

The static-isids are associated with a remote BMAC that must be declared as a static-mac for unicast traffic. ISIDs are advertised as if they were attached to the local BMAC. Only remote I-VPLS ISIDs need to be defined. In the MFIB, the group MACs are then associated with the active SAP or spoke SDP. An ISID policy may be defined to suppress the advertisement of an ISID if the ISID is primary used for unicast services. The following rules govern the usage of multiple ISID statements:
• overlapping values are allowed:
  – isid from 301 to 310
  – isid from 305 to 315
  – isid 316

• the minimum and maximum values from overlapping ranges are considered and displayed. The
  above entries will be equivalent with “ISID from 301 to 316” statement.

• there is no consistency check with the content of ISID statements from other entries. The entries
  will be evaluated in the order of their IDs and the first match will cause the implementation to
  execute the associated action for that entry.

no isid - removes all the previous statements under one interface

no isid value | from value to higher-value - removes a specific ISID value or range. Must match a
previously used positive statement: for example if the command “isid 316 to 400” was used using “no
isid 316 to 350” will not work but “no isid 316 to 400 will be successful.

Parameters

entry-id — Sets context for specified entry ID for the static-isids.

Values

1— 65535

isd — Configures the ISID or the start of an ISID range. Specifies the ISID value in 24 bits. When
just one present identifies a particular ISID to be used for matching.

Values 0..16777215

to isid — Identifies upper value in a range of ISIDs to be used as matching criteria.

Values 0..16777215

static-mac

Syntax [no] static-mac ieee-mac-address [create]

Context config>service>vpls>sap
config>service>vpls>mesh-sdp
config>service>vpls>spoke-sdp

Description This command creates a local static MAC entry in the Virtual Private LAN Service (VPLS)
forwarding database (FDB) associated with the Service Access Point (SAP).

In a VPLS service, MAC addresses are associated with a Service Access Point (SAP) or with a
Service Distribution Point (SDP). MACs associated with a SAP are classified as local MACs, and
MACs associated with an SDP are remote MACs.

Local static MAC entries create a permanent MAC address to SAP association in the forwarding
database for the VPLS instance so that MAC address will not be learned on the edge device.

Note that static MAC definitions on one edge device are not propagated to other edge devices
participating in the VPLS instance, that is, each edge device has an independent forwarding database
for the VPLS.

Only one static MAC entry (local or remote) can be defined per MAC address per VPLS instance.
By default, no static MAC address entries are defined for the SAP.
The **no** form of this command deletes the static MAC entry with the specified MAC address associated with the SAP from the VPLS forwarding database.

**Parameters**

- `ieee-mac-address` — Specifies the 48-bit MAC address for the static ARP in the form `aa:bb:cc:dd:ee:ff` or `aa-bb-cc-dd-ee-ff` where `aa`, `bb`, `cc`, `dd`, `ee` and `ff` are hexadecimal numbers. Allowed values are any non-broadcast, non-multicast MAC and non-IEEE reserved MAC addresses.

- `create` — This keyword is mandatory when specifying a static MAC address.

**managed-vlan-list**

**Syntax**

```plaintext
managed-vlan-list
```

**Context**

`config>service>vpls>sap`

**Description**

This command enables the context to configure VLAN ranges to be managed by a management VPLS. The list indicates, for each SAP, the ranges of associated VLANs that will be affected when the SAP changes state. This managed-vlan-list is not used when STP mode is MSTP in which case the vlan-range is taken from the `config>service>vpls>stp>msti` configuration.

This command is only valid when the VPLS in which it is entered was created as a management VPLS.

**default-sap**

**Syntax**

```plaintext
[no] default-sap
```

**Context**

`config>service>vpls>sap>managed-vlan-list`

**Description**

This command adds a default SAP to the managed VLAN list. The **no** form of the command removes the default SAP to the managed VLAN list.

**range**

**Syntax**

```plaintext
[no] range vlan-range
```

**Context**

`config>service>vpls>sap>managed-vlan-list`

**Description**

This command configures a range of VLANs on an access port that are to be managed by an existing management VPLS.

This command is only valid when the VPLS in which it is entered was created as a management VPLS, and when the SAP in which it was entered was created on an Ethernet port with encapsulation type of dot1q or qinq, or on a Sonet/SDH port with encapsulation type of bcp-dot1q.

To modify the range of VLANs, first the new range should be entered and afterwards the old range removed. See **Modifying VPLS Service Parameters on page 705**.

**Default**

None
Parameters

*vlan-range* — Specify the VLAN start value and VLAN end value. The end-vlan must be greater than start-vlan. The format is `<start-vlan>-<end-vlan>`

**Values**

- start-vlan: 0 — 4094
- end-vlan: 0 — 4094
VPLS SAP ATM Commands

atm

Syntax       atm
Context      config>service>vpls>sap
Description  This command enables access to the context to configure ATM-related attributes. This command can only be used when a given context (for example, a channel or SAP) supports ATM functionality such as:

- Configuring ATM port or ATM port-related functionality on MDAs supporting ATM functionality
- Configuring ATM-related configuration for ATM-based SAPs that exist on MDAs supporting ATM functionality.

If ATM functionality is not supported for a given context, the command returns an error.

egress

Syntax       egress
Context      config>service>vpls>sap>atm
Description  This command enables the context to configure egress ATM attributes for the SAP.

encapsulation

Syntax       encapsulation atm-encap-type
Context      config>service>vpls>sap>atm
Description  This command specifies the data encapsulation for an ATM PVCC delimited SAP. The definition references RFC 2684, Multiprotocol Encapsulation over ATM AAL5, and to the ATM Forum LAN Emulation specification.

Ingress traffic that does not match the configured encapsulation will be dropped.

Default     The encapsulation is driven by the services for which the SAP is configured. For IES and VPRN service SAPs, the default is aal5snap-routed.

Parameters  atm-encap-type — Specify the encapsulation type.

Values       aal5snap-routed — Routed encapsulation for LLC encapsulated circuit (LLC/ SNAP precedes protocol datagram) as defined in RFC 2684.
              aal5mux-ip — Routed IP encapsulation for VC multiplexed circuit as defined in RFC 2684.
ingress

**Syntax**

```plaintext
ingress
```

**Context**

```plaintext
config>service>vpls>sap>atm
```

**Description**

This command enables the context to configure ingress ATM attributes for the SAP.

traffic-desc

**Syntax**

```plaintext
traffic-desc traffic-desc-profile-id
no traffic-desc
```

**Context**

```plaintext
config>service>vpls>sap>atm>ingress
config>service>vpls>sap>atm>egress
```

**Description**

This command assigns an ATM traffic descriptor profile to a given context (for example, a SAP).

When configured under the ingress context, the specified traffic descriptor profile defines the traffic contract in the forward direction.

When configured under the egress context, the specified traffic descriptor profile defines the traffic contract in the backward direction.

The `no` form of the command reverts the traffic descriptor to the default traffic descriptor profile.

**Default**

The default traffic descriptor (trafficDescProfileId. = 1) is associated with newly created PVCC-delimited SAPs.

**Parameters**

```plaintext
traffic-desc-profile-id — Specify a defined traffic descriptor profile (see the QoS atm-td-profile command).
```

oam

**Syntax**

```plaintext
oam
```

**Context**

```plaintext
config>service>vpls>sap>atm
```

**Description**

This command enables the context to configure OAM functionality for a PVCC delimiting a SAP.

The ATM-capable MDAs support F5 end-to-end OAM functionality (AIS, RDI, Loopback):

- ITU-T Recommendation I.610 - B-ISDN Operation and Maintenance Principles and Functions version 11/95
- GR-1113-CORE - Bellcore, Asynchronous Transfer Mode (ATM) and ATM Adaptation Layer (AAL) Protocols Generic Requirements, Issue 1, July 1994
alarm-cells

**Syntax**

```
[no] alarm-cells
```

**Context**

```
config>service>vpls>sap>atm
```

**Description**

This command configures AIS/RDI fault management on a PVCC. Fault management allows PVCC termination to monitor and report the status of their connection by propagating fault information through the network and by driving PVCC’s operational status.

When alarm-cells functionality is enabled, a PVCC’s operational status is affected when a PVCC goes into an AIS or RDI state because of an AIS/RDI processing (assuming nothing else affects PVCC’s operational status, for example, if the PVCC goes DOWN, or enters a fault state and comes back UP, or exits that fault state). RDI cells are generated when PVCC is operationally DOWN. No OAM-specific SNMP trap is raised whenever an endpoint enters/exits an AIS or RDI state, however, if as result of an OAM state change, the PVCC changes operational status, then a trap is expected from an entity the PVCC is associated with (for example a SAP).

The **no** command disables alarm-cells functionality for a PVCC. When alarm-cells functionality is disabled, the PVCC’s operational status is no longer affected by the PVCC’s OAM state changes due to AIS/RDI processing. Note that when alarm-cells is disabled, a PVCC will change operational status to UP from DOWN due to alarm-cell processing. RDI cells are not generated as result of PVCC going into an AIS or RDI state, however, the PVCC’s OAM status will record OAM faults as described above.

**Default**

Enabled for PVCCs delimiting VPLS SAPs.
VPLS Filter and QoS Policy Commands

egress

**Syntax**

```
egress
```

**Context**

```
config>service>vpls>sap
```

**Description**

This command enables the context to configure egress filter policies.

If no sap-egress QoS policy is defined, the system default sap-egress QoS policy is used for egress processing. If no egress filter is defined, no filtering is performed.

ingress

**Syntax**

```
ingress
```

**Context**

```
config>service>vpls>sap
```

**Description**

This command enables the context to configure ingress SAP Quality of Service (QoS) policies and filter policies.

If no sap-ingress QoS policy is defined, the system default sap-ingress QoS policy is used for ingress processing. If no ingress filter is defined, no filtering is performed.

agg-rate

**Syntax**

```
[no] agg-rate
```

**Context**

```
config>service>vpls>sap>egress>
config>service>template>vpls-sap-template>egress
config>service>vpls>sap>egress>encap-defined-qos>encap-group
```

**Description**

This command is used to control an HQoS aggregate rate limit. It is used in conjunction with the following parameter commands: **rate**, **limit-unused-bandwidth**, and **queue-frame-based-accounting**.
rate

Syntax  
rate (max | rate)
no rate

Context  
config>service>vpls>sap>egress>agg-rate
config>service>template>vpls-sap-template>egress>agg-rate
config>service>vpls>sap>egress>encap-defined-qos>encap-group>agg-rate

Description  
This command defines the enforced aggregate rate for all queues associated with the agg-rate context. A rate must be specified for the agg-rate context to be considered to be active on the context’s object (SAP, subscriber, VPORT etc.).

limit-unused-bandwidth

Syntax  
[no] limit-unused-bandwidth

Context  
config>service>vpls>sap>egress>agg-rate
config>service>template>vpls-sap-template>egress>agg-rate
config>service>vpls>sap>egress>encap-defined-qos>encap-group>agg-rate

Description  
This command is used to enable (or disable) aggregate rate overrun protection on the agg-rate context.

queue-frame-based-accounting

Syntax  
[no] queue-frame-based-accounting

Context  
config>service>vpls>sap>egress>agg-rate
config>service>template>vpls-sap-template>egress>agg-rate

Description  
This command is used to enabled (or disable) frame based accounting on all queues associated with the agg-rate context. Only supported on Ethernet ports. Not supported on HSMDA Ethernet ports.

encap-defined-qos

Syntax  
encap-defined-qos

Context  
config>service>vpls>sap>egress

Description  
This command creates a new QoS sub-context in B-VPLS SAP egress context. The user can define encapsulation groups, referred to as encap-group, based on the ISID value in the packet’s encapsulation and assign a QoS policy and a scheduler policy or aggregate rate limit to the group.
encap-group

Syntax  
encap-group group-name [type group-type] [qos-per-member] [create]
no encap-group group-name

Context  
config>service>vpls>sap>egress>encap-defined-qos

Description  
This command defines an encapsulation group which consists of a group of ISID values. All packets forwarded on the egress of a B-VPLS SAP which payload header matches one of the ISID value in the encap-group will use the same QoS policy instance and scheduler policy or aggregate rate limit instance.

The user adds or removes members to the encap-group one at a time or as a range of contiguous values using the member command. However, when the qos-per-member option is enabled, members must be added or removed one at a time. These members are also referred to as ISID contexts.

The user can configure one or more encap-groups in the egress context of the same B-SAP, thus defining different ISID values and applying each a different SAP egress QoS policy, and optionally a different scheduler policy/agg-rate. Note that ISID values are unique within the context of a B-SAP. The same ISID value cannot be re-used in another encap-group under the same B-SAP but can be re-used in an encap-group under a different B-SAP. Finally, if the user adds to an encap-group an ISID value which is already a member of this encap-group, the command causes no effect. The same if the user attempts to remove an ISID value which is not a member of this encap-group.

Once a group is created, the user will assign a SAP egress QoS policy, and optionally a scheduler policy or aggregate rate limit, using the following commands:

config>service> vpls>sap>egress>encap-defined-qos>encap-group>qos sap-egress-policy-id
config>service> vpls>sap>egress>encap-defined-qos>encap-group>scheduler-policy scheduler-policy-name
config>service> vpls>sap>egress>encap-defined-qos>encap-group>agg-rate kilobits-per-second

Note that a SAP egress QoS policy must first be assigned to the created encap-group before the user can add members to this group. Conversely, the user cannot perform no qos command until all members are deleted from the encap-group.

An explicit or the default SAP egress QoS policy will continue to be applied to the entire B-SAP but this will serve to create the set of egress queues which will be used to store and forward a packet which does not match any of the defined ISID values in any of the encap-groups for this SAP.

Only the queue definition and fc-to-queue mapping from the encap-group SAP egress QoS policy is applied to the ISID members. All other parameters configurable in a SAP egress QoS policy must be inherited from egress QoS policy applied to the B-SAP.

Furthermore, any other CLI option configured in the egress context of the B-SAP will continue to apply to packets matching a member of any encap-group defined in this B-SAP.

The keyword qos-per-member allows the user to specify that a separate queue set instance and scheduler/agg-rate instance will be created for each ISID value in the encap-group. By default, shared instances will be created for the entire encap-group.

Note that when the B-SAP is configured on a LAG port, the ISID queue instances defined by all the encap-groups applied to the egress context of the SAP will be replicated on each member link of the LAG. The set of scheduler/agg-rate instances will be replicated per link or perXMA depending if the adapt-qos option is set to link mode or distribute mode. This is the same behavior as that applied to the entire B-SAP in the current implementation.
The **no** form of this command deletes the encap-group.

**Parameters**

- **group-name** — Specifies the name of the encap-group and can be up to 32 ASCII characters in length.
- **type** — This specifies the type of the encapsulation ID used by this encap-group.
  - **Values**
    - **isin**
  - **Default**
    - None
- **qos-per-member** — Specifies that a separate queue set instance and scheduler/agg-rate instance will be created for each ISID value in the encap-group.

**member**

**Syntax**

```
[no] member encap-id [to encap-id]
```

**Context**

```
config>service>vpls>sap>egress>encap-defined-qos>encap-group
```

**Description**

This command adds or removes a member ISID or a range of contiguous ISID members to an encap-group. The user can add or remove members to the encap-group one at a time or as a range of contiguous values using the member command. However, when the **qos-per-member** option is enabled, members must be added or removed one at a time.

The **no** form of this command removes the single or range of ISID values from the encap-group.

**Parameters**

- **encap-id** — The value of the single encap-id or the start encap-id of the range. ISID is the only encap-id supported.
- **to encap-id** — The value of the end encap-id of the range. ISID is the only encap-id supported.

**qos**

**Syntax**

```
qos policy-id
no qos
```

**Context**

```
config>service>vpls>sap>egress>encap-defined-qos>encap-group
```

**Description**

This command configures the QoS ID.

**scheduler-policy**

**Syntax**

```
scheduler-policy scheduler-policy-name
no scheduler-policy
```

**Context**

```
config>service>vpls>sap>egress>encap-defined-qos>encap-group
```

**Description**

This command configures the scheduler policy.
filter

Syntax

filter ip ip-filter-id
filter ipv6 ipv6-filter-id
filter mac mac-filter-id
no filter [ip ip-filter-id] [mac mac-filter-id] [ipv6 ipv6-filter-id]

Context

config>service>vpls>sap>egress
config>service>vpls>sap>ingress
config>service>vpls>mesh-sdp>egress
config>service>vpls>mesh-sdp>ingress
config>service>vpls>spoke-sdp>egress
config>service>vpls>spoke-sdp>ingress

Description

This command associates an IP filter policy or MAC filter policy with an ingress or egress Service Access Point (SAP) or IP interface.

Filter policies control the forwarding and dropping of packets based on IP or MAC matching criteria. There are two types of filter policies: IP and MAC. Only one type may be applied to a SAP at a time.

The filter command is used to associate a filter policy with a specified filter ID with an ingress or egress SAP. The filter ID must already be defined before the filter command is executed. If the filter policy does not exist, the operation will fail and an error message returned.

In general, filters applied to SAPs (ingress or egress) apply to all packets on the SAP. One exception is non-IP packets are not applied to IP match criteria, so the default action in the filter policy applies to these packets.

The no form of this command removes any configured filter ID association with the SAP or IP interface. The filter ID itself is not removed from the system unless the scope of the created filter is set to local. To avoid deletion of the filter ID and only break the association with the service object, use scope command within the filter definition to change the scope to local or global. The default scope of a filter is local.

Special Cases

VPLS — Both MAC and IP filters are supported on a VPLS service SAP.

Parameters

- ip ip-filter-id — Specifies IP filter policy. The filter ID must already exist within the created IP filters.
  - Values 1 — 65535
- ipv6 ipv6-filter-id — Specifies the IPv6 filter policy. The filter ID must already exist within the created IPv6 filters.
  - Values 1 — 65535
- mac mac-filter-id — Specifies the MAC filter policy. The specified filter ID must already exist within the created MAC filters. The filter policy must already exist within the created MAC filters.
  - Values 1 — 65535
hsmda-queue-override

Syntax  [no] hsmda-queue-override
Context  config>service>vpls>sap>egress
Description  This command enables the context to configure HSMDA queue overrides.

queue

Syntax  queue queue-id [create]
no queue queue-id
Context  config>service>vpls>sap>egress>hsmda-queue-override
Description  This command configures overrides for a HSMDA queue. The actual valid values are those defined in the given SAP QoS policy.
Parameters  queue-id — Specifies the queue ID to override.
            Values  1 — 8
            create — This keyword is mandatory while creating a new queue override.

packet-byte-offset

Syntax  packet-byte-offset {add add-bytes | subtract sub-bytes}
no packet-byte-offset
Context  config>service>vpls>sap>egress>hsmda-queue-override
Description  This command adds or subtracts the specified number of bytes to the accounting function for each packet handled by the HSMDA queue. Normally, the accounting and leaky bucket functions are based on the Ethernet DLC header, payload and the 4 byte CRC (everything except the preamble and inter-frame gap). As an example, the packet-byte-offset command can be used to add the frame encapsulation overhead (20 bytes) to the queues accounting functions.

The accounting functions affected include:

• Offered High Priority / In-Profile Octet Counter
• Offered Low Priority / Out-of-Profile Octet Counter
• Discarded High Priority / In-Profile Octet Counter
• Discarded Low Priority / Out-of-Profile Octet Counter
• Forwarded In-Profile Octet Counter
• Forwarded Out-of-Profile Octet Counter
• Peak Information Rate (PIR) Leaky Bucket Updates
• Committed Information Rate (CIR) Leaky Bucket Updates
• Queue Group Aggregate Rate Limit Leaky Bucket Updates
The secondary shaper leaky bucket, scheduler priority level leaky bucket and the port maximum rate updates are not affected by the configured packet-byte-offset. Each of these accounting functions are frame based and always include the preamble, DLC header, payload and the CRC regardless of the configured byte offset.

The packet-byte-offset command accepts either add or subtract as valid keywords which define whether bytes are being added or removed from each packet traversing the queue. Up to 31 bytes may be added to the packet and up to 32 bytes may be removed from the packet. An example use case for subtracting bytes from each packet is an IP-based accounting function. Given a Dot1Q encapsulation, the command packet-byte-offset subtract 14 would remove the DLC header and the Dot1Q header from the size of each packet for accounting functions only. The 14 bytes are not actually removed from the packet, only the accounting size of the packet is affected.

As inferred above, the variable accounting size offered by the packet-byte-offset command is targeted at the queue and queue group level. The packet-byte-offset, when set, applies to all queues in the queue group. The accounting size of the packet is ignored by the secondary shapers, the scheduling priority level shapers and the scheduler maximum rate. The actual on-the-wire frame size is used for these functions to allow an accurate representation of the behavior of the subscribers packets on an Ethernet aggregation network.

The packet-byte-offset value may be overridden at the queue-group level.

### Parameters

- **add add-bytes** — Indicates that the byte value should be added to the packet for queue and queue group level accounting functions. Either the `add` or `subtract` keyword must be specified. The corresponding byte value must be specified when executing the packet-byte-offset command. The `add` keyword is mutually exclusive with the `subtract` keyword.
  - **Values** 0 — 31

- **subtract sub-bytes** — Indicates that the byte value should be subtracted from the packet for queue and queue group level accounting functions. The `subtract` keyword is mutually exclusive with the `add` keyword. Either the `add` or `subtract` keyword must be specified. The corresponding byte value must be specified when executing the packet-byte-offset command.
  - **Values** 1 — 32

### slope-policy

**Syntax**

```plaintext
slope-policy hsmda-slope-policy-name
no slope-policy
```

**Context**

```
config>service>vpls>sap>egress>hsmda-queue-over>queue
```

**Description**

This command specifies an existing slope policy name.

### rate

**Syntax**

```plaintext
rate pir-rate
no rate
```

**Context**

```
config>service>vpls>sap>egress>hsmda-queue-over
```
ETH-CFM Service Commands

Description
This command specifies the administrative PIR by the user.

Parameters
pir-rate — Configures the administrative PIR specified by the user.

Values
1 — 40000000, max

wrr-weight

Syntax
wrr-weight value
no wrr-weight

Context
config>service>vpls>sap>egress>hsmda-queue-over>queue

Description
This command assigns the weight value to the HSMDA queue.

The no form of the command returns the weight value for the queue to the default value.

Parameters
percentage — Specifies the weight for the HSMDA queue.

Values
1— 32

wrr-policy

Syntax
wrr-policy hsmda-wrr-policy-name
no wrr-policy

Context
config>service>vpls>sap>egress>hsmda-queue-over

Description
This command associates an existing HSMDA weighted-round-robin (WRR) scheduling loop policy to the HSMDA queue.

Parameters
hsmda-wrr-policy-name — Specifies the existing HSMDA WRR policy name to associate to the queue.

secondary-shaper

Syntax
secondary-shaper secondary-shaper-name
no secondary-shaper

Context
config>service>vpls>sap>egress>hsmda-queue-over

Description
This command configures an HSMDA secondary shaper. Note that an shaper override can only be configured on an HSMDA SAP.

Parameters
secondary-shaper-name — Specifies a secondary shaper name up to 32 characters in length.
multicast-group

Syntax  multicast-group group-name
        no multicast-group

Context  config>service>vpls>sap>egress

Description  This command places a VPLS Ethernet SAP into an egress multicast group. The SAP must comply
              with the egress multicast group’s common requirements for member SAPs. If the SAP does not
              comply, the command will fail and the SAP will not be a member of the group. Common
              requirements for an egress multicast group are listed below:

              • If an egress-filter is specified on the egress multicast group, the SAP must have the same egress
                filter applied.
              • If an egress-filter is not defined on the egress multicast group, the SAP cannot have an egress fil-
                ter applied.
              • If the egress multicast group has an encap-type set to null, the SAP must be defined on a port
                with the port encapsulation type set to null.
              • If the egress multicast group has an encap-type set to dot1q, the SAP must be defined on a port
                with the port encapsulation type set to dot1q and the port’s dot1q-etype must match the dot1q-
                etype defined on the egress multicast group.
              • The access port the SAP is created on cannot currently be an egress mirror source.

Once a SAP is a member of an egress multicast group, the following rules apply:

• The egress filter defined on the SAP cannot be removed or modified. Egress filtering is managed
  at the egress multicast group for member SAPs.
• If the encapsulation type for the access port the SAP is created on is set to dot1q, the port’s
  dot1q-etype value cannot be changed.
• Attempting to define an access port with a SAP that is currently defined in an egress multicast
  group as an egress mirror source will fail.

Once a SAP is included in an egress multicast group, it is then eligible for efficient multicast
replication if the egress forwarding plane performing replication for the SAP is capable. If the SAP is
defined as a Link Aggregation Group (LAG) SAP, it is possible that some links in the LAG are on
forwarding planes that support efficient multicast replication while others are not. The fact that some
or all the forwarding planes associated with the SAP cannot perform efficient multicast replication
does not affect the ability to place the SAP into an Egress multicast group.

A SAP may be a member of one and only one egress multicast group. If the multicast-group
command is executed with another egress multicast group name, the system will attempt to move the
SAP to the specified group. If the SAP is not placed into the new group, the SAP will remain a
member of the previous egress multicast group. Moving a SAP into an egress multicast group may
cause a momentary gap in replications to the SAP destination while the move is being processed.

The no form of the command removes the SAP from any egress multicast group in which it may
currently have membership. The SAP will be removed from all efficient multicast replication chains
and normal replication will apply to the SAP. A momentary gap in replications to the SAP destination
while it is being moved is possible. If the SAP is not currently a member in an egress multicast group,
the command has no effect.

Default  no multicast-group
Parameters

*group-name* — The *group-name* is required when specifying egress multicast group membership on a SAP. An egress multicast group with the specified egress-multicast-group-name must exist and the SAP must pass all common requirements or the command will fail.

**Values** Any valid egress multicast group name.

**Default** None, an egress multicast group name must be explicitly specified.

qinq-mark-top-only

**Syntax**

```plaintext
[no] qinq-mark-top-only
```

**Context**

`config>service>vpls>sap>egress`

**Description**

When enabled (the encapsulation type of the access port where this SAP is defined as qinq), the `qinq-mark-top-only` command specifies which P-bits/DEI bit to mark during packet egress. When disabled, both set of P-bits/DEI bit are marked. When enabled, only the P-bits/DEI bit in the top Q-tag are marked.

The **no** form of this command disables the command.

**Default**

`no qinq-mark-top-only`

policer-control-override

**Syntax**

```plaintext
policer-control-override [create]
no policer-control-override
```

**Context**

`config>service>vpls>sap>egress`
`config>service>vpls>sap>ingress`

**Description**

This command, within the SAP ingress or egress contexts, creates a CLI node for specific overrides to the applied policer-control-policy. A policy must be applied for a policer-control-overrides node to be created. If the policer-control-policy is removed or changed, the policer-control-overrides node is automatically deleted from the SAP.

The **no** form of the command removes any existing policer-control-policy overrides and the policer-control-overrides node from the SAP.

**Default**

`no policer-control-override`

**Parameters**

*create* — The create keyword is required when the policer-control-overrides node is being created and the system is configured to expect explicit confirmation that a new object is being created. When the system is not configured to expect explicit confirmation, the create keyword is not required.

max-rate

**Syntax**

```plaintext
max-rate {rate | max}
```

**Context**

`config>service>vpls>sap>egress`
config>service>vpls>sap>ingress

**Description**
This command, within the SAP ingress and egress contexts, overrides the root arbiter parent policer max-rate that is defined within the policer-control-policy applied to the SAP.

When the override is defined, modifications to the policer-control-policy max-rate parameter have no effect on the SAP’s parent policer until the override is removed using the `no max-rate` command within the SAP.

**Parameters**
`rate | max` — Specifies the max rate override in kilobits-per-second or use the maximum.

<table>
<thead>
<tr>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 — 20000000 Kbps, max</td>
</tr>
</tbody>
</table>

**priority-mbs-thresholds**

**Syntax**
`priority-mbs-thresholds`

**Context**
`config>service>vpls>sap>egress`

**Description**
This command overrides the CLI node contains the configured min-thresh-separation and the various priority level mbs-contribution override commands.

**min-thresh-separation**

**Syntax**
`min-thresh-separation size [bytes | kilobytes]`

**Context**
`config>service>vpls>sap>egress`
`config>service>vpls>sap>ingress`

**Description**
This command within the SAP ingress and egress contexts is used to override the root arbiter’s parent policer min-thresh-separation parameter that is defined within the policer-control-policy applied to the SAP.

When the override is defined, modifications to the policer-control-policy min-thresh-separation parameter have no effect on the SAP’s parent policer until the override is removed using the `no min-thresh-separation` command within the SAP.

The no form of the command removes the override and allows the min-thresh-separation setting from the policer-control-policy to control the root arbiter’s parent policer’s minimum discard threshold separation size.

**Default**
`no min-thresh-separation`

**Parameters**
`bytes` — Signifies that size is expressed in bytes. The bytes and kilobytes keywords are mutually exclusive and are optionally used to qualify whether size is expressed in bytes or kilobytes. The default is kilobytes.

`kilobytes` — The size parameter is required when specifying the min-thresh-separation override. It is specified as an integer representing either a number of bytes or kilobytes that are the minimum separation between the parent policer’s priority level discard thresholds.

<table>
<thead>
<tr>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 — 16777216</td>
</tr>
</tbody>
</table>

**Default**
kilobytes
priority

Syntax  [no] priority level

Context  config>service>vpls>sap>egress
         config>service>vpls>sap>ingress

Description  The priority-level level override CLI node contains the specified priority level’s mbs-contribution override value.

This node does not need to be created and will not be output in show or save configurations unless an mbs-contribution override exist for level.

Parameters  level — The level parameter is required when specifying priority-level and identifies which of the parent policer instances priority level’s the mbs-contribution is overriding.

Values  1 — 8

mbs-contribution

Syntax  mbs-contribution size [bytes | kilobytes]

Context  config>service>vpls>sap>egress
         config>service>vpls>sap>ingress

Description  The mbs-contribution override command within the SAP ingress and egress contexts is used to override a parent policer’s priority level’s mbs-contribution parameter that is defined within the policer-control-policy applied to the SAP. This override allow the priority level’s burst tolerance to be tuned based on the needs of the SAP’s child policers attached to the priority level.

When the override is defined, modifications to the policer-control-policy priority level’s mbs-contribution parameter have no effect on the SAP’s parent policer priority level until the override is removed using the no mbs-contribution command within the SAP.

The no form of the command removes the override and allows the mbs-contribution setting from the policer-control-policy to control the parent policer’s priority level’s burst tolerance.

Default  no mbs-contribution

Parameters  bytes — This keyword signifies that size is expressed in bytes.

kilobytes — The optional kilobytes keyword signifies that size is expressed in kilobytes.

Values  0 – 16777216 or default

policer-control-policy

Syntax  policer-control-policy policy-name [create]
        no policer-control-policy

Context  config>service>vpls>sap>egress
         config>service>vpls>sap>ingress
Description

This command, within the qos CLI node, is used to create, delete or modify policer control policies. A policer control policy is very similar to the scheduler-policy which is used to manage a set of queues by defining a hierarchy of virtual schedulers and specifying how the virtual schedulers interact to provide an aggregate SLA. In a similar fashion, the policer-control-policy controls the aggregate bandwidth available to a set of child policers. Once created, the policy can be applied to ingress or egress SAPs. The policy may also be applied to the ingress or egress context of a sub-profile.

Policer Control Policy Instances

On the SAP side, an instance of a policy is created each time a policy is applied. When applied to a sub-profile, an instance of the policy is created each time a subscriber successfully maps one or more hosts to the profile per ingress SAP.

Each instance of the policer-control-policy manages the policers associated with the object that owns the policy instance (SAP or subscriber). If a policer on the object is parented to an appropriate arbiter name that exists within the policy, the policer will be managed by the instance. If a policer is not parented or is parented to a non-existent arbiter, the policer will be orphaned and will not be subject to bandwidth control by the policy instance.

Maximum Rate and Root Arbiter

The policer-control-policy supports an overall maximum rate (max-rate) that defines the total amount of bandwidth that may be distributed to all associated child policers. By default, that rate is set to max which provides an unlimited amount of bandwidth to the policers. Once the policy is created, an actual rate should be configured in order for the policy instances to be effective. At the SAP level, the maximum rate may be overridden on a per instance basis. For subscribers, the maximum rate may only be overridden on the subscriber profile which will then be applied to all instances associated with the profile.

The maximum rate is defined within the context of the root arbiter which is always present in a policer-control-policy. The system creates a parent policer which polices the output of all child policers attached to the policy instance to the configured rate. Child policers may be parented directly to the root arbiter (parent root) or parented to one of the tiered arbiters (parent arbiter-name). Since each tiered arbiter must be parented to either another tiered arbiter or the root arbiter (default), every parented child policer is associated with the root arbiter and thus the root arbiter’s parent policer.

Parent Policer PIR Leaky Bucket Operation

The parent policer is a single leaky bucket that monitors the aggregate throughput rate of the associated child policers. Forwarded packets increment the bucket by the size of each packet. The rate of the parent policer is implemented as a bucket decrement function which attempts to drain the bucket. If the rate of the packets flowing through the bucket is less than the decrement rate, the bucket does not accumulate depth. Each packet that flows through the bucket is accompanied by a derived discard threshold. If the current depth of the bucket is less than the discard threshold, the packet is allowed to pass through, retaining the colors derived from the packet’s child policer. If the current depth is equal to or greater than the threshold value, the packet is colored red and the bucket depth is not incremented by the packet size. Also, any increased bucket depths in the child policer are canceled making any discard event an atomic function between the child and the parent.

Due to the fact that multiple thresholds are supported by the parent policer, the policer control policy is able to protect the throughput of higher priority child policers from the throughput of the lower priority child policers within the aggregate rate.

Tier 1 and Tier 2 Arbiters

As stated above, each child is attached either to the always available root arbiter or to an explicitly created tier 1 or tier 2 arbiter. Unlike the hardware parent policer based root arbiter, the arbiters at tier
1 and tier 2 are only represented in software and are meant to provide an arbitrary hierarchical bandwidth distribution capability. An arbiter created on tier 2 must parent to either an arbiter on tier 1 or to the root arbiter. Arbiters created on tier 1 always parent to the root arbiter. In this manner, every arbiter ultimately is parented or grand-parented by the root arbiter.

Each tiered arbiter supports an optional rate parameter that defines a rate limit for all child arbiters or child policers associated with the arbiter. Child arbiters and policers attached to the arbiter have a level attribute that defines the strict level at which the child is given bandwidth by the arbiter. Level 8 is the highest and 1 is the lowest. Also a weight attribute defines each child’s weight at that strict level in order to determine how bandwidth is distributed to multiple children at that level when insufficient bandwidth is available to meet each child’s required bandwidth.

Fair and Unfair Bandwidth Control

Each child policer supports three leaky buckets. The PIR bucket manages the policer’s peak rate and maximum burst size, the CIR leaky bucket manages the policer’s committed rate (in-profile / out-of-profile) and committed burst size. The third leaky bucket is used by the policer control policy instance to manage the child policer’s fair rate (FIR). When multiple child policers are attached to the root arbiter at the same priority level, the policy instance uses each child’s FIR bucket rate to control how much of the traffic forwarded by the policer is fair and how much is unfair.

In the simplest case where all the child policers in the same priority level are directly attached to the root arbiter, each child’s FIR rate is set according to the child’s weight divided by the sum of the active children’s weights multiplied by the available bandwidth at the priority level. The result is that the FIR bucket will mark the appropriate amount of traffic for each child as fair based on the weighted fair output of the policy instance.

The fair/unfair forwarding control in the root parent policer is accomplished by implementing two different discard thresholds for the priority. The first threshold is discard-unfair and the second is discard-all for packet associated with the priority level. As the parent policer PIR bucket fills (due the aggregate forwarded rate being greater than the parent policers PIR decrement rate) and the bucket depth reaches the first threshold, all unfair packets within the priority are discarded. This leaves room in the bucket for the fair packets to be forwarded.

In the more complex case where one or more tiered arbiters are attached at the priority level, the policer control policy instance must consider more than just the child policer weights associated with the attached arbiter. If the arbiter is configured with an aggregate rate limit that its children cannot exceed, the policer control policy instance will switch to calculating the rate each child serviced by the arbiter should receive and enforces that rate using each child policers PIR leaky bucket.

When the child policer PIR leaky bucket is used to limit the bandwidth for the child policer and the child’s PIR bucket discard threshold is reached, packets associated with the child policer are discarded. The child policer’s discarded packets do not consume depth in the child policer’s CIR or FIR buckets. The child policers discarded packets are also prevented from impacting the parent policer and will not consume the aggregate bandwidth managed by the parent policer.

Parent Policier Priority Level Thresholds

As stated above, each child policer is attached either to the root arbiter or explicitly to one of the tier 1 or tier 2 arbiters. When attached directly to the root arbiter, its priority relative to all other child policers is indicated by the parenting level parameter. When attached through one of the tiered arbiters, the parenting hierarchy of the arbiters must be traced through to the ultimate attachment to the root arbiter. The parenting level parameter of the arbiter parented to the root arbiter defines the child policer’s priority level within the parent policer.

The priority level is important since it defines the parent policer discard thresholds that will be applied at the parent policer. The parent policer has 8 levels of strict priority and each priority level
has its own discard-unfair and discard-all thresholds. Each priority’s thresholds are larger than the thresholds of the lower priority levels. This ensures that when the parent policer is discarding, it will be priority sensitive.

To visualize the behavior of the parent policer, picture that when the aggregate forwarding rate of all child policers is currently above the decrement rate of the parent PIR leaky bucket, the bucket depth will increase over time. As the bucket depth increases, it will eventually cross the lowest priority’s discard-unfair threshold. If this amount of discard sufficiently lowers the remaining aggregate child policer rate, the parent PIR bucket will hover around this bucket depth. If however, the remaining aggregate child rate is still greater than the decrement rate, the bucket will continue to rise and eventually reach the lowest priority’s discard-all threshold which will cause all packets associated with the priority level to be discarded (fair and unfair). Again, if the remaining aggregate child rate is less than or equal to the bucket decrement rate, the parent PIR bucket will hover around this higher bucket depth. If the remaining aggregate child rate is still higher than the decrement rate, the bucket will continue to rise through the remaining priority level discards until equilibrium is achieved.

As noted above, each child’s rate feeding into the parent policer is governed by the child policer’s PIR bucket decrement rate. The amount of bandwidth the child policer offers to the parent policer will not exceed the child policer’s configured maximum rate.

**Root Arbiter’s Parent Policer’s Priority Aggregate Thresholds**

Each policer-control-policy root arbiter supports configurable aggregate priority thresholds which are used to control burst tolerance within each priority level. Two values are maintained per priority level; the shared-portion and the fair-portion. The shared-portion represents the amount of parent PIR bucket depth that is allowed to be consumed by both fair and unfair child packets at the priority level. The fair-portion represents the amount of parent PIR bucket depth that only the fair child policer packets may consume within the priority level. It should be noted that the fair and unfair child packets associated with a higher parent policer priority level may also consume the bucket depth set aside for this priority.

While the policy maintains a parent policer default or explicit configurable values for shared-portion and fair-portion within each priority level, it is possible that some priority levels will not be used within the parent policer. Most parent policer use cases require fewer than eight strict priority levels.

In order to derive the actual priority level discard-unfair and discard-all thresholds while only accounting for the actual in-use priority levels, the system maintains a child policer to parent policer association counter per priority level for each policer control policy instance. As a child policer is parented to either the root or a tiered arbiter, the system determines the parent policer priority level for the child policer and increments the association counter for that priority level on the parent policer instance.

The shared-portion for each priority level is affected by the parent policer global min-thresh-separation parameter that defines the minimum separation between any in-use discard thresholds. When more than one child policer is associated with a parent policer priority level, the shared-portion for that priority level will be the current value of min-thresh-separation. When only a single child policer is associated, the priority level’s shared-portion is zero since all packets from the child will be marked fair and the discard-unfair threshold is meaningless. When the association counter is zero, both the shared-portion and the fair-portion for that priority level are zero since neither discard thresholds will be used. Whenever the association counter is greater than 0, the fair-portion for that priority level will be derived from the current value of the priority’s mbs-contribution parameter and the global min-thresh-separation parameter.

Each priority level’s discard-unfair and discard-all thresholds are calculated based on an accumulation of lower priorities shared-portions and fair-portions and the priority level’s own shared-
portion and fair-portion. The base threshold value for each priority level is equal to the sum of all lower priority level’s shared-portions and fair-portions. The discard-unfair threshold is the priority level’s base threshold plus the priority level’s shared-portion. The discard-all threshold for the priority level is the priority level’s base threshold plus both the shared-portion and fair-portion values of the priority. As can be seen, an in-use priority level’s thresholds are always greater than the thresholds of lower priority levels.

Policer Control Policy Application

A policer-control-policy may be applied on any Ethernet ingress or egress SAP that is associated with a port (or ports in the case of LAG).

The no form of the command removes a non-associated policer control policy from the system. The command will not execute when policer-name is currently associated with any SAP or subscriber management sub-profile context.

Default

none

Parameters

policy-name — Each policer-control-policy must be created with a unique policy name. The name must given as policy-name must adhere to the system policy ASCII naming requirements. If the defined policy-name already exists, the system will enter that policy’s context for editing purposes. If policy-name does not exist, the system will attempt to create a policy with the specified name. Creating a policy may require use of the create parameter when the system is configured for explicit object creation mode.

create — The keyword is required when a new policy is being created and the system is configured for explicit object creation mode.

policer-override

Syntax  [no] policer-override

Context config>service>vpls>sap>egress
       config>service>vpls>sap>ingress

Description This command, within the SAP ingress or egress contexts, is used to create a CLI node for specific overrides to one or more policers created on the SAP through the sap-ingress or sap-egress QoS policies.

The no form of the command is used to remove any existing policer overrides.

Default no policer-overrides

policer

Syntax  policer policer-id [create]
        no policer policer-id

Context config>service>vpls>sap>egress>policer-override
       config>service>vpls>sap>ingress>policer-override

Description This command, within the SAP ingress or egress contexts, is used to create a CLI node for specific overrides to a specific policer created on the SAP through a sap-ingress or sap-egress QoS policy.
The **no** form of the command is used to remove any existing overrides for the specified policer-id.

**Parameters**

- **policer-id** — The policer-id parameter is required when executing the policer command within the policer-overrides context. The specified policer-id must exist within the sap-ingress or sap-egress QoS policy applied to the SAP. If the policer is not currently used by any forwarding class or forwarding type mappings, the policer will not actually exist on the SAP. This does not preclude creating an override context for the policer-id.

- **create** — The create keyword is required when a policer policer-id override node is being created and the system is configured to expect explicit confirmation that a new object is being created. When the system is not configured to expect explicit confirmation, the create keyword is not required.

---

**cbs**

**Syntax**

```
cbs size [bytes | kilobytes]
no cbs
```

**Context**

```
config>service>vpls>sap>egress>policer-override
config>service>vpls>sap>ingress>policer-override
```

**Description**

This command, within the SAP ingress and egress policer-overrides contexts, is used to override the sap-ingress and sap-egress QoS policy configured CBS parameter for the specified policer-id. The **no** form of this command returns the CBS size to the default value.

**Default**

no cbs

**Parameters**

- **size** — This parameter is required when specifying mbs override and is expressed as an integer representing the required size in either bytes or kilobytes. The default is kilobytes. The optional `byte` and `kilobyte` keywords are mutually exclusive and are used to explicitly define whether size represents bytes or kilobytes.

  **Values**

  - `0` — 16777216 or default

---

**mbs**

**Syntax**

```
mbs size [bytes | kilobytes]
no mbs
```

**Context**

```
config>service>vpls>sap>egress>policer-override>policer
config>service>vpls>sap>ingress>policer-override>policer
```

**Description**

This command, within the SAP ingress and egress policer-overrides contexts, is used to override the sap-ingress and sap-egress QoS policy configured mbs parameter for the specified policer-id. The **no** form of the command is used to restore the policer? mbs setting to the policy defined value.

**Default**

no mbs

**Parameters**

- **size** — The size parameter is required when specifying mbs override and is expressed as an integer representing the required size in either bytes or kilobytes. The default is kilobytes. The optional
byte and kilobyte keywords are mutually exclusive and are used to explicitly define whether size represents bytes or kilobytes.

Values 0 – 16777216

byte — When byte is defined, the value given for size is interpreted as the queue? MBS value given in bytes. When kilobytes is defined, the value is interpreted as the queue? MBS value given in kilobytes.

packet-byte-offset

Syntax packet-byte-offset {add add-bytes | subtract sub-bytes}

Context config>service>vpls>sap>egress>policer-override>policer
         config>service>vpls>sap>ingress>policer-override>policer

Description This command, within the SAP ingress and egress policer-overrides contexts, is used to override the sap-ingress and sap-egress QoS policy configured packet-byte-offset parameter for the specified policer-id.

The no packet-byte-offset command is used to restore the policer? packet-byte-offset setting to the policy defined value.

Default no packet-byte-offset

Parameters add add-bytes — The add keyword is mutually exclusive to the subtract keyword. Either add or subtract must be specified. When add is defined the corresponding bytes parameter specifies the number of bytes that is added to the size each packet associated with the policer for rate metering, profiling and accounting purposes. From the policer’s perspective, the maximum packet size is increased by the amount being added to the size of each packet.

Values 1 — 32

subtract sub-bytes — The subtract keyword is mutually exclusive to the add keyword. Either add or subtract must be specified. When subtract is defined the corresponding bytes parameter specifies the number of bytes that is subtracted from the size of each packet associated with the policer for rate metering, profiling and accounting purposes. From the policer’s perspective, the maximum packet size is reduced by the amount being subtracted from the size of each packet.

Values 1 — 32

rate

Syntax rate {rate | max} [cir {max | rate}]

Context config>service>vpls>sap>egress>policer-override>policer
         config>service>vpls>sap>ingress>policer-override>policer

Description This command within the SAP ingress and egress policer-overrides contexts is used to override the sap-ingress and sap-egress QoS policy configured rate parameters for the specified policer-id.

The no rate command is used to restore the policy defined metering and profiling rate to a policer.
Virtual Private LAN Services

Parameters

{rate | max} — Specifying the keyword max or an explicit kilobits-per-second parameter directly following the rate override command is required and identifies the policer instance? metering rate for the PIR leaky bucket. The kilobits-per-second value must be expressed as an integer and defines the rate in Kilobits-per-second. The integer value is multiplied by 1,000 to derive the actual rate in bits-per-second. When max is specified, the maximum policer rate used will be equal to the maximum capacity of the card on which the policer is configured. If the policer rate is set to a value larger than the maximum rate possible for the card, then the PIR used is equivalent to max.

Values

1 — 2000000000, max

cir {max | rate} — The optional cir keyword is used to override the policy derived profiling rate of the policer. Specifying the keyword max or an explicit kilobits-per-second parameter directly following the cir keyword is required. The kilobits-per-second value must be expressed as an integer and defines the rate in Kilobits-per-second. The integer value is multiplied by 1,000 to derive the actual rate in bits-per-second. When max is specified, the maximum policer rate used will be equal to the maximum capacity of the card on which the policer is configured. If the policer rate is set to a value larger than the maximum rate possible for the card, then the CIR used is equivalent to max.

Values

0 — 2000000000, max

stat-mode

Syntax

stat-mode stat-mode
no stat-mode

Context

config>service>vpls>sap>egress>policer-override>policer
config>service>vpls>sap>ingress>policer-override>policer

Description

The sap-egress QoS policy’s policer stat-mode command is used to configure the forwarding plane counters that allow offered, output and discard accounting to occur for the policer. An egress policer has multiple types of offered packets (soft in-profile and out-of-profile from ingress and hard in-profile and out-of-profile due to egress profile overrides) and each of these offered types is interacting with the policers metering and profiling functions resulting in colored output packets (green, yellow and red). Due to the potential large number of egress policers, it is not economical to allocate counters in the forwarding plane for all possible offered packet types and output conditions. Many policers will not be configured with a CIR profiling rate and not all policers will receive explicitly re-profiled offered packets. The stat-mode command allows provisioning of the number of counters each policer requires and how the offered packet types and output conditions should be mapped to the counters.

While a no-stats mode is supported which prevents any packet accounting, the use of the policer’s parent command requires at the policer’s stat-mode to be set at least to the minimal setting so that offered stats are available for the policer’s Fair Information Rate (FIR) to be calculated. Once a policer has been made a child to a parent policer, the stat-mode cannot be changed to no-stats unless the policer parenting is first removed.

Each time the policer’s stat-mode is changed, any previous counter values are lost and any new counters are set to zero.

Each mode uses a certain number of counters per policer instance that are allocated from the forwarding plane’s policer counter resources. If insufficient counters exist to implement a mode on
any policer instance, the stat-mode change will fail and the previous mode will continue unaffected for all instances of the policer.

The default stat-mode when a policer is created within the policy is no-stats.

The stat-mode setting defined for the policer in the QoS policy may be overridden on an sla-profile or SAP where the policy is applied. If insufficient policer counter resources exist to implement the override, the stat-mode override command will fail. The previous stat-mode setting active for the policer will continue to be used by the policer.

The no stat-mode command attempts to return the policer’s stat-mode setting to no-stats. The command will fail if the policer is currently configured as a child policer using the policer’s parent command. The no parent command must first be executed for the no stat-mode command to succeed.

**Parameters**

*stat-mode* — Specifies the mode of statistics collected by this policer.

**Values**

<table>
<thead>
<tr>
<th>no-stats, minimal, offered-profile-no-cir, offered-profile-cir, offered-total-cir</th>
</tr>
</thead>
</table>

**no-stats** — Counter resource allocation: 0

The no-stats mode is the default stat-mode for the policer. The policer does not have any forwarding plane counters allocated and cannot provide offered, discard and forward statistics. A policer using no-stats cannot be a child to a parent policer and the policers parent command will fail.

When collect-stats is enabled, the lack of counters causes the system to generate the following statistics:

a. offered-in = 0
b. offered-out = 0
c. discard-in = 0
d. discard-out = 0
e. forward-in = 0
f. forward-out = 0

Counter 0 indicates that the accounting statistic returns a value of zero.

**minimal** — Counter resource allocation: 1

The minimal mode allocates 1 forwarding plane offered counter and one traffic manager discard counter. The forwarding counter is derived by subtracting the discard counter from the offered counter. The counters do not differentiate possible offered types (soft or hard profile) and do not count green or yellow output. This does not prevent the policer from supporting different offered packet types and does not prevent the policer from supporting a CIR rate.

This counter mode is useful when only the most basic accounting information is required.

The counters are used in the following manner:

1. offered <= soft-in-profile-out-of-profile, profile in/out
2. discarded <= Same as 1
3. forwarded <= Derived from 1 – 2

When collect-stats is enabled, the counters are used by the system to generate the following statistics:

a. offered-in = 1
b. offered-out = 0
c. discard-in = 2
Virtual Private LAN Services

d. discard-out = 0
e. forward-in = 3
f. forward-out = 0

Counter 0 indicates that the accounting statistic returns a value of zero.

offered-profile-no-cir — Counter resource allocation: 2
The offered-profile-no-cir mode allocates two forwarding plane offered counters and two traffic manager discard counters.
The offered-profile-no-cir mode is most useful when profile based offered, discard and forwarding stats are required from the ingress policer, but a CIR is not being used to recolor the soft in-profile and out-of-profile packets. This mode does not prevent the policer from being configured with a CIR rate.
The counters are used in the following manner:

1. offered-in <= soft-in-profile, profile in
2. offered-out <= soft-out-of-profile, profile out
3. dropped-in <= Same as 1
4. dropped-out <= Same as 2
5. forwarded-in <= Derived from 1 – 3
6. forwarded-out <= Derived from 2 – 4

When collect-stats is enabled, the counters are used by the system to generate the following statistics:

a. offered-in = 1
b. offered-out = 2
c. discard-in = 3
d. discard-out = 4
e. forward-in = 5
f. forward-out = 6

offered-profile-cir — Counter resource allocation: 3
The offered-profile-cir mode allocates three forwarding plane offered counters and three traffic manager discard counters.
The offered-profile-cir mode is most useful when profile based offered, discard and forwarding stats are required from the ingress policer and a CIR rate is being used to recolor the soft in-profile and out-of-profile packets.
The counters are used in the following manner:

1. offered-in-that-stayed-green-or-turned-red <= profile in
2. offered-soft-that-turned-green <= soft-in-profile-out-of-profile
3. offered-soft-or-out-that-turned-yellow-or-red <= soft-in-profile-out-of-profile, profile out
4. dropped-in-that-stayed-green-or-turned-red <= Same as 1
5. dropped-soft-that-turned-green <= Same as 2
6. dropped-soft-or-out-that-turned-yellow-or-red <= Same as 3
7. forwarded-in-that-stayed-green <= Derived from 1 – 4
8. forwarded-soft-that-turned-green <= Derived from 2 – 5
When collect-stats is enabled, the counters are used by the system to generate the following statistics:

a. offered-in = 1
b. offered-out = 2 + 3
c. discard-in = 4
d. discard-out = 5 + 6
e. forward-in = 7 + 8
f. forward-out = 9

**offered-total-cir** — Counter resource allocation: 2

The offered-total-cir mode allocates two forwarding plane offered counters and two traffic manager discard counters.

The offered-total-cir mode is most useful when profile based offered stats are not required from the ingress policer and a CIR rate is being used to recolor the soft in-profile and out-of-profile packets.

The counters are used in the following manner:

1. offered-that-turned-green <= soft-in-profile-out-of-profile, profile in/out
2. offered-that-turned-yellow-or-red <= soft-in-profile-out-of-profile, profile in/out
3. dropped-offered-that-turned-green <= Same as 1
4. dropped-offered-that-turned-yellow-or-red <= Same as 2
5. forwarded-offered-that-turned-green <= Derived from 1 – 3
6. forwarded-offered-that-turned-yellow <= Derived from 2 – 4

When collect-stats is enabled, the counters are used by the system to generate the following statistics:

a. offered-in = 1 + 2 (Or 1 and 2 could be summed on b)
b. offered-out = 0
c. discard-in = 3
d. discard-out = 4
e. forward-in = 5
f. forward-out = 6

Counter 0 indicates that the accounting statistic returns a value of zero.

**QOS**

**Syntax**

```
qos policy-id [shared-queuing | multipoint-shared] [fp-redirect-group queue-group-name instance instance-id]
no qos
```

**Context**

```
config>service>vpls>sap>ingress
```

Page 844
**Description**

This command associates a Quality of Service (QoS) policy with an ingress Service Access Point (SAP).

QoS ingress and egress policies are important for the enforcement of SLA agreements. The policy ID must be defined prior to associating the policy with a SAP or IP interface. If the policy-id does not exist, an error will be returned.

The qos command is used to associate both ingress and egress QoS policies. The qos command only allows ingress policies to be associated on SAP ingress and egress policies on SAP egress. Attempts to associate a QoS policy of the wrong type returns an error.

Only one ingress and one egress QoS policy can be associated with a SAP at one time. Attempts to associate a second QoS policy of a given type will return an error.

When an ingress QoS policy is defined on IES ingress IP interface that is bound to a VPLS, the policy becomes associated with every SAP on the VPLS and augments the QoS policy that is defined on each SAP. Packets that are bridged will be processed using the policy defined on the VPLS SAP; packets that are routed will be processed using the policy defined in the IES IP interface-binding context.

By default, if no specific QoS policy is associated with the SAP for ingress or egress, the default QoS policy is used.

The no form of this command removes the QoS policy association from the SAP, and the QoS policy reverts to the default.

**Default**

none

**Parameters**

**policy-id** — The ingress policy ID to associate with SAP or IP interface on ingress. The policy ID must already exist.

  **Values**

  1 — 65535

**shared-queuing** — This keyword can only be specified on SAP ingress. Specify the ingress shared queue policy used by this SAP. When the value of this object is null, the SAP will use individual ingress QoS queues, instead of the shared ones.

**multipoint-shared** — This keyword can only be specified on SAP ingress. Multipoint shared queuing is a superset of shared queuing. When multipoint shared queuing keyword is set, in addition to the unicast packets, multipoint packets also used shared queues.

Ingress unicast service queues are mapped one-for-one with hardware queues and unicast packets traverse the ingress forwarding plane twice, similar to the shared-queuing option. In addition, the multipoint queues defined in the ingress SAP QoS policy are not created. Instead, multipoint packets (broadcast, multicast and unknown unicast destined) are treated to the same dual pass ingress forwarding plane processing as unicast packets.

When the value of this object is null, the SAP will use individual ingress QoS queues, instead of the shared ones.

When the value of this object is null, the SAP will use individual ingress QoS queues, instead of the shared ones.

  **Values**

  Multipoint or not present.

  **Default**

  Present (the queue is created as non-multipoint).

**fp-redirect-group** — This keyword creates an instance of a named queue group template on the ingress forwarding plane of a given IOM/IMM/XMA. The queue-group-name and instance
instance-id are mandatory parameters when executing the command. The named queue group template can contain only policers. If it contains queues, then the command will fail.

queue-group-name — Specifies the name of the queue group template to be instantiated on the forwarding plane of the IOM/IMM/XMA, up to 32 characters in length. The queue-group-name must correspond to a valid ingress queue group template name, configured under config>qos>queue-group-templates.

instance-id — Specifies the instance of the named queue group to be created on the IOM/IMM/XMA ingress forwarding plane.

QoS

Syntax

```
qos policy-id [port-redirect-group queue-group-name instance instance-id]
```

no qos

Context

config>service>vpls>sap>egress

Description

This command associates a Quality of Service (QoS) policy with an egress Service Access Point (SAP).

QoS ingress and egress policies are important for the enforcement of SLA agreements. The policy ID must be defined prior to associating the policy with a SAP. If the policy-id does not exist, an error will be returned.

The qos command is used to associate both ingress and egress QoS policies. The qos command only allows ingress policies to be associated on SAP ingress and egress policies on SAP egress. Attempts to associate a QoS policy of the wrong type returns an error.

Only one ingress and one egress QoS policy can be associated with a SAP at one time. Attempts to associate a second QoS policy of a given type will return an error.

When an egress QoS policy is associated with an IES IP interface that has been bound to a VPLS, the policy becomes associated with every SAP on the VPLS and augments the egress QoS policy that is defined on each SAP. Packets that are bridged will be processed using the policy defined on the VPLS SAP; packets that are routed will be processed using the policy defined in the IES IP interface-binding context.

By default, if no specific QoS policy is associated with the SAP for ingress or egress, so the default QoS policy is used.

The no form of this command removes the QoS policy association from the SAP, and the QoS policy reverts to the default.

Default

none

Parameters

port-redirect-group — This keyword associates a SAP egress with an instance of a named queue group template on the egress port of a given IOM/IMM/XMA. The queue-group-name and instance instance-id are mandatory parameters when executing the command.

queue-group-name — Specifies the name of the egress port queue group of the IOM/IMM/XMA, up to 32 characters in length. The queue-group-name must correspond to a valid egress queue group, created under config>port>ethernet>access>egress.

instance instance-id — Specifies the instance of the named egress port queue group on the IOM/IMM/XMA.
queue-override

Syntax  
[no] queue-override

Context  
config>service>vpls>sap>egress
config>service>vpls>sap>ingress
config>service>vpls>sap>egress>hsmda-queue-over>queue
config>service>vpls>sap>ingress>hsmda-queue-over>queue

Description  
This command enables the context to configure override values for the specified SAP egress or ingress QoS queue. These values override the corresponding ones specified in the associated SAP egress or ingress QoS policy.

queue

Syntax  
[no] queue queue-id

Context  
config>service>vpls>sap>egress>queue-override
config>service>vpls>sap>ingress>queue-override

Description  
This command specifies the ID of the queue whose parameters are to be overridden.

Parameters  
queue-id — The queue ID whose parameters are to be overridden.

Values  
1 — 32

adaptation-rule

Syntax  
adaptation-rule [pir {max | min | closest}] [cir {max | min | closest}] [no adaptation-rule]

Context  
config>service>vpls>sap>egress>queue-override>queue
config>service>vpls>sap>ingress>queue-override>queue

Description  
This command can be used to override specific attributes of the specified queue’s adaptation rule parameters. The adaptation rule controls the method used by the system to derive the operational CIR and PIR settings when the queue is provisioned in hardware. For the CIR and PIR parameters individually, the system attempts to find the best operational rate depending on the defined constraint.

The no form of the command removes any explicitly defined constraints used to derive the operational CIR and PIR created by the application of the policy. When a specific adaptation-rule is removed, the default constraints for rate and cir apply.

Default  
no adaptation-rule
Parameters

pir — The pir parameter defines the constraints enforced when adapting the PIR rate defined within the queue queue-id rate command. The pir parameter requires a qualifier that defines the constraint used when deriving the operational PIR for the queue. When the rate command is not specified, the default applies.

cir — The cir parameter defines the constraints enforced when adapting the CIR rate defined within the queue queue-id rate command. The cir parameter requires a qualifier that defines the constraint used when deriving the operational CIR for the queue. When the cir parameter is not specified, the default constraint applies.

adaptation-rule — Specifies the criteria to use to compute the operational CIR and PIR values for this queue, while maintaining a minimum offset.

Values

max — The max (maximum) keyword is mutually exclusive with the min and closest options. When max is defined, the operational PIR for the queue will be equal to or less than the administrative rate specified using the rate command.

min — The min (minimum) keyword is mutually exclusive with the max and closest options. When min is defined, the operational PIR for the queue will be equal to or greater than the administrative rate specified using the rate command.

closest — The closest parameter is mutually exclusive with the min and max parameter. When closest is defined, the operational PIR for the queue will be the rate closest to the rate specified using the rate command.

avg-frame-overhead

Syntax

avg-frame-overhead percent
no avg-frame-overhead

Context

config>service>vpls>sap>egress>queue-override>queue

Description

This command configures the average frame overhead to define the average percentage that the offered load to a queue will expand during the frame encapsulation process before sending traffic on-the-wire. While the avg-frame-overhead value may be defined on any queue, it is only used by the system for queues that egress a Sonet or SDH port or channel. Queues operating on egress Ethernet ports automatically calculate the frame encapsulation overhead based on a 20 byte per packet rule (8 bytes for preamble and 12 bytes for Inter-Frame Gap).

When calculating the frame encapsulation overhead for port scheduling purposes, the system determines the following values:

- **Offered-load** — The offered-load of a queue is calculated by starting with the queue depth in octets, adding the received octets at the queue and subtracting queue discard octets. The result is the number of octets the queue has available to transmit. This is the packet based offered-load.

- **Frame encapsulation overhead** — Using the avg-frame-overhead parameter, the frame encapsulation overhead is simply the queue’s current offered-load (how much has been received by the queue) multiplied by the avg-frame-overhead. If a queue had an offered load of 10000 octets and the avg-frame-overhead equals 10%, the frame encapsulation overhead would be 10000 x 0.1 or 1000 octets.
For egress Ethernet queues, the frame encapsulation overhead is calculated by multiplying the number of offered-packets for the queue by 20 bytes. If a queue was offered 50 packets then the frame encapsulation overhead would be 50 x 20 or 1000 octets.

- Frame based offered-load — The frame based offered-load is calculated by adding the offered-load to the frame encapsulation overhead. If the offered-load is 10000 octets and the encapsulation overhead was 1000 octets, the frame based offered-load would equal 11000 octets.

- Packet to frame factor — The packet to frame factor is calculated by dividing the frame encapsulation overhead by the queue’s offered-load (packet based). If the frame encapsulation overhead is 1000 octets and the offered-load is 10000 octets then the packet to frame factor would be 1000 / 10000 or 0.1. When in use, the avg-frame-overhead will be the same as the packet to frame factor making this calculation unnecessary.

- Frame based CIR — The frame based CIR is calculated by multiplying the packet to frame factor with the queue’s configured CIR and then adding that result to that CIR. If the queue CIR is set at 500 octets and the packet to frame factor equals 0.1, the frame based CIR would be 500 x 1.1 or 550 octets.

- Frame based within-cir offered-load — The frame based within-cir offered-load is the portion of the frame based offered-load considered to be within the frame-based CIR. The frame based within-cir offered-load is the lesser of the frame based offered-load and the frame based CIR. If the frame based offered-load equaled 11000 octets and the frame based CIR equaled 550 octets, the frame based within-cir offered-load would be limited to 550 octets. If the frame based offered-load equaled 450 octets and the frame based CIR equaled 550 octets, the frame based within-cir offered-load would equal 450 octets (or the entire frame based offered-load).

As a special case, when a queue or associated intermediate scheduler is configured with a CIR-weight equal to 0, the system automatically sets the queue’s frame based within-cir offered-load to 0, preventing it from receiving bandwidth during the port scheduler’s within-cir pass.

- Frame based PIR — The frame based PIR is calculated by multiplying the packet to frame factor with the queue’s configured PIR and then adding the result to that PIR. If the queue PIR is set to 7500 octets and the packet to frame factor equals 0.1, the frame based PIR would be 7500 x 1.1 or 8250 octets.

- Frame based within-pir offered-load — The frame based within-pir offered-load is the portion of the frame based offered-load considered to be within the frame based PIR. The frame based within-pir offered-load is the lesser of the frame based offered-load and the frame based PIR. If the frame based offered-load equaled 11000 octets and the frame based PIR equaled 8250 octets, the frame based within-pir offered-load would be limited to 8250 octets. If the frame based offered-load equaled 7000 octets and the frame based PIR equaled 8250 octets, the frame based within-pir offered load would equal 7000 octets.

Port scheduler operation using frame transformed rates — The port scheduler uses the frame based rates to calculate the maximum rates that each queue may receive during the within-cir and above-cir bandwidth allocation passes. During the within-cir pass, a queue may receive up to its frame based within-cir offered-load. The maximum it may receive during the above-cir pass is the difference between the frame based within-pir offered load and the amount of actual bandwidth allocated during the within-cir pass.

SAP and subscriber SLA-profile average frame overhead override — The average frame overhead parameter on a sap-egress may be overridden at an individual egress queue basis. On each SAP and within the sla-profile policy used by subscribers an avg-frame-overhead command may be defined under the queue-override context for each queue. When overridden, the queue instance will use its local value for the average frame overhead instead of the sap-egress defined overhead.
The **no** form of this command restores the average frame overhead parameter for the queue to the default value of 0 percent. When set to 0, the system uses the packet based queue statistics for calculating port scheduler priority bandwidth allocation. If the **no avg-frame-overhead** command is executed in a queue-override queue id context, the avg-frame-overhead setting for the queue within the sap-egress QoS policy takes effect.

**Default**  
0

**Parameters**  
percent — This parameter sets the average amount of packet-to-frame encapsulation overhead expected for the queue. This value is not used by the system for egress Ethernet queues.  

**Values**  
0 — 100

---

**cbs**

**Syntax**  
cbs size-in-kbytes  
no cbs

**Context**  
config>service>vpls>sap>egress>queue-override>queue  
config>service>vpls>sap>ingress>queue-override>queue

**Description**  
This command can be used to override specific attributes of the specified queue’s CBS parameters. It is permissible, and possibly desirable, to oversubscribe the total CBS reserved buffers for a given access port egress buffer pool. Oversubscription may be desirable due to the potential large number of service queues and the economy of statistical multiplexing the individual queue’s CBS setting into the defined reserved total.

When oversubscribing the reserved total, it is possible for a queue depth to be lower than its CBS setting and still not receive a buffer from the buffer pool for an ingress frame. As more queues are using their CBS buffers and the total in use exceeds the defined reserved total, essentially the buffers are being removed from the shared portion of the pool without the shared in use average and total counts being decremented. This can affect the operation of the high and low priority RED slopes on the pool, causing them to miscalculate when to start randomly drop packets. If the CBS value is larger than the MBS value, an error will occur, preventing the CBS change.

The **no** form of this command returns the CBS size to the default value.

**Default**  
no cbs

**Parameters**  
size-in-kbytes — The size parameter is an integer expression of the number of kilobytes reserved for the queue. If a value of 10KBytes is desired, enter the value 10. A value of 0 specifies that no reserved buffers are required by the queue (a minimal reserved size can still be applied for scheduling purposes).  

**Values**  
0 — 131072 or default
virtual-private-lan-services

high-prio-only

Syntax

high-prio-only percent
no high-prio-only

Context

config>service>vpls>sap>egress>queue-override>queue
config>service>vpls>sap>ingress>queue-override>queue

Description

This command can be used to override specific attributes of the specified queue’s high-prio-only parameters. The high-prio-only command configures the percentage of buffer space for the queue, used exclusively by high priority packets.

The priority of a packet can only be set in the SAP ingress QoS policy and is only applicable on the ingress queues for a SAP. The high-prio-only parameter is used to override the default value derived from the network-queue command.

The defined high-prio-only value cannot be greater than the MBS size of the queue. Attempting to change the MBS to a value smaller than the high priority reserve will generate an error and fail execution. Attempting to set the high-prio-only value larger than the current MBS size will also result in an error and fail execution.

The no form of this command restores the default high priority reserved size.

Parameters

percent — The percent parameter is the percentage reserved for high priority traffic on the queue. If a value of 10KBytes is desired, enter the value 10. A value of 0 specifies that none of the MBS of the queue will be reserved for high priority traffic. This does not affect RED slope operation for packets attempting to be queued.

Values 0 — 100, default

mbs

Syntax

mbs {size-in-kbytes | default}
no mbs

Context

config>service>vpls>sap>egress>queue-override>queue
config>service>vpls>sap>ingress>queue-override>queue

Description

This command can be used to override specific attributes of the specified queue’s MBS parameters. The MBS is a mechanism to override the default maximum size for the queue.

The sum of the MBS for all queues on an egress access port can oversubscribe the total amount of buffering available. When congestion occurs and buffers become scarce, access to buffers is controlled by the RED slope a packet is associated with. A queue that has not exceeded its MBS size is not guaranteed that a buffer will be available when needed or that the packet’s RED slope will not force the discard of the packet. Setting proper CBS parameters and controlling CBS oversubscription is one major safeguard to queue starvation (when a queue does not receive its fair share of buffers). Another is properly setting the RED slope parameters for the needs of services on this port or channel.

If the CBS value is larger than the MBS value, an error will occur, preventing the MBS change.

The no form of this command returns the MBS size assigned to the queue.

Default default
Parameters

**size-in-kbytes** — The size parameter is an integer expression of the maximum number of kilobytes of buffering allowed for the queue. For a value of 100 kbps, enter the value 100. A value of 0 causes the queue to discard all packets.

**Values**

0 — 131072 or default

mbs

**Syntax**

`mbs {size-in-kbytes | default}`

`no mbs`

**Context**

`config>service>vpls>sap>ingress>queue-override>queue`

**Description**

This command can be used to override specific attributes of the specified queue’s MBS parameters. The MBS value is used by a queue to determine whether it has exhausted all of its buffers while enqueuing packets. Once the queue has exceeded the amount of buffers allowed by MBS, all packets are discarded until packets have been drained from the queue.

The sum of the MBS for all queues on an ingress access port can oversubscribe the total amount of buffering available. When congestion occurs and buffers become scarce, access to buffers is controlled by the RED slope a packet is associated with. A queue that has not exceeded its MBS size is not guaranteed that a buffer will be available when needed or that the packets RED slope will not force the discard of the packet. Setting proper CBS parameters and controlling CBS oversubscription is one major safeguard to queue starvation (when a queue does not receive its fair share of buffers). Another is properly setting the RED slope parameters for the needs of services on this port or channel.

If the CBS value is larger than the MBS value, an error will occur, preventing the MBS change.

The defined high-prio-only value cannot be greater than the MBS size of the queue. Attempting to change the MBS to a value smaller than the high priority reserve will generate an error and fail execution. Attempting to set the high-prio-only value larger than the current MBS size will also result in an error and fail execution.

The `no` form of this command returns the MBS size assigned to the queue to the default value.

**Default**

`default`

**Parameters**

**size-in-kbytes** — The size parameter is an integer expression of the maximum number of kilobytes of buffering allowed for the queue. For a value of 100 kbps, enter the value 100. A value of 0 causes the queue to discard all packets.

**Values**

0 — 131072 or default

rate

**Syntax**

`rate pir-rate [cir cir-rate]`

`no rate`

**Context**

`config>service>vpls>sap>egress>queue-override>queue`

`config>service>vpls>sap>ingress>queue-override>queue`

`config>service>vpls>sap>egress>hsmda-queue-over>queue`
Description

This command can be used to override specific attributes of the specified queue’s Peak Information Rate (PIR) and the Committed Information Rate (CIR) parameters.

The PIR defines the maximum rate that the queue can transmit packets out an egress interface (for SAP egress queues). Defining a PIR does not necessarily guarantee that the queue can transmit at the intended rate. The actual rate sustained by the queue can be limited by oversubscription factors or available egress bandwidth.

The CIR defines the rate at which the system prioritizes the queue over other queues competing for the same bandwidth. In-profile packets are preferentially queued by the system at egress and at subsequent next hop nodes where the packet can traverse. To be properly handled as in- or out-of-profile throughout the network, the packets must be marked accordingly for profiling at each hop.

The CIR can be used by the queue’s parent commands cir-level and cir-weight parameters to define the amount of bandwidth considered to be committed for the child queue during bandwidth allocation by the parent scheduler.

The rate command can be executed at any time, altering the PIR and CIR rates for all queues created through the association of the SAP egress QoS policy with the queue-id.

The no form of the command returns all queues created with the queue-id by association with the QoS policy to the default PIR and CIR parameters (max, 0).

Default rate max cir 0 — The max default specifies the amount of bandwidth in kilobits per second (thousand bits per second). The max value is mutually exclusive to the pir-rate value.

Parameters

pir-rate — Defines the administrative PIR rate, in kilobits, for the queue. When the rate command is executed, a valid PIR setting must be explicitly defined. When the rate command has not been executed, the default PIR of max is assumed.

Fractional values are not allowed and must be given as a positive integer.

The actual PIR rate is dependent on the queue’s adaptation-rule parameters and the actual hardware where the queue is provisioned.

Values 1 — 100000000

Default max

cir cir-rate — The cir parameter overrides the default administrative CIR used by the queue. When the rate command is executed, a CIR setting is optional. When the rate command has not been executed or the cir parameter is not explicitly specified, the default CIR (0) is assumed.

Fractional values are not allowed and must be given as a positive integer. The sum keyword specifies that the CIR be used as the summed CIR values of the children schedulers or queues.

Values 0 — 100000000, max, sum

Default 0

queue-override

Syntax [no] queue-override

Context config>service>vpls>sap>egress
config>service>vpls>sap>ingress
config>service>vpls>sap>egress>hsmda-queue-over>queue
config>service>vpls>sap>ingress>hsmda-queue-over>queue
Description
This command enables the context to configure override values for the specified SAP egress or ingress QoS queue. These values override the corresponding ones specified in the associated SAP egress or ingress QoS policy.

queue
Syntax
[no] queue queue-id
Context
config>service>vpls>sap>egress>queue-override
config>service>vpls>sap>ingress>queue-override
Description
This command specifies the ID of the queue whose parameters are to be overridden.
Parameters
queue-id — The queue ID whose parameters are to be overridden.
Values
1 — 32

adaptation-rule
Syntax
adaptation-rule [pir {max | min | closest}] [cir {max | min | closest}]
no adaptation-rule
Context
config>service>vpls>sap>egress>queue-override>queue
config>service>vpls>sap>ingress>queue-override>queue
Description
This command can be used to override specific attributes of the specified queue’s adaptation rule parameters. The adaptation rule controls the method used by the system to derive the operational CIR and PIR settings when the queue is provisioned in hardware. For the CIR and PIR parameters individually, the system attempts to find the best operational rate depending on the defined constraint.

The no form of the command removes any explicitly defined constraints used to derive the operational CIR and PIR created by the application of the policy. When a specific adaptation-rule is removed, the default constraints for rate and cir apply.

Default
no adaptation-rule
Parameters
pir — The pir parameter defines the constraints enforced when adapting the PIR rate defined within the queue queue-id rate command. The pir parameter requires a qualifier that defines the constraint used when deriving the operational PIR for the queue. When the rate command is not specified, the default applies.

cir — The cir parameter defines the constraints enforced when adapting the CIR rate defined within the queue queue-id rate command. The cir parameter requires a qualifier that defines the constraint used when deriving the operational CIR for the queue. When the cir parameter is not specified, the default constraint applies.

adaptation-rule — Specifies the criteria to use to compute the operational CIR and PIR values for this queue, while maintaining a minimum offset.
Values

**max** — The **max** (maximum) keyword is mutually exclusive with the **min** and **closest** options. When **max** is defined, the operational PIR for the queue will be equal to or less than the administrative rate specified using the **rate** command.

**min** — The **min** (minimum) keyword is mutually exclusive with the **max** and **closest** options. When **min** is defined, the operational PIR for the queue will be equal to or greater than the administrative rate specified using the **rate** command.

**closest** — The **closest** parameter is mutually exclusive with the **min** and **max** parameter. When **closest** is defined, the operational PIR for the queue will be the rate closest to the rate specified using the **rate** command.

---

### avg-frame-overhead

**Syntax**

```
avg-frame-overhead percent
no avg-frame-overhead
```

**Context**

```
cfg>service>vpls>sap>egress>queue-override>queue
```

**Description**

This command configures the average frame overhead to define the average percentage that the offered load to a queue will expand during the frame encapsulation process before sending traffic on-the-wire. While the avg-frame-overhead value may be defined on any queue, it is only used by the system for queues that egress a Sonet or SDH port or channel. Queues operating on egress Ethernet ports automatically calculate the frame encapsulation overhead based on a 20 byte per packet rule (8 bytes for preamble and 12 bytes for Inter-Frame Gap).

When calculating the frame encapsulation overhead for port scheduling purposes, the system determines the following values:

- **Offered-load** — The offered-load of a queue is calculated by starting with the queue depth in octets, adding the received octets at the queue and subtracting queue discard octets. The result is the number of octets the queue has available to transmit. This is the packet based offered-load.

- **Frame encapsulation overhead** — Using the avg-frame-overhead parameter, the frame encapsulation overhead is simply the queue’s current offered-load (how much has been received by the queue) multiplied by the avg-frame-overhead. If a queue had an offered load of 10000 octets and the avg-frame-overhead equals 10%, the frame encapsulation overhead would be 10000 x 0.1 or 1000 octets.

For egress Ethernet queues, the frame encapsulation overhead is calculated by multiplying the number of offered-packets for the queue by 20 bytes. If a queue was offered 50 packets then the frame encapsulation overhead would be 50 x 20 or 1000 octets.

- **Frame based offered-load** — The frame based offered-load is calculated by adding the offered-load to the frame encapsulation overhead. If the offered-load is 10000 octets and the encapsulation overhead was 1000 octets, the frame based offered-load would equal 11000 octets.

- **Packet to frame factor** — The packet to frame factor is calculated by dividing the frame encapsulation overhead by the queue’s offered-load (packet based). If the frame encapsulation overhead is 1000 octets and the offered-load is 10000 octets then the packet to frame factor would be 1000 / 10000 or 0.1. When in use, the avg-frame-overhead will be the same as the packet to frame factor making this calculation unnecessary.
• Frame based CIR — The frame based CIR is calculated by multiplying the packet to frame factor with the queue’s configured CIR and then adding that result to that CIR. If the queue CIR is set at 500 octets and the packet to frame factor equals 0.1, the frame based CIR would be 500 x 1.1 or 550 octets.

• Frame based within-cir offered-load — The frame based within-cir offered-load is the portion of the frame based offered-load considered to be within the frame-based CIR. The frame based within-cir offered-load is the lesser of the frame based offered-load and the frame based CIR. If the frame based offered-load equaled 11000 octets and the frame based CIR equaled 550 octets, the frame based within-cir offered-load would be limited to 550 octets. If the frame based offered-load equaled 450 octets and the frame based CIR equaled 550 octets, the frame based within-cir offered-load would equal 450 octets (or the entire frame based offered-load).

As a special case, when a queue or associated intermediate scheduler is configured with a CIR-weight equal to 0, the system automatically sets the queue’s frame based within-cir offered-load to 0, preventing it from receiving bandwidth during the port scheduler’s within-cir pass.

• Frame based PIR — The frame based PIR is calculated by multiplying the packet to frame factor with the queue’s configured PIR and then adding the result to that PIR. If the queue PIR is set to 7500 octets and the packet to frame factor equals 0.1, the frame based PIR would be 7500 x 1.1 or 8250 octets.

• Frame based within-pir offered-load — The frame based within-pir offered-load is the portion of the frame based offered-load considered to be within the frame based PIR. The frame based within-pir offered-load is the lesser of the frame based offered-load and the frame based PIR. If the frame based offered-load equaled 11000 octets and the frame based PIR equaled 8250 octets, the frame based within-pir offered-load would be limited to 8250 octets. If the frame based offered-load equaled 7000 octets and the frame based PIR equaled 8250 octets, the frame based within-pir offered load would equal 7000 octets.

Port scheduler operation using frame transformed rates — The port scheduler uses the frame based rates to calculate the maximum rates that each queue may receive during the within-cir and above-cir bandwidth allocation passes. During the within-cir pass, a queue may receive up to its frame based within-cir offered-load. The maximum it may receive during the above-cir pass is the difference between the frame based within-pir offered load and the amount of actual bandwidth allocated during the within-cir pass.

SAP and subscriber SLA-profile average frame overhead override — The average frame overhead parameter on a sap-egress may be overridden at an individual egress queue basis. On each SAP and within the sla-profile policy used by subscribers an avg-frame-overhead command may be defined under the queue-override context for each queue. When overridden, the queue instance will use its local value for the average frame overhead instead of the sap-egress defined overhead.

The no form of this command restores the average frame overhead parameter for the queue to the default value of 0 percent. When set to 0, the system uses the packet based queue statistics for calculating port scheduler priority bandwidth allocation. If the no avg-frame-overhead command is executed in a queue-override queue id context, the avg-frame-overhead setting for the queue within the sap-egress QoS policy takes effect.

```
Default 0

Parameters percent — This parameter sets the average amount of packet-to-frame encapsulation overhead expected for the queue. This value is not used by the system for egress Ethernet queues.

Values 0 — 100
```
cbs

Syntax  
cbs size-in-kbytes
no cbs

Context  
config>service>vpls>sap>egress>queue-override>queue
config>service>vpls>sap>ingress>queue-override>queue

Description  
This command can be used to override specific attributes of the specified queue’s CBS parameters.

It is permissible, and possibly desirable, to oversubscribe the total CBS reserved buffers for a given access port egress buffer pool. Oversubscription may be desirable due to the potential large number of service queues and the economy of statistical multiplexing the individual queue’s CBS setting into the defined reserved total.

When oversubscribing the reserved total, it is possible for a queue depth to be lower than its CBS setting and still not receive a buffer from the buffer pool for an ingress frame. As more queues are using their CBS buffers and the total in use exceeds the defined reserved total, essentially the buffers are being removed from the shared portion of the pool without the shared in use average and total counts being decremented. This can affect the operation of the high and low priority RED slopes on the pool, causing them to miscalculate when to start randomly drop packets.

If the CBS value is larger than the MBS value, an error will occur, preventing the CBS change.

The no form of this command returns the CBS size to the default value.

Default  
no cbs

Parameters  
size-in-kbytes — The size parameter is an integer expression of the number of kilobytes reserved for the queue. If a value of 10KBytes is desired, enter the value 10. A value of 0 specifies that no reserved buffers are required by the queue (a minimal reserved size can still be applied for scheduling purposes).

Values  
0 — 131072 or default

high-prio-only

Syntax  
high-prio-only percent
no high-prio-only

Context  
config>service>vpls>sap>egress>queue-override>queue
config>service>vpls>sap>ingress>queue-override>queue

Description  
This command can be used to override specific attributes of the specified queue’s high-prio-only parameters. The high-prio-only command configures the percentage of buffer space for the queue, used exclusively by high priority packets.

The priority of a packet can only be set in the SAP ingress QoS policy and is only applicable on the ingress queues for a SAP. The high-prio-only parameter is used to override the default value derived from the network-queue command.

The defined high-prio-only value cannot be greater than the MBS size of the queue. Attempting to change the MBS to a value smaller than the high priority reserve will generate an error and fail.
The no form of this command restores the default high priority reserved size.

**Parameters**

- **percent** — The *percent* parameter is the percentage reserved for high priority traffic on the queue. If a value of 10KBytes is desired, enter the value 10. A value of 0 specifies that none of the MBS of the queue will be reserved for high priority traffic. This does not affect RED slope operation for packets attempting to be queued.

  **Values**  
  0 — 100, default

### mbs

**Syntax**

- `mbs {size-in-kbytes | default}`
- `no mbs`

**Context**

- `config>service>vpls>sap>egress>queue-override>queue`

**Description**

This command can be used to override specific attributes of the specified queue’s MBS parameters. The MBS is a mechanism to override the default maximum size for the queue.

The sum of the MBS for all queues on an egress access port can oversubscribe the total amount of buffering available. When congestion occurs and buffers become scarce, access to buffers is controlled by the RED slope a packet is associated with. A queue that has not exceeded its MBS size is not guaranteed that a buffer will be available when needed or that the packet’s RED slope will not force the discard of the packet. Setting proper CBS parameters and controlling CBS oversubscription is one major safeguard to queue starvation (when a queue does not receive its fair share of buffers). Another is properly setting the RED slope parameters for the needs of services on this port or channel.

If the CBS value is larger than the MBS value, an error will occur, preventing the MBS change.

The no form of this command returns the MBS size assigned to the queue.

**Default**

- default

**Parameters**

- **size-in-kbytes** — The size parameter is an integer expression of the maximum number of kilobytes of buffering allowed for the queue. For a value of 100 kbps, enter the value 100. A value of 0 causes the queue to discard all packets.

  **Values**  
  0 — 131072 or default
The sum of the MBS for all queues on an ingress access port can oversubscribe the total amount of buffering available. When congestion occurs and buffers become scarce, access to buffers is controlled by the RED slope a packet is associated with. A queue that has not exceeded its MBS size is not guaranteed that a buffer will be available when needed or that the packets RED slope will not force the discard of the packet. Setting proper CBS parameters and controlling CBS oversubscription is one major safeguard to queue starvation (when a queue does not receive its fair share of buffers). Another is properly setting the RED slope parameters for the needs of services on this port or channel. If the CBS value is larger than the MBS value, an error will occur, preventing the MBS change.

The defined high-prio-only value cannot be greater than the MBS size of the queue. Attempting to change the MBS to a value smaller than the high priority reserve will generate an error and fail execution. Attempting to set the high-prio-only value larger than the current MBS size will also result in an error and fail execution.

The no form of this command returns the MBS size assigned to the queue to the default value.

**Default**

default

**Parameters**

default [size-in-kbytes] — The size parameter is an integer expression of the maximum number of kilobytes of buffering allowed for the queue. For a value of 100 kbps, enter the value 100. A value of 0 causes the queue to discard all packets.

Values 0 — 131072 or default

**rate**

**Syntax**

rate pir-rate [cir cir-rate]

no rate

**Context**

config>service>vpls>sap>egress>queue-override>queue
config>service>vpls>sap>ingress>queue-override>queue
config>service>vpls>sap>egress>hsmda-queue-over>queue

**Description**

This command can be used to override specific attributes of the specified queue’s Peak Information Rate (PIR) and the Committed Information Rate (CIR) parameters.

The PIR defines the maximum rate that the queue can transmit packets out an egress interface (for SAP egress queues). Defining a PIR does not necessarily guarantee that the queue can transmit at the intended rate. The actual rate sustained by the queue can be limited by oversubscription factors or available egress bandwidth.

The CIR defines the rate at which the system prioritizes the queue over other queues competing for the same bandwidth. In-profile packets are preferentially queued by the system at egress and at subsequent next hop nodes where the packet can traverse. To be properly handled as in- or out-of-profile throughout the network, the packets must be marked accordingly for profiling at each hop.

The CIR can be used by the queue’s parent commands cir-level and cir-weight parameters to define the amount of bandwidth considered to be committed for the child queue during bandwidth allocation by the parent scheduler.

The rate command can be executed at any time, altering the PIR and CIR rates for all queues created through the association of the SAP egress QoS policy with the queue-id.
The no form of the command returns all queues created with the queue-id by association with the QoS policy to the default PIR and CIR parameters (max, 0).

**Default**
rate max cir 0 — The max default specifies the amount of bandwidth in kilobits per second (thousand bits per second). The max value is mutually exclusive to the pir-rate value.

**Parameters**
pir-rate — Defines the administrative PIR rate, in kilobits, for the queue. When the rate command is executed, a valid PIR setting must be explicitly defined. When the rate command has not been executed, the default PIR of max is assumed.
Fractional values are not allowed and must be given as a positive integer.
The actual PIR rate is dependent on the queue’s adaptation-rule parameters and the actual hardware where the queue is provisioned.

Values 1 — 100000000
Default max

cir cir-rate — The cir parameter overrides the default administrative CIR used by the queue. When the rate command is executed, a CIR setting is optional. When the rate command has not been executed or the cir parameter is not explicitly specified, the default CIR (0) is assumed.
Fractional values are not allowed and must be given as a positive integer. The sum keyword specifies that the CIR be used as the summed CIR values of the children schedulers or queues.

Values 0 — 100000000, max, sum
Default 0

wred-queue-policy

**Syntax**
wred-queue-policy slope-policy-name
no wred-queue-policy

**Context**
config>service>vpls>sap>egress>queue-override>queue

**Description**
The wred-queue-policy command is used on an egress SAP to override the slope policy associated with a WRED queue. When specified, the SAP egress QoS policy derived slope policy is ignored and the configured override slope policy is applied to the WRED queue. The specified queue-id must be a WRED-enabled queue to be successful.

The no form of the command removes the slope policy override for the WRED queue on the egress SAP.

**Parameters**
slope-policy-name — Overrides the SAP Egress QoS policy derived WRED slope policy for the specified queue-id. The defined slope policy must exist or the command will fail.

scheduler-override

**Syntax**
[no] scheduler-override

**Context**
config>service>vpls>sap>egress
cfgin>service>vpls>sap>ingress
Description
This command specifies the set of attributes whose values have been overridden via management on this virtual scheduler. Clearing a given flag will return the corresponding overridden attribute to the value defined on the SAP’s ingress scheduler policy.

scheduler

Syntax
scheduler scheduler-name
no scheduler scheduler-name

Context  config>service>vpls>sap>egress>sched-override

Description
This command can be used to override specific attributes of the specified scheduler name. A scheduler defines a bandwidth controls that limit each child (other schedulers and queues) associated with the scheduler. Scheduler objects are created within the hierarchical tiers of the policy. It is assumed that each scheduler created will have queues or other schedulers defined as child associations. The scheduler can be a child (take bandwidth from a scheduler in a higher tier, except for schedulers created in tier 1). A total of 32 schedulers can be created within a single scheduler policy with no restriction on the distribution between the tiers.

Each scheduler must have a unique name within the context of the scheduler policy; however the same name can be reused in multiple scheduler policies. If scheduler-name already exists within the policy tier level (regardless of the inclusion of the keyword create), the context changes to that scheduler name for the purpose of editing the scheduler parameters. Modifications made to an existing scheduler are executed on all instantiated schedulers created through association with the policy of the edited scheduler. This can cause queues or schedulers to become orphaned (invalid parent association) and adversely affect the ability of the system to enforce service level agreements (SLAs).

If the scheduler-name exists within the policy on a different tier (regardless of the inclusion of the keyword create), an error occurs and the current CLI context will not change.

If the scheduler-name does not exist in this or another tier within the scheduler policy, it is assumed that an attempt is being made to create a scheduler of that name. The success of the command execution is dependent on the following:

1. The maximum number of schedulers has not been configured.
2. The provided scheduler-name is valid.
3. The create keyword is entered with the command if the system is configured to require it (enabled in the environment create command).

When the maximum number of schedulers has been exceeded on the policy, a configuration error occurs and the command will not execute, nor will the CLI context change.

If the provided scheduler-name is invalid according to the criteria below, a name syntax error will occur, the command will not execute, and the CLI context will not change.

Parameters

Values
Valid names consist of any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

Default
None. Each scheduler must be explicitly created.
create — This optional keyword explicitly specifies that it is acceptable to create a scheduler with the given scheduler-name. If the create keyword is omitted, scheduler-name is not created when the system environment variable create is set to true. This safeguard is meant to avoid accidental creation of system objects (such as schedulers) while attempting to edit an object with a mistyped name or ID. The keyword has no effect when the object already exists.

rate

Syntax  
rate pir-rate [cir cir-rate]

no rate

Context  
config>service>vpls>sap>egress>sched-override>scheduler

Description  
This command can be used to override specific attributes of the specified scheduler rate. The rate command defines the maximum bandwidth that the scheduler can offer its child queues or schedulers. The maximum rate is limited to the amount of bandwidth the scheduler can receive from its parent scheduler. If the scheduler has no parent, the maximum rate is assumed to be the amount available to the scheduler. When a parent is associated with the scheduler, the CIR parameter provides the amount of bandwidth to be considered during the parent scheduler’s `within CIR` distribution phase.

The actual operating rate of the scheduler is limited by bandwidth constraints other than its maximum rate. The scheduler’s parent scheduler may not have the available bandwidth to meet the scheduler’s needs or the bandwidth available to the parent scheduler could be allocated to other child schedulers or child queues on the parent based on higher priority. The children of the scheduler may not need the maximum rate available to the scheduler due to insufficient offered load or limits to their own maximum rates.

When a scheduler is defined without specifying a rate, the default rate is max. If the scheduler is a root scheduler (no parent defined), the default maximum rate must be changed to an explicit value. Without this explicit value, the scheduler will assume that an infinite amount of bandwidth is available and allow all child queues and schedulers to operate at their maximum rates.

The no form of this command returns all queues created with this queue-id by association with the QoS policy to the default PIR and CIR parameters.

Parameters  
pir-rate — The pir parameter accepts a step multiplier value that specifies the multiplier used to determine the PIR rate at which the queue will operate. A value of 0 to 100000000 or the keyword max is accepted. Any other value will result in an error without modifying the current PIR rate.

To calculate the actual PIR rate, the rate described by the queue’s rate is multiplied by the pir-rate.

The SAP ingress context for PIR is independent of the defined forwarding class (fc) for the queue. The default pir and definable range is identical for each class. The PIR in effect for a queue defines the maximum rate at which the queue will be allowed to forward packets in a given second, thus shaping the queue’s output.

The PIR parameter for SAP ingress queues do not have a negate (no) function. To return the queues PIR rate to the default value, that value must be specified as the PIR value.

Values  
1 — 100000000, max

Default  
max
**cir cir-rate** — The **cir** parameter accepts a step-multiplier value that specifies the multiplier used to determine the CIR rate at which the queue will operate. A value of 0 — 10000000 or the keyword **max** or **sum** is accepted. Any other value will result in an error without modifying the current CIR rate.

To calculate the actual CIR rate, the rate described by the **rate pir pir-rate** is multiplied by the **cir cir-rate**. If the **cir** is set to max, then the CIR rate is set to infinity.

The SAP ingress context for CIR is dependent on the defined forwarding class (fc) for the queue. The default CIR and definable range is different for each class. The CIR in effect for a queue defines both its profile (in or out) marking level as well as the relative importance compared to other queues for scheduling purposes during congestion periods.

**Values**  
0 — 10000000, **max**, **sum**

**Default**  
**sum**

---

**scheduler-policy**

**Syntax**  
scheduler-policy scheduler-policy-name  
no scheduler-policy

**Context**  
config>service>vpls>sap>ingress  
config>service>vpls>sap>egress

**Description**  
This command applies an existing scheduler policy to an ingress or egress scheduler used by SAP queues associated with this multi-service customer site. The schedulers defined in the scheduler policy can only be created once the customer site has been appropriately assigned to a chassis port, channel or slot. Scheduler policies are defined in the config>qos>scheduler-policy scheduler-policy-name context.

The **no** form of this command removes the configured ingress or egress scheduler policy from the multi-service customer site. When the policy is removed, the schedulers created due to the policy are removed also making them unavailable for the ingress SAP queues associated with the customer site. Queues that lose their parent scheduler association are deemed to be orphaned and are no longer subject to a virtual scheduler. The SAPs that have ingress queues reliant on the removed schedulers enter into an operational state depicting the orphaned status of one or more queues. When the **no** scheduler-policy command is executed, the customer site ingress or egress node will not contain an applied scheduler policy.

**scheduler-policy-name:** — The **scheduler-policy-name** parameter applies an existing scheduler policy that was created in the config>qos>scheduler-policy scheduler-policy-name context to create the hierarchy of ingress or egress virtual schedulers. The scheduler names defined within the policy are created and made available to any ingress or egress queues created on associated SAPs.

**Values**  
Any existing valid scheduler policy name.
vlan-translation

Syntax

```
vlan-translation {vlan-id | copy-outer}
no vlan-translation
```

Context

```
config>service>vpls>sap>ingress
```

Description

This command configures ingress VLAN translation. If enabled with an explicit VLAN value, the preserved VLAN ID will be overwritten with this value. This setting is applicable to Dot1q-encapsulated ports. If enabled with the `copy-outer` keyword, the outer VLAN ID will be copied to the inner position on QinQ-encapsulated ports. The feature is not supported on default-dot1q SAPs (1/1/1:* and 1/1/1:0), as well as on TopQ SAPs.

The `no` form of this command sets the default value, and no action will be taken.

Default

per default the preserved VLAN values will not be overwritten

Parameters

- `vlan-id` — Specifies the to use the VLAN ID of the SAP.
  - Values: 0 — 4094
- `copy-outer` — Specifies that the outer VLAN ID will be copied to the inner position on QinQ-encapsulated ports

match-qinq-dot1p

Syntax

```
match-qinq-dot1p {top | bottom}
no match-qinq-dot1p de
```

Context

```
config>service>vpls>sap>ingress
```

Description

This command specifies which Dot1Q tag position Dot1P bits in a QinQ encapsulated packet should be used to evaluate Dot1P QoS classification.

The `match-qinq-dot1p` command allows the top or bottom PBits to be used when evaluating the applied sap-ingress QoS policy’s Dot1P entries. The `top` and `bottom` keywords specify which position should be evaluated for QinQ encapsulated packets.

The setting also applies to classification based on the DE indicator bit.

The `no` form of this command reverts the dot1p and de bits matching to the default tag.

By default, the bottom most service delineating Dot1Q tags Dot1P bits are used. Table 11 defines the default behavior for Dot1P evaluation.

<table>
<thead>
<tr>
<th>Port / SAP Type</th>
<th>Existing Packet Tags</th>
<th>PBits Used for Match</th>
</tr>
</thead>
<tbody>
<tr>
<td>Null</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>Null</td>
<td>Dot1P (VLAN-ID 0)</td>
<td>Dot1P PBits</td>
</tr>
<tr>
<td>Null</td>
<td>Dot1Q</td>
<td>Dot1Q PBits</td>
</tr>
</tbody>
</table>
Virtual Private LAN Services

Table 11: Default QinQ and TopQ SAP Dot1P Evaluation  (Continued)

<table>
<thead>
<tr>
<th>Port / SAP Type</th>
<th>Existing Packet Tags</th>
<th>PBits Used for Match</th>
</tr>
</thead>
<tbody>
<tr>
<td>Null</td>
<td>TopQ BottomQ</td>
<td>TopQ PBits</td>
</tr>
<tr>
<td>Null</td>
<td>TopQ (No BottomQ)</td>
<td>TopQ PBits</td>
</tr>
<tr>
<td>Dot1Q</td>
<td>None (Default SAP)</td>
<td>None</td>
</tr>
<tr>
<td>Dot1Q</td>
<td>Dot1P (Default SAP VLAN-ID 0)</td>
<td>Dot1P PBits</td>
</tr>
<tr>
<td>Dot1Q</td>
<td>Dot1Q</td>
<td>Dot1Q PBits</td>
</tr>
<tr>
<td>QinQ / TopQ</td>
<td>TopQ</td>
<td>TopQ PBits</td>
</tr>
<tr>
<td>QinQ / TopQ</td>
<td>TopQ BottomQ</td>
<td>TopQ PBits</td>
</tr>
<tr>
<td>QinQ / QinQ</td>
<td>TopQ BottomQ</td>
<td>BottomQ PBits</td>
</tr>
</tbody>
</table>

Default: no match-qinq-dot1p (no filtering based on p-bits) (top or bottom must be specified to override the default QinQ dot1p behavior)

Parameters:

**top** — The top parameter is mutually exclusive to the bottom parameter. When the top parameter is specified, the top most PBits are used (if existing) to match any dot1p dot1p-value entries. The following table defines the dot1p evaluation behavior when the top parameter is specified.

<table>
<thead>
<tr>
<th>Port / SAP Type</th>
<th>Existing Packet Tags</th>
<th>PBits Used for Match</th>
</tr>
</thead>
<tbody>
<tr>
<td>Null</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>Null</td>
<td>Dot1P (VLAN-ID 0)</td>
<td>Dot1P PBits</td>
</tr>
<tr>
<td>Null</td>
<td>Dot1Q</td>
<td>Dot1Q PBits</td>
</tr>
<tr>
<td>Null</td>
<td>TopQ BottomQ</td>
<td>TopQ PBits</td>
</tr>
<tr>
<td>Null</td>
<td>TopQ (No BottomQ)</td>
<td>TopQ PBits</td>
</tr>
<tr>
<td>Dot1Q</td>
<td>None (Default SAP)</td>
<td>None</td>
</tr>
<tr>
<td>Dot1Q</td>
<td>Dot1P (Default SAP VLAN-ID 0)</td>
<td>Dot1P PBits</td>
</tr>
<tr>
<td>Dot1Q</td>
<td>Dot1Q</td>
<td>Dot1Q PBits</td>
</tr>
<tr>
<td>QinQ / TopQ</td>
<td>TopQ</td>
<td>TopQ PBits</td>
</tr>
<tr>
<td>QinQ / TopQ</td>
<td>TopQ BottomQ</td>
<td>TopQ PBits</td>
</tr>
<tr>
<td>QinQ / QinQ</td>
<td>TopQ BottomQ</td>
<td>TopQ PBits</td>
</tr>
</tbody>
</table>

**bottom** — The bottom parameter is mutually exclusive to the top parameter. When the bottom parameter is specified, the bottom most PBits are used (if existing) to match any dot1p dot1p-value entries. The following table defines the dot1p evaluation behavior when the bottom parameter is specified.
The QinQ and TopQ SAP PBit/DEI bit marking follows the default behavior defined in the table above when `qinq-mark-top-only` is not specified.

### Table 12: Bottom Position QinQ and TopQ SAP Dot1P Evaluation

<table>
<thead>
<tr>
<th>Port / SAP Type</th>
<th>Existing Packet Tags</th>
<th>PBits Used for Match</th>
</tr>
</thead>
<tbody>
<tr>
<td>Null</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>Null</td>
<td>Dot1P (VLAN-ID 0)</td>
<td>Dot1P PBits</td>
</tr>
<tr>
<td>Null</td>
<td>Dot1Q</td>
<td>Dot1Q PBits</td>
</tr>
<tr>
<td>Null</td>
<td>TopQ BottomQ</td>
<td>TopQ PBits</td>
</tr>
<tr>
<td>Null</td>
<td>TopQ (No BottomQ)</td>
<td>TopQ PBits</td>
</tr>
<tr>
<td>Dot1Q</td>
<td>None (Default SAP)</td>
<td>None</td>
</tr>
<tr>
<td>Dot1Q</td>
<td>Dot1P (Default SAP VLAN-ID 0)</td>
<td>Dot1P PBits</td>
</tr>
<tr>
<td>Dot1Q</td>
<td>Dot1Q</td>
<td>Dot1Q PBits</td>
</tr>
<tr>
<td>QinQ / TopQ</td>
<td>TopQ</td>
<td>TopQ PBits</td>
</tr>
<tr>
<td>QinQ / TopQ</td>
<td>TopQ BottomQ</td>
<td>TopQ PBits</td>
</tr>
<tr>
<td>QinQ / QinQ</td>
<td>TopQ BottomQ</td>
<td>BottomQ PBits</td>
</tr>
</tbody>
</table>

### Egress SAP Type

<table>
<thead>
<tr>
<th>Egress SAP Type</th>
<th>Ingress Packet Preserved Dot1P State</th>
<th>Marked (or Remarked) PBits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Null</td>
<td>No preserved Dot1P bits</td>
<td>None</td>
</tr>
<tr>
<td>Null</td>
<td>Preserved Dot1P bits</td>
<td>Preserved tag PBits remarked using dot1p-value</td>
</tr>
<tr>
<td>Dot1Q</td>
<td>No preserved Dot1P bits</td>
<td>New PBits marked using dot1p-value</td>
</tr>
<tr>
<td>Dot1Q</td>
<td>Preserved Dot1P bits</td>
<td>Preserved tag PBits remarked using dot1p-value</td>
</tr>
<tr>
<td>TopQ</td>
<td>No preserved Dot1P bits</td>
<td>TopQ PBits marked using dot1p-value</td>
</tr>
<tr>
<td>TopQ</td>
<td>Preserved Dot1P bits (used as TopQ and BottomQ PBits)</td>
<td>TopQ PBits marked using dot1p-value, BottomQ PBits preserved</td>
</tr>
<tr>
<td>QinQ</td>
<td>No preserved Dot1P bits</td>
<td>TopQ PBits and BottomQ PBits marked using dot1p-value</td>
</tr>
<tr>
<td>QinQ</td>
<td>Preserved Dot1P bits (used as TopQ and BottomQ PBits)</td>
<td>TopQ PBits and BottomQ PBits marked using dot1p-value</td>
</tr>
</tbody>
</table>
The dot1p dot1p-value command must be configured without the qinq-mark-top-only parameter to remove the TopQ PBits only marking restriction.

Note that a QinQ-encapsulated Ethernet port can have two different sap types:
- For a TopQ SAP type, only the outer (top) tag is explicitly specified. For example, sap 1/1/1:10.*
- For QinQ SAP type, both inner (bottom) and outer (top) tags are explicitly specified. For example, sap 1/1/1:10.100.

policer-control-policy

Syntax
```
policer-control-policy policy-name [create]
no policer-control-policy
```

Context
config>service>vpls>sap>egress

Description
This command, within the qos CLI node, is used to create, delete or modify policer control policies. A policer control policy is very similar to the scheduler-policy which is used to manage a set of queues by defining a hierarchy of virtual schedulers and specifying how the virtual schedulers interact to provide an aggregate SLA. In a similar fashion, the policer-control-policy controls the aggregate bandwidth available to a set of child policers. Once created, the policy can be applied to ingress or egress SAPs. The policy may also be applied to the ingress or egress context of a sub-profile.

Policer Control Policy Instances

On the SAP side, an instance of a policy is created each time a policy is applied. When applied to a sub-profile, an instance of the policy is created each time a subscriber successfully maps one or more hosts to the profile per ingress SAP.

Each instance of the policer-control-policy manages the policers associated with the object that owns the policy instance (SAP or subscriber). If a policer on the object is parented to an appropriate arbiter name that exists within the policy, the policer will be managed by the instance. If a policer is not parented or is parented to a non-existent arbiter, the policer will be orphaned and will not be subject to bandwidth control by the policy instance.

Maximum Rate and Root Arbiter

The policer-control-policy supports an overall maximum rate (max-rate) that defines the total amount of bandwidth that may be distributed to all associated child policers. By default, that rate is set to max which provides an unlimited amount of bandwidth to the policers. Once the policy is created, an actual rate should be configured in order for the policy instances to be effective. At the SAP level, the maximum rate may be overridden on a per instance basis. For subscribers, the maximum rate may only be overridden on the subscriber profile which will then be applied to all instances associated with the profile.

The maximum rate is defined within the context of the root arbiter which is always present in a policer-control-policy. The system creates a parent policer which polices the output of all child policers attached to the policy instance to the configured rate. Child policers may be parented directly to the root arbiter (parent root) or parented to one of the tiered arbiters (parent arbiter-name). Since
each tiered arbiter must be parented to either another tiered arbiter or the root arbiter (default), every parented child policer is associated with the root arbiter and thus the root arbiter’s parent policer.

Parent Policer PIR Leaky Bucket Operation

The parent policer is a single leaky bucket that monitors the aggregate throughput rate of the associated child policers. Forwarded packets increment the bucket by the size of each packet. The rate of the parent policer is implemented as a bucket decrement function which attempts to drain the bucket. If the rate of the packets flowing through the bucket is less than the decrement rate, the bucket does not accumulate depth. Each packet that flows through the bucket is accompanied by a derived discard threshold. If the current depth of the bucket is less than the discard threshold, the packet is allowed to pass through, retaining the colors derived from the packet’s child policer. If the current depth is equal to or greater than the threshold value, the packet is colored red and the bucket depth is not incremented by the packet size. Also, any increased bucket depths in the child policer are canceled making any discard event an atomic function between the child and the parent.

Due to the fact that multiple thresholds are supported by the parent policer, the policer control policy is able to protect the throughput of higher priority child policers from the throughput of the lower priority child policers within the aggregate rate.

Tier 1 and Tier 2 Arbiters

As stated above, each child is attached either to the always available root arbiter or to an explicitly created tier 1 or tier 2 arbiter. Unlike the hardware parent policer based root arbiter, the arbiters at tier 1 and tier 2 are only represented in software and are meant to provide an arbitrary hierarchical bandwidth distribution capability. An arbiter created on tier 2 must parent to either to an arbiter on tier 1 or to the root arbiter. Arbiters created on tier 1 always parent to the root arbiter. In this manner, every arbiter ultimately is parented or grand-parented by the root arbiter.

Each tiered arbiter supports an optional rate parameter that defines a rate limit for all child arbiters or child policers associated with the arbiter. Child arbiters and policers attached to the arbiter have a level attribute that defines the strict level at which the child is given bandwidth by the arbiter. Level 8 is the highest and 1 is the lowest. Also a weight attribute defines each child’s weight at that strict level in order to determine how bandwidth is distributed to multiple children at that level when insufficient bandwidth is available to meet each child’s required bandwidth.

Fair and Unfair Bandwidth Control

Each child policer supports three leaky buckets. The PIR bucket manages the policer’s peak rate and maximum burst size, the CIR leaky bucket manages the policer’s committed rate (in-profile / out-of-profile) and committed burst size. The third leaky bucket is used by the policer control policy instance to manage the child policer’s fair rate (FIR). When multiple child policers are attached to the root arbiter at the same priority level, the policy instance uses each child’s FIR bucket rate to control how much of the traffic forwarded by the policer is fair and how much is unfair.

In the simplest case where all the child policers in the same priority level are directly attached to the root arbiter, each child’s FIR rate is set according to the child’s weight divided by the sum of the active children’s weights multiplied by the available bandwidth at the priority level. The result is that the FIR bucket will mark the appropriate amount of traffic for each child as ?fair?based on the weighted fair output of the policy instance.

The fair/unfair forwarding control in the root parent policer is accomplished by implementing two different discard thresholds for the priority. The first threshold is discard-unfair and the second is discard-all for packet associated with the priority level. As the parent policer PIR bucket fills (due the aggregate forwarded rate being greater than the parent policers PIR decrement rate) and the bucket depth reaches the first threshold, all unfair packets within the priority are discarded. This leaves room in the bucket for the fair packets to be forwarded.
In the more complex case where one or more tiered arbiters are attached at the priority level, the policer control policy instance must consider more than just the child policer weights associated with the attached arbiter. If the arbiter is configured with an aggregate rate limit that its children cannot exceed, the policer control policy instance will switch to calculating the rate each child serviced by the arbiter should receive and enforces that rate using each child policers PIR leaky bucket.

When the child policer PIR leaky bucket is used to limit the bandwidth for the child policer and the child’s PIR bucket discard threshold is reached, packets associated with the child policer are discarded. The child policer’s discarded packets do not consume depth in the child policer’s CIR or FIR buckets. The child policers discarded packets are also prevented from impacting the parent policer and will not consume the aggregate bandwidth managed by the parent policer.

Parent Policier Priority Level Thresholds

As stated above, each child policer is attached either to the root arbiter or explicitly to one of the tier 1 or tier 2 arbiters. When attached directly to the root arbiter, its priority relative to all other child policers is indicated by the parenting level parameter. When attached through one of the tiered arbiters, the parenting hierarchy of the arbiters must be traced through to the ultimate attachment to the root arbiter. The parenting level parameter of the arbiter parented to the root arbiter defines the child policer’s priority level within the parent policer.

The priority level is important since it defines the parent policer discard thresholds that will be applied at the parent policer. The parent policer has 8 levels of strict priority and each priority level has its own discard-unfair and discard-all thresholds. Each priority’s thresholds are larger than the thresholds of the lower priority levels. This ensures that when the parent policer is discarding, it will be priority sensitive.

To visualize the behavior of the parent policer, picture that when the aggregate forwarding rate of all child policers is currently above the decrement rate of the parent PIR leaky bucket, the bucket depth will increase over time. As the bucket depth increases, it will eventually cross the lowest priority’s discard-unfair threshold. If this amount of discard sufficiently lowers the remaining aggregate child policer rate, the parent PIR bucket will hover around this bucket depth. If however, the remaining aggregate child rate is still greater than the decrement rate, the bucket will continue to rise and eventually reach the lowest priority’s discard-all threshold which will cause all packets associated with the priority level to be discarded (fair and unfair). Again, if the remaining aggregate child rate is less than or equal to the bucket decrement rate, the parent PIR bucket will hover around this higher bucket depth. If the remaining aggregate child rate is still higher than the decrement rate, the bucket will continue to rise through the remaining priority level discards until equilibrium is achieved.

As noted above, each child’s rate feeding into the parent policer is governed by the child policer’s PIR bucket decrement rate. The amount of bandwidth the child policer offers to the parent policer will not exceed the child policer’s configured maximum rate.

Root Arbiter’s Parent Policier’s Priority Aggregate Thresholds

Each policer-control-policy root arbiter supports configurable aggregate priority thresholds which are used to control burst tolerance within each priority level. Two values are maintained per priority level; the shared-portion and the fair-portion. The shared-portion represents the amount of parent PIR bucket depth that is allowed to be consumed by both fair and unfair child packets at the priority level. The fair-portion represents the amount of parent PIR bucket depth that only the fair child policer packets may consume within the priority level. It should be noted that the fair and unfair child packets associated with a higher parent policer priority level may also consume the bucket depth set aside for this priority.
While the policy maintains a parent policer default or explicit configurable values for shared-portion and fair-portion within each priority level, it is possible that some priority levels will not be used within the parent policer. Most parent policer use cases require fewer than eight strict priority levels.

In order to derive the actual priority level discard-unfair and discard-all thresholds while only accounting for the actual in-use priority levels, the system maintains a child policer to parent policer association counter per priority level for each policer control policy instance. As a child policer is parented to either the root or a tiered arbiter, the system determines the parent policer priority level for the child policer and increments the association counter for that priority level on the parent policer instance.

The shared-portion for each priority level is affected by the parent policer global min-thresh-separation parameter that defines the minimum separation between any in-use discard thresholds. When more than one child policer is associated with a parent policer priority level, the shared-portion for that priority level will be the current value of min-thresh-separation. When only a single child policer is associated with the parent policer priority level, the priority level’s shared-portion is zero since all packets from the child will be marked fair and the discard-unfair threshold is meaningless. When the association counter is zero, both the shared-portion and the fair-portion for that priority level are zero since neither discard thresholds will be used. Whenever the association counter is greater than 0, the fair-portion for that priority level will be derived from the current value of the priority’s mbs-contribution parameter and the global min-thresh-separation parameter.

Each priority level’s discard-unfair and discard-all thresholds are calculated based on an accumulation of lower priorities shared-portions and fair-portions and the priority level’s own shared-portion and fair-portion. The base threshold value for each priority level is equal to the sum of all lower priority level’s shared-portions and fair-portions. The discard-unfair threshold is the priority level’s base threshold plus the priority level’s shared-portion. The discard-all threshold for the priority level is the priority level’s base threshold plus both the shared-portion and fair-portion values of the priority. As can be seen, an in-use priority level’s thresholds are always greater than the thresholds of lower priority levels.

Policer Control Policy Application

A policer-control-policy may be applied on any Ethernet ingress or egress SAP that is associated with a port (or ports in the case of LAG).

The no form of the command removes a non-associated policer control policy from the system. The command will not execute when policer-name is currently associated with any SAP or subscriber management sub-profile context.

**Default**

```
none
```

**Parameters**

- `policy-name` — Each policer-control-policy must be created with a unique policy name. The name must given as policy-name must adhere to the system policy ASCII naming requirements. If the defined policy-name already exists, the system will enter that policy’s context for editing purposes. If policy-name does not exist, the system will attempt to create a policy with the specified name. Creating a policy may require use of the create parameter when the system is configured for explicit object creation mode.

- `create` — The keyword is required when a new policy is being created and the system is configured for explicit object creation mode.
accounting-policy

**Syntax**

```
accounting-policy acct-policy-id
no accounting-policy
```

**Context**

```
config>service>vpls>spoke-sdp
config>service>vpls>mesh-sdp
config>service>vpls>sap
```

**Description**

This command creates the accounting policy context that can be applied to a SAP or SDP. An accounting policy must be defined before it can be associated with a SAP. If the `policy-id` does not exist, an error message is generated. A maximum of one accounting policy can be associated with a SAP or SDP at one time. Accounting policies are configured in the `config>log` context.

The `no` form of this command removes the accounting policy association from the SAP or SDP, and the accounting policy reverts to the default.

**Default**

Default accounting policy.

**Parameters**

`acct-policy-id` — Enter the accounting `policy-id` as configured in the `config>log>accounting-policy` context.

**Values**

1 — 99

---

app-profile

**Syntax**

```
app-profile app-profile-name
no app-profile
```

**Context**

```
config>service>vpls>spoke-sdp
```

**Description**

This command configures the application profile name.

**Parameters**

`app-profile-name` — Specifies an existing application profile name configured in the `config>app-assure>group>policy` context.

---

collect-stats

**Syntax**

```
[no] collect-stats
```

**Context**

```
config>service>vpls>spoke-sdp
config>service>vpls>mesh-sdp
config>service>vpls>sap
```

**Description**

This command enables accounting and statistical data collection for either the SAP or SDP, network port, or IP interface. When applying accounting policies the data, by default, is collected in the appropriate records and written to the designated billing file.

When the `no collect-stats` command is issued the statistics are still accumulated by the XCM cards. However, the CPU will not obtain the results and write them to the billing file. If a subsequent
**collect-stats** command is issued then the counters written to the billing file include all the traffic while the **no collect-stats** command was in effect.

**Default**  
no collect-stats
VPLS Template Commands

template

Syntax       template
Context       config>service
Description   This is the node for service templates.

vpls-template

Syntax       vpls-template name/id create
[no] vpls-template name/id
Context       config>service>template
Description   This command is used to create a vpls-template to be used to auto-instantiate a range of VPLS services. Only certain existing VPLS attributes specified in the command reference section can be changed in the vpls-template, not in the instantiated VPLS. The following attributes will be automatically set in the instantiated VPLSes (no template configuration necessary) and the operator cannot change these values.

- vpn-id: none
- description: “Service <svc id> auto-generated by control VPLS <svc-id>”
- service-name: “Service <svc-id>” (Auto-generated)
- shutdown: no shutdown

Following existing attributes can be set by the user in the instantiated VPLSes:

- [no] sap

All the other VPLS attributes are not supported.

Parameters

name/id — Specifies the name in ASCII or the template ID.

Values

- name: ASCII string
- ID: [1..2147483647]

vpls-sap-template

Syntax       vpls-sap-template name/id create
[no] vpls-sap-template name/id
Context       config>service>template
Description

This is the command used to create a SAP template to be used in a vpls-template. Only certain existing VPLS SAP attributes can be changed in the vpls-sap-template, not in the instantiated VPLS SAP.

Following SAP attributes will be set in the instantiated saps (no configuration allowed):

- description: “Sap <sap-id> controlled by MVRP service <svc id>” – auto generated
- shutdown: no shutdown

Parameters

name/id — Specifies the name in ASCII or the template ID.

Values

1..2147483647

mac-move-level

Syntax

mac-move-level {primary | secondary}
no mac-move-level

Context

config>service>template>vpls-sap-template

Description

When a sap is instantiated using vpls-sap-template, if the MAC move feature is enabled at VPLS level, the command mac-move-level indicates whether the sap should be populated as primary-port, secondary-port or tertiary-port in the instantiated VPLS.

Default

no mac-move-level; SAP is populated as a tertiary-port

temp-flooding

Syntax

temp-flooding flood-time
no temp-flooding

Context

config>service>vpls
config>service>template>vpls-template

Description

The temporary flooding is designed to minimize failover times by eliminating the time it takes to flush the MAC tables and if MVRP is enabled the time it takes for MVRP registration. Temporary flooding is initiated only upon xSTP TCN reception. During this procedure while the MAC flush takes place the frames received on one of the VPLS SAPs/pseudowires are flooded in a VPLS context which for MVRP case includes also the unregistered MVRP trunk ports. Note that the MAC Flush action is initiated by the STP TCN reception or if MVRP is enabled for the data VPLS, by the reception of a MVRP New message for the SVLAN ID associated with the data VPLS. As soon as the MAC Flush is done, regardless of whether the temp-flooding timer expired or not, traffic will be delivered according to the regular FIB content which may be built from MAC Learning or based on MVRP registrations. This command provides a flood-time value that configures a fixed amount of time, in seconds, during which all traffic is flooded (BUM or known unicast) as a safety mechanism. Once the flood-time expires, traffic will be delivered according to the regular FIB content which may be built from MAC Learning or based on MVRP registrations. The temporary flooding timer should be configured in such a way to allow auxiliary processes like MAC Flush, MMRP and/or MVRP to complete/converge. The temporary flooding behavior applies to regular VPLS, VPLS instantiated with VPLS-template, IVPLS and BVPLS when MMRP is disabled.
The **no** form of the command disables the temporary flooding behavior.

**Default**

no temp-flooding

**Parameters**

- `flood-time` — Specifies the flood time, in seconds.
  
  **Values**
  
  3 — 600
Provider Tunnel Commands

**provider-tunnel**

**Syntax**

```
provider-tunnel
```

**Context**

```
configure>service>vpls
```

**Description**

This command creates the context to configure the use of a P2MP LSP for forwarding Broadcast, Unicast unknown and Multicast (BUM) packets of a VPLS or B-VPLS instance. The P2MP LSP is referred to as the Provider Multicast Service Interface (PMSI).

inclusive

**Syntax**

```
inclusive
```

**Context**

```
configure>service>vpls>provider-tunnel
```

**Description**

This command creates the context to configure the use of a P2MP LSP as the default tree for forwarding Broadcast, Unicast unknown, and Multicast (BUM) packets of a VPLS or B-VPLS instance. The P2MP LSP is referred to, in this case, as the Inclusive Provider Multicast Service Interface (I-PMSI).

When enabled, this feature relies on BGP Auto-Discovery (BGP-AD) or BGP-VPLS to discover the PE nodes participating in a given VPLS/B-VPLS instance. The AD route contains the information required to signal both the point-to-point (P2P) PWs used for forwarding unicast known Ethernet frames and the RSVP or mLDP P2MP LSP used to forward the BUM frames.

The root node signals the RSVP P2MP LSP based on an LSP template associated with the I-PMSI at configuration time. The leaf node will join automatically the P2MP LSP, which matches the I-PMSI tunnel information discovered via BGP.

With a mLDP I-PMSI, each leaf node will initiate the signaling of the mLDP P2MP LSP upstream using the P2MP FEC information in the I-PMSI tunnel information discovered via BGP-AD.

If IGMP or PIM snooping are configured on the VPLS/B-VPLS instance, multicast packets matching a L2 multicast Forwarding Information Base (FIB) record will also be forwarded over the P2MP LSP.

The user enables the use of an RSVP P2MP LSP as the I-PMSI for forwarding Ethernet BUM and IP multicast packets in a VPLS/B-VPLS instance using the following commands:

```
config>service>vpls [b-vpls]>provider-tunnel>inclusive>rsvp>lsp-template p2mp-lsp-template-name
```

The user enables the use of an LDP P2MP LSP as the I-PMSI for forwarding Ethernet BUM and IP multicast packets in a VPLS instance using the following command:

```
config>service>vpls [b-vpls]>provider-tunnel>inclusive>mldp
```

After the user performs a **no shutdown** under the context of the inclusive node and the expiration of a delay timer, BUM packets will be forwarded over an automatically signaled mLDP P2MP LSP or over an automatically signaled instance of the RSVP P2MP LSP specified in the LSP template.

The user can specify if the node is both root and leaf in the VPLS instance:
The `root-and-leaf` command is required otherwise this node will behave as a leaf only node by default. When the node is leaf only for the I-PMSI of type P2MP RSVP LSP, no PMSI Tunnel Attribute is included in BGP-AD route update messages and thus no RSVP P2MP LSP is signaled but the node can join RSVP P2MP LSP rooted at other PE nodes participating in this VPLS/B-VPLS service. Note that the user must still configure a LSP template even if the node is a leaf only. For the I-PMSI of type mLDP, the leaf-only node will join I-PMSI rooted at other nodes it discovered but will not include a PMSI Tunnel Attribute in BGP-AD route update messages. This way a leaf only node will forward packets to other nodes in the VPLS/B-VPLS using the point-to-point spoke-sdp’s.

Note that BGP-AD must have been enabled in this VPLS/B-VPLS instance or the execution of the "no shutdown" command under the context of the inclusive node is failed and the I-PMSI will not come up.

Any change to the parameters of the I-PMSI, such as disabling the P2MP LSP type or changing the LSP template requires that the inclusive node be first shutdown. The LSP template is configured in MPLS.

If the P2MP LSP instance goes down, VPLS/B-VPLS immediately reverts the forwarding of BUM packets to the P2P PWs. The user can however restore at any time the forwarding of BUM packets over the P2P PWs by performing a `shutdown` under the context of the inclusive node.

This feature is supported with VPLS, H-VPLS, and B-VPLS. It is not supported with I-VPLS and Routed VPLS.

data-delay-interval

**Syntax**

```
data-delay-interval seconds
no data-delay-interval
```

**Context**

```
configure>service>vpls>provider-tunnel>inclusive
```

**Description**

This command configures the I-PMSI data delay timer.

This delay timer is intended to allow time for the RSVP control plane to signal and bring up the S2L sub-LSP to each destination PE participating in the VPLS/B-VPLS service. The delay timer is started as soon as the P2MP LSP instance becomes operationally up after the user performed a 'no shutdown' under the inclusive node, i.e., as soon as the first S2L sub-LSP is up. In general, it is started when the P2MP LSP instance transitions from the operationally down state to the up state.

For a mLDP P2MP LSP, the delay timer is started as soon as the P2MP FEC corresponding to the I-PMSI is resolved and installed at the root node. Note that the user must factor in the value configured in the data-delay-interval at the root node any delay configured in IGP-LDP sync timer (config>router>interface>ldp-sync-timer) on interfaces over the network. This is because the mLDP P2MP LSP may move to a different interface at the expiry of this timer since the routing upstream of the LDP Label Mapping message may change when this timer expires and the interface metric is restored.

At the expiry of this timer, the VPLS/B-VPLS will begin forwarding of BUM packets over the P2MP LSP instance even if not all the S2L paths are up.

The `no` version of this command re-instates the default value for this delay timer.

**Parameters**

`seconds` — The delay time value in seconds.
mldp

 values 3—180 seconds
 default 15 seconds

Syntax [no] mldp
Context configure>service>vpls>provider-tunnel>inclusive
Description This command creates the context to configure the parameters of an LDP P2MP LSP used for forwarding Broadcast, Unicast unknown and Multicast (BUM) packets of a VPLS or B-VPLS instance.

root-and-leaf

Syntax [no] root-and-leaf
Context configure>service>vpls>provider-tunnel>inclusive
Description This command configures the node to operate as both root and leaf of the I-PMSI in a given VPLS/B-VPLS instance.

By default, a node will behave as a leaf only node. When the node is leaf only for the I-PMSI of type P2MP RSVP LSP, no PMSI Tunnel Attribute is included in BGP-AD route update messages and thus no RSVP P2MP LSP is signaled but the node can join RSVP P2MP LSP rooted at other PE nodes participating in this VPLS/B-VPLS service. Note that the user must still configure a LSP template even if the node is a leaf only.

For the I-PMSI of type mLDP, the leaf-only node will join I-PMSI rooted at other nodes it discovered but will not include a PMSI Tunnel Attribute in BGP-AD route update messages. This way a leaf only node will forward packets to other nodes in the VPLS/B-VPLS using the point-to-point spoke-sdp’s.

The no version of this command re-instates the default value.

rsvp

Syntax [no] rsvp
Context configure>service>vpls>provider-tunnel>inclusive
Description This command creates the context to configure the parameters of an RSVP P2MP LSP used for forwarding Broadcast, Unicast unknown and Multicast (BUM) packets of a VPLS or B-VPLS instance.
lsp-template

Syntax

```
lsp-template p2mp-lsp-template-name
no lsp-template
```

Context

configure>service>vpls>provider-tunnel>inclusive>rsvp

Description

This command specifies the template name of the RSVP P2MP LSP instance to be used by the leaf node or the root-and-leaf node that participates in BGP-AD VPLS. The P2MP LSP is referred to as the Inclusive Provider Multicast Service Interface (I-PMSI).

After the user performs a “no shutdown” under the context of the inclusive node and the delay timer expires, BUM packets will be forwarded over an automatically signaled instance of the RSVP P2MP LSP specified in the LSP template.

The no version of this command removes the P2MP LSP template from the I-PMIS configuration.

Parameters

```
p2mp-lsp-template-name — The name of the P2MP LSP template. This is a string of 32 characters maximum.
```

Default

None
VPLS SDP Commands

mesh-sdp

Syntax

mesh-sdp  sdp-id[;vc-id] [vc-type {ether | vlan}]
nomesh-sdp  sdp-id[;vc-id]

Context

config>service>vpls

Description

This command binds a VPLS service to an existing Service Distribution Point (SDP). Mesh SDPs bound to a service are logically treated like a single bridge “port” for flooded traffic where flooded traffic received on any mesh SDP on the service is replicated to other “ports” (spoke SDPs and SAPs) and not transmitted on any mesh SDPs.

Note that this command creates a binding between a service and an SDP. The SDP has an operational state which determines the operational state of the SDP within the service. For example, if the SDP is administratively or operationally down, the SDP for the service will be down.

The SDP must already be defined in the config>service>sdp context in order to associate the SDP with a valid service. If the sdp sdp-id is not already configured, an error message is generated. If the sdp-id does exist, a binding between that sdp-id and the service is created.

SDPs must be explicitly associated and bound to a service. If an SDP is not bound to a service, no far-end devices can participate in the service.

The no form of this command removes the SDP binding from the service. The SDP configuration is not affected; only the binding of the SDP to a service. Once removed, no packets are forwarded to the far-end router.

Default

No sdp-id is bound to a service.

Special Cases

VPLS — Several SDPs can be bound to a VPLS. Each SDP must be destined to a different router. If two sdp-id bindings terminate on the same router, an error occurs and the second SDP is binding is rejected.

Parameters

sdp-id — The SDP identifier.

Values

1 — 17407

vc-id — The virtual circuit identifier. This value is used to validate the VC ID portion of each mesh SDP binding defined in the service. The default value of this object is equal to the service ID.

Values

1 — 4294967295

vc-type — This command overrides the default VC type signaled for the spoke or mesh binding to the far end of the SDP. The VC type is a 15 bit-quantity containing a value which represents the type of VC. The actual signaling of the VC type depends on the signaling parameter defined for the SDP. If signaling is disabled, the vc-type command can still be used to define the dot1q value expected by the far-end provider equipment. A change of the bindings VC type causes the binding to signal the new VC type to the far end when signaling is enabled.

VC types are derived according to IETF draft-martini-l2circuit-trans-mpls.

• The VC type value for Ethernet is 0x0005.
• The VC type value for an Ethernet VLAN is 0x0004.
ether — Defines the VC type as Ethernet. The ethernet and vlan keywords are mutually exclusive. When the VC type is not defined then the default is Ethernet for spoke SDP bindings. Defining Ethernet is the same as executing no vc-type and restores the default VC type for the spoke SDP binding. (hex 5)

vlan — Defines the VC type as VLAN. The ethernet and vlan keywords are mutually exclusive. When the VC type is not defined then the default is Ethernet for mesh SDP bindings.

spoke-sdp

Syntax

spoke-sdp sdp-id[:vc-id] [vc-type {ether | vlan}] [split-horizon-group group-name] endpoint [no-endpoint]
no spoke-sdp sdp-id[:vc-id]

Context config>service>vpls

Description

This command binds a service to an existing Service Distribution Point (SDP). A spoke SDP is treated like the equivalent of a traditional bridge “port” where flooded traffic received on the spoke SDP is replicated on all other “ports” (other spoke and mesh SDPs or SAPs) and not transmitted on the port it was received.

The SDP has an operational state which determines the operational state of the SDP within the service. For example, if the SDP is administratively or operationally down, the SDP for the service will be down.

The SDP must already be defined in the config>service>sdp context in order to associate an SDP with a VPLS service. If the sdp sdp-id is not already configured, an error message is generated. If the sdp-id does exist, a binding between that sdp-id and the service is created.

SDPs must be explicitly associated and bound to a service. If an SDP is not bound to a service, no far-end devices can participate in the service.

The no form of this command removes the SDP binding from the service. The SDP configuration is not affected; only the binding of the SDP to a service. Once removed, no packets are forwarded to the far-end router.

Default No sdp-id is bound to a service.

Special Cases VPLS — Several SDPs can be bound to a VPLS service. Each SDP must use unique vc-ids. An error message is generated if two SDP bindings with identical vc-ids terminate on the same router. Split horizon groups can only be created in the scope of a VPLS service.

Parameters

sdp-id — The SDP identifier.

Values 1 — 17407

vc-id — The virtual circuit identifier.

Values 1 — 4294967295

vc-type — This command overrides the default VC type signaled for the spoke or mesh binding to the far end of the SDP. The VC type is a 15 bit-quantity containing a value which represents the type of VC. The actual signaling of the VC type depends on the signaling parameter defined for the SDP. If signaling is disabled, the vc-type command can still be used to define the dot1q value expected by the far-end provider equipment. A change of the bindings VC type causes the
binding to signal the new VC type to the far end when signaling is enabled. VC types are derived according to IETF draft-martini-l2circuit-trans-mpls.

- The VC type value for Ethernet is 0x0005.
- The VC type value for an Ethernet VLAN is 0x0004.

**Values**

ether — Defines the VC type as Ethernet. The ethernet and vlan keywords are mutually exclusive. When the VC type is not defined then the default is Ethernet for spoke SDP bindings. Defining Ethernet is the same as executing no vc-type and restores the default VC type for the spoke SDP binding. (hex 5)

vlan — Defines the VC type as VLAN. The ethernet and vlan keywords are mutually exclusive. When the VC type is not defined then the default is Ethernet for spoke SDP bindings. The VLAN VC-type requires at least one dot1Q tag within each encapsulated Ethernet packet transmitted to the far end.

**split-horizon-group group-name** — Specifies the name of the split horizon group to which the SDP belongs.

**endpoint** — Specifies the service endpoint to which this SDP bind is attached. The service ID of the SDP binding must match the service ID of the service endpoint.

**no endpoint** — removes the association of a spoke SDP with an explicit endpoint name.

---

**control-word**

**Syntax**

[no] control word

**Context**

config>service>vpls>mesh-sdp
config>service>vpls>spoke-sdp

**Description**

This command enables the use of the control word on pseudowire packets in VPLS and enables the use of the control word individually on each mesh SDP or spoke SDP. By default, the control word is disabled. When the control word is enabled, all VPLS packets, including the BPDUs, are encapsulated with the control word when sent over the pseudowire. The T-LDP control plane behavior is the same as in the implementation of control word for VLL services. The configuration for the two directions of the Ethernet pseudowire should match. The no form of the command reverts the mesh SDP or spoke SDP to the default behavior of not using the control word. The control word must be enabled to use MPLS-TP OAM on a static spoke-sdp terminating in a VPLS.

**Default**

no control word

---

**egress**

**Syntax**

egress

**Context**

config>service>vpls>mesh-sdp
config>service>vpls>spoke-sdp

**Description**

This command configures the egress SDP context.
**Syntax**

```
qos network-policy-id port-redirect-group queue-group-name instance instance-id
no qos [network-policy-id]
```

**Context**

- configure>service>apipe>spoke-sdp>egress
- configure>service>cpipe>spoke-sdp>egress
- configure>service>epipe>spoke-sdp>egress
- configure>service>fpipe>spoke-sdp>egress
- configure>service>ipipe>spoke-sdp>egress
- config>service>vplspoke-sdp>egress
- config>service>vplspmesh-sdp>egress
- config>service>pw-template>egress
- config>service>vprn>interface>spoke-sdp>egress
- config>service>ies>interface>spoke-sdp>egress

**Description**

This command is used to redirect pseudowire packets to an egress port queue-group for the purpose of shaping.

The egress pseudowire shaping provisioning model allows the mapping of one or more pseudowires to the same instance of queues, or policers and queues, which are defined in the queue-group template.

Operationally, the provisioning model consists of the following steps:

1. Create an egress queue-group template and configure queues only or policers and queues for each FC that needs to be redirected.
2. Apply the queue-group template to the network egress context of all ports where there exists a network IP interface on which the pseudowire packets can be forwarded. This creates one instance of the template on the egress of the port. One or more instances of the same template can be created.
3. Configure FC-to-policer or FC-to-queue mappings together with the redirect to a queue-group in the egress context of a network QoS policy. No queue-group name is specified in this step, which means the same network QoS policy can redirect different pseudowires to different queue-group templates.
4. Apply this network QoS policy to the egress context of a spoke-SPD inside a service or to the egress context of a pseudowire template and specify the redirect queue-group name.

One or more spoke-SPDs can have their FCs redirected to use queues only or queues and policers in the same queue-group instance.

The following are the constraints and rules of this provisioning model:

1. When a pseudowire FC is redirected to use a queue or a policer and a queue in a queue-group and the queue-group name does not exist, the association is failed at the time the user associates the egress context of a spoke-SPD to the named queue-group. In such a case, the pseudowire packet will be fed directly to the corresponding egress queue for that FC used by the IP network interface on which the pseudowire packet is forwarded. This queue can be a queue-group queue, or the egress shared queue for that FC defined in the network-queue policy applied to the egress of this port. This is the existing implementation and default behavior for a pseudowire packet.
2. When a pseudowire FC is redirected to use a queue or a policer, and a queue in a queue-group and the queue-group name exists, but the policer-id and/or the queue-id is not defined
in the queue-group template, the association is failed at the time the user associates the egress context of a spoke-SPD to the named queue-group. In such a case, the pseudowire packet will be fed directly to the corresponding egress queue for that FC used by the IP network interface the pseudowire packet is forwarded on.

3. When a pseudowire FC is redirected to use a queue, or a policer and a queue in a queue-group, and the queue-group name exists and the policer-id or policer-id plus queue-id exist, it is not required to check that an instance of that queue-group exists in all egress network ports which have network IP interfaces. The handling of this is dealt with in the data path as follows:

a. When a pseudowire packet for that FC is forwarded and an instance of the referenced queue-group name exists on that egress port, the packet is processed by the queue-group policer and will then be fed to the queue-group queue.

b. When a pseudowire packet for that FC is forwarded and an instance of the referenced queue-group name does not exist on that egress port, the pseudowire packet will be fed directly to the corresponding egress shared queue for that FC defined in the network-queue policy applied to the egress of this port.

4. If a network QoS policy is applied to the egress context of a pseudowire, any pseudowire FC, which is not explicitly redirected in the network QoS policy, will have the corresponding packets feed directly the corresponding the egress shared queue for that FC defined in the network-queue policy applied to the egress of this port.

When the queue-group name the pseudowire is redirected to exists and the redirection succeeds, the marking of the packet DEI/dot1.p/DSCP and the tunnel DEI/dot1.p/DSCP/EXP is performed; according to the relevant mappings of the (FC, profile) in the egress context of the network QoS policy applied to the pseudowire. This is true regardless, whether an instance of the queue-group exists or not on the egress port to which the pseudowire packet is forwarded. If the packet profile value changed due to egress child policer CIR profiling, the new profile value is used to mark the packet DEI/dot1.p and the tunnel DEI/dot1.p/EXP, but the DSCP is not modified by the policer operation.

When the queue-group name the pseudowire is redirected does not exist, the redirection command is failed. In this case, the marking of the packet DEI/dot1.p/DSCP and the tunnel DEI/dot1.p/DSCP/EXP fields is performed according to the relevant commands in the egress context of the network QoS policy applied to the network IP interface to which the pseudowire packet is forwarded.

The no version of this command removes the redirection of the pseudowire to the queue-group.

**Parameters**

- `network-policy-id` — Specifies the network policy identification. The value uniquely identifies the policy on the system.
  
  **Values**
  
  1 — 65535

- `queue-redirect-group` `queue-group-name` — This optional parameter specifies that the `queue-group-name` will be used for all egress forwarding class redirections within the network QoS policy ID. The specified `queue-group-name` must exist as a port egress queue group on the port associated with the IP interface.

- `egress-instance` `instance-id` — Specifies the identification of a specific instance of the queue-group.
  
  **Values**
  
  1 — 16384
ingress

**Syntax**

```plaintext
ingress
```

**Context**

```plaintext
config>service>vpls>mesh-sdp
config>service>vpls>spoke-sdp
```

**Description**

This command configures the ingress SDP context.

qos

**Syntax**

```plaintext
qos network-policy-id fp-redirect-group queue-group-name instance instance-id
no qos
```

**Context**

```plaintext
configure>service>apipe>spoke-sdp>ingress
configure>service>cpipe>spoke-sdp>ingress
configure>service>epipe>spoke-sdp>ingress
configure>service>fpipe>spoke-sdp>ingress
configure>service>ipipe>spoke-sdp>ingress
configure>service>vpls>spoke-sdp>ingress
configure>service>vpls>mesh-sdp>ingress
configure>service>pw-template>ingress
configure>service>vprn>interface>spoke-sdp>ingress
configure>service>ies>interface>spoke-sdp>ingress
```

**Description**

This command is used to redirect pseudowire packets to an ingress forwarding plane queue-group for the purpose of rate-limiting.

The ingress pseudowire rate-limiting feature uses a policer in queue-group provisioning model. This model allows the mapping of one or more pseudowires to the same instance of policers, which are defined in a queue-group template.

Operationally, the provisioning model in the case of the ingress pseudowire shaping feature consists of the following steps:

1. Create an ingress queue-group template and configure policers for each FC that needs to be redirected and optionally, for each traffic type (unicast or multicast).
2. Apply the queue-group template to the network ingress forwarding plane where there exists a network IP interface to which the pseudowire packets can be received. This creates one instance of the template on the ingress of the FP. One or more instances of the same template can be created.
3. Configure FC-to-policer mappings together with the policer redirect to a queue-group in the ingress context of a network QoS policy. No queue-group name is specified in this step, which means the same network QoS policy can redirect different pseudowires to different queue-group templates.
4. Apply this network QoS policy to the ingress context of a spoke-SDP inside a service, or to the ingress context of a pseudowire template, and specify the redirect queue-group name.
5. One or more spoke-SDPs can have their FCs redirected to use policers in the same policer queue-group instance.
The following are the constraints and rules of this provisioning model when used in the ingress pseudowire rate-limiting feature:

1. When a pseudowire FC is redirected to use a policer in a named policer queue-group and the queue-group name does not exist, the association is failed at the time the user associates the ingress context of a spoke-SDP to the named queue-group. In such a case, the pseudowire packet will feed directly the ingress network shared queue for that FC defined in the network-queue policy applied to the ingress of the MDA/FP.

2. When a pseudowire FC is redirected to use a policer in a named policer queue-group and the queue-group name exists but the policer-id is not defined in the queue-group template, the association is failed at the time the user associates the ingress context of a spoke-SDP to the named queue-group. In such a case, the pseudowire packet will feed directly the ingress network shared queue for that FC defined in the network-queue policy applied to the ingress of the MDA/FP.

3. When a pseudowire FC is redirected to use a policer in a named policer queue-group and the queue-group name exists and the policer-id is defined in the queue-group template, it is not required to check that an instance of that queue-group exists in all ingress FPs which have network IP interfaces. The handling of this is dealt with in the data path as follows:
   a. When a pseudowire packet for that FC is received and an instance of the referenced queue-group name exists on that FP, the packet is processed by the policer and will then feed the per-FP ingress shared queues referred to as policer-output-queues.
   b. When a pseudowire packet for that FC is received and an instance of the referenced queue-group name does not exist on that FP, the pseudowire packets will be fed directly into the corresponding ingress network shared queue for that FC defined in the network-queue policy applied to the ingress of the MDA/FP.

4. If a network QoS policy is applied to the ingress context of a pseudowire, any pseudowire FC which is not explicitly redirected in the network QoS policy will have the corresponding packets feed directly the ingress network shared queue for that FC defined in the network-queue policy applied to the ingress of the MDA/FP.

5. If no network QoS policy is applied to the ingress context of the pseudowire, then all packets of the pseudowire will feed:
   a. the ingress network shared queue for the packet FC defined in the network-queue policy applied to the ingress of the MDA/FP. This is the default behavior.
   b. a queue-group policer followed by the per-FP ingress shared queues referred to as policer-output-queues if the ingress context of the network IP interface from which the packet is received is redirected to a queue-group (csc-policing). The only exceptions to this behavior are for packets received from a IES/VPRN spoke interface and from an R-VPLS spoke-SPD, which is forwarded to the R-VPLS IP interface. In these two cases, the ingress network shared queue for the packet FC defined in the network-queue policy applied to the ingress of the MDA/FP is used.

When a pseudowire is redirected to use a policer queue-group, the classification of the packet for the purpose of FC and profile determination is performed according to default classification rule or the QoS filters defined in the ingress context of the network QoS policy applied to the pseudowire. This is true regardless of whether an instance of the named policer queue-group exists on the ingress FP on which the pseudowire packet is received. The user can apply a QoS filter matching the dot1.p in the VLAN tag corresponding to the Ethernet port encapsulation, the EXP in the outer label when the tunnel is an LSP, the DSCP in the IP header if the tunnel encapsulation is GRE, and the DSCP in the
payload IP header if the user enabled the `ler-use-dscp` option and the pseudowire terminates in IES or VPRN service (spoke-interface).

When the policer queue-group name the pseudowire is redirected does not exist, the redirection command is failed. In this case, the packet classification is performed according to default classification rule or the QoS filters defined in the ingress context of the network QoS policy applied to the network IP interface on which the pseudowire packet is received.

The `no` version of this command removes the redirection of the pseudowire to the queue-group.

**Parameters**

- **network-policy-id** — Specifies the network policy identification. The value uniquely identifies the policy on the system.
  - Values 1 — 65535

- **fp-redirect-group queue-group-name** — Specifies the name of the queue group template up to 32 characters in length.

- **ingress-instance instance-id** — Specifies the identification of a specific instance of the queue-group.
  - Values 1 — 16384

**mfib-allowed-mda-destinations**

**Syntax**

```
mfib-allowed-mda-destinations
```

**Context**

```
config>service>vpls>mesh-sdp>egress
config>service>vpls>spoke-sdp>egress
```

**Description**

This command enables the context to configure MFIB-allowed MDA destinations.

The allowed-mda-destinations node and the corresponding `mda` command are used on spoke and mesh SDP bindings to provide a list of MDA destinations in the chassis that are allowed as destinations for multicast streams represented by [*,g] and [s,g] multicast flooding records on the VPLS service. The MDA list only applies to IP multicast forwarding when IGMP snooping is enabled on the VPLS service. The MDA list has no effect on normal VPLS flooding such as broadcast, L2 multicast, unknown destinations or non-snooped IP multicast.

At the IGMP snooping level, a spoke or mesh SDP binding is included in the flooding domain for an IP multicast stream when it has either been defined as a multicast router port, received a IGMP query through the binding or has been associated with the multicast stream through an IGMP request by a host over the binding. Due to the dynamic nature of the way that a spoke or mesh SDP binding is associated with one or more egress network IP interfaces, the system treats the binding as appearing on all network ports. This causes all possible network destinations in the switch fabric to be included in the multicast streams flooding domain. The MDA destination list provides a simple mechanism that narrows the IP multicast switch fabric destinations for the spoke or mesh SDP binding.

If no MDAs are defined within the allowed-mda-destinations node, the system operates normally and will forward IP multicast flooded packets associated with the spoke or mesh SDP binding to all switch fabric taps containing network IP interfaces.

The MDA inclusion list should include all MDAs that the SDP binding may attempt to forward through. A simple way to ensure that an MDA that is not included in the list is not being used by the binding is to define the SDP the binding is associated with as MPLS and use an RSVP-TE LSP with a strict egress hop. The MDA associated with the IP interface defined as the strict egress hop should be
present in the inclusion list. If the inclusion list does not currently contain the MDA that the binding is forwarding through, the multicast packets will not reach the destination represented by the binding.

By default, the MDA inclusion list is empty.

If an MDA is removed from the list, the MDA is automatically removed from the flooding domain of any snooped IP multicast streams associated with a destination on the MDA unless the MDA was the last MDA on the inclusion list. Once the inclusion list is empty, all MDAs are eligible for snooped IP multicast flooding for streams associated with the SDP binding.

**mda**

**Syntax**

```plaintext
[no] mda mda-id
```

**Context**

config>service>vpls>mesh-sdp>egress>mfib-allowed-mda-destinations
cfg>service>vpls>spoke-sdp>egress>mfib-allowed-mda-destinations

**Description**

This command specifies an MFIB-allowed MDA destination for an SDP binding configured in the system.

**Parameters**

- `mda-id` — Specifies an MFIB-allowed MDA destination.

  **Values**
  
  - slot/mda: 1 — 10
  - mda: 1 — 2

**vc-label**

**Syntax**

```plaintext
[no] vc-label vc-label
```

**Context**

config>service>vpls>mesh-sdp>egress
cfg>service>vpls>spoke-sdp>egress

**Description**

This command configures the egress VC label.

**Parameters**

- `vc-label` — A VC egress value that indicates a specific connection.

  **Values**
  
  16 — 1048575

**vc-label**

**Syntax**

```plaintext
[no] vc-label vc-label
```

**Context**

config>service>vpls>mesh-sdp>ingress
cfg>service>vpls>spoke-sdp>ingress

**Description**

This command configures the ingress VC label.

**Parameters**

- `vc-label` — A VC ingress value that indicates a specific connection.

  **Values**
  
  2048 — 18431
static-mac

**Syntax**

```
[no] static-mac ieee-mac-address
```

**Context**

```
config>service>vpls>mesh-sdp
config>service>vpls>spoke-sdp
```

**Description**

This command creates a remote static MAC entry in the Virtual Private LAN Service (VPLS) forwarding database (FDB) associated with the Service Distribution Point (SDP).

In a VPLS service, MAC addresses are associated with a Service Access Point (SAP) or with a Service Distribution Point (SDP). MACs associated with a SAP are classified as local MACs, and MACs associated with an SDP are remote MACs.

Remote static MAC entries create a permanent MAC address to SDP association in the forwarding database for the VPLS instance so that MAC address will not be learned on the edge device.

Note that static MAC definitions on one edge device are not propagated to other edge devices participating in the VPLS instance, that is, each edge device has an independent forwarding database for the VPLS.

Only one static MAC entry (local or remote) can be defined per MAC address per VPLS instance.

The `no` form of this command deletes the static MAC entry with the specified MAC address associated with the SDP from the VPLS forwarding database.

**Default**

`none`

**Parameters**

- `ieee-mac-address` — Specifies the 48-bit MAC address for the static ARP in the form `aa:bb:cc:dd:ee:ff` or `aa-bb-cc-dd-ee-ff` where `aa`, `bb`, `cc`, `dd`, `ee` and `ff` are hexadecimal numbers. Allowed values are any non-broadcast, non-multicast MAC and non-IEEE reserved MAC addresses.

transit-policy

**Syntax**

```
transit-policy prefix prefix-aasub-policy-id
no transit-policy
```

**Context**

```
config>service>vpls>spoke-sdp
```

**Description**

This command assigns a transit policy id.

The `no` form of the command removes the transit policy ID from the spoke SDP configuration.

**Default**

`no transit-policy`

**Parameters**

- `prefix-aasub-policy-id` — Specifies the transit policy ID.

  **Values**

  `1` — `65535`

vlan-vc-tag

**Syntax**

```
vlan-vc-tag 0..4094
no vlan-vc-tag [0..4094]
```
Context  config>service>vpls>spoke-sdp
          config>service>vpls>mesh-sdp

Description  This command specifies an explicit Dot1q value used when encapsulating to the SDP far end. When
              signaling is enabled between the near and far end, the configured Dot1q tag can be overridden by a
              received TLV specifying the Dot1q value expected by the far end. This signaled value must be stored
              as the remote signaled Dot1q value for the binding. The provisioned local Dot1q tag must be stored as
              the administrative Dot1q value for the binding.

              When the Dot1q tag is not defined, the default value of zero is stored as the administrative dot1q
              value. Setting the value to zero is equivalent to not specifying the value.

              The no form of this command disables the command.

Default  no vlan-vc-tag

Parameters  0..4094 — Specifies a valid VLAN identifier to bind an 802.1Q VLAN tag ID.
VPLS Multicast Commands

fast-leave

Syntax  
[no] fast-leave

Context  
config>service>vpls>sap>igmp-snooping  
config>service>vpls>sap>mld-snooping  
config>service>vpls>spoke-sdp>igmp-snooping  
config>service>vpls>mesh-sdp>igmp-snooping

Description  
This command enables fast leave. When IGMP fast leave processing is enabled, the SR OS router will immediately remove a SAP or SDP from the multicast group when it detects an IGMP “leave” on that SAP or SDP. Fast leave processing allows the switch to remove a SAP or SDP that sends a ‘leave’ from the forwarding table without first sending out group-specific queries to the SAP or SDP, and thus speeds up the process of changing channels ('zapping').

Fast leave should only be enabled when there is a single receiver present on the SAP or SDP. When fast leave is enabled, the configured last-member-query-interval value is ignored.

Default  
no fast-leave

from-vpls

Syntax  
from-vpls vpls-id
no from-vpls

Context  
config>service>vpls>sap>igmp-snooping>mvr  
config>service>vpls>sap>mld-snooping>mvr

Description  
This command configures the VPLS from which multicast traffic is copied upon receipt of an IGMP join request. IGMP snooping must be enabled on the MVR VPLS.

Default  
no from-vpls

Parameters  

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>vpls-id</td>
<td>service-id: 1 — 2147483648</td>
</tr>
</tbody>
</table>


group

Syntax  
[no] group grp-address

Context  
config>service>vpls>sap>igmp-snooping>static  
config>service>vpls>spoke-sdp>snooping>static  
config>service>vpls>mesh-sdp>snooping>static
VPLS Multicast Commands

**Description**
This command adds a static multicast group either as a (*, g). When a static IGMP group is added, multicast data for that (*,g) or (s,g) is forwarded to the specific SAP or SDP without receiving any membership report from a host.

**Default**
none

**Parameters**
*grp-address* — Specifies an IGMP multicast group address that receives data on an interface. The IP address must be unique for each static group.

**group-policy**

**Syntax**
group-policy *policy-name*
no group-policy

**Context**
config>service>vpls>sap>igmp-snooping>mvr
config>service>vpls>mld-snooping>mvr

**Description**
This command identifies filter policy of multicast groups to be applied to this VPLS entity. The sources of the multicast traffic must be a member of the VPLS.

The *no* form of the command removes the policy association from the VPLS configuration.

**Default**
No group policy is specified.

**Parameters**
*policy-name* — The group policy name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes. Routing policies are configured in the config>router>policy-options context. The router policy must be defined before it can be imported. For details on IGMP policies, see section “Enabling IGMP group membership report filtering” in the OS Router Configuration Guide.

**fault-propagation-bmac**

**Syntax**
fault-propagation-bmac [mac-name | ieee-address] [create]
no fault-propagation-bmac [mac-name | ieee-address]

**Context**
config>service>vpls>mesh-sdp
config>service>vpls>sap
config>service>vpls>spoke-sdp

**Description**
This command configures associated BMAC addresses for fault propagation on a B-VPLS SAP or SDP binding. The statement can appear up to four times in the configuration to support four remote BMAC addresses in the same remote B-VPLS. The configured VPLS must be a B-VPLS.

The *no* form of the command removes the specified MAC name or MAC address from the list of Fault Propagation BMAC addresses associated with the SAP (or SDP).

**Parameters**
*mac-name* — Specifies a (predefined) MAC name to associate with the SAP or SDP, indirectly specifying a Fault Propagation BMAC address. Up to 32 characters in length.
*ieee-address* — Specifies a MAC address to associate with the SAP or SDP, directly specifying a Fault Propagation BMAC address. The value should be input in either a *xx:* *xx:* *xx:* *xx:* *xx:* or *xx:* *xx:* *xx:* *xx:* *xx:* format.

**feature**

**Syntax**

```
[no] feature
```

**Context**

```
config>service>vpls>sap
config>service>ies|vprn
```

**Description**

This command enables feature.

**force-vlan-vc-forwarding**

**Syntax**

```
[no] force-vlan-vc-forwarding
```

**Context**

```
config>service>epipe>spoke-sdp
config>service>vpls>mesh-sdp
config>service>vpls>spoke-sdp
```

This command forces vc-vlan-type forwarding in the data path for spoke/mesh SDPs which have either vc-type. This command is not allowed on vlan-vc-type SDPs.

The *no* form of this command sets default behavior.

**Default**

disabled

**hash-label**

**Syntax**

```
hash-label [signal-capability]
no hash-label
```

**Context**

```
config>service>vpls>spoke-sdp
config>service>vpls>mesh-sdp
```

**Description**

This command enables the use of the hash label on a VLL, VPRN or VPLS service bound to LDP or RSVP SDP as well as to a VPRN service using the autobind mode with the *ldp*, *rsvp-te*, or *mpls* options. This feature is not supported on a service bound to a GRE SDP. This feature is also not supported on multicast packets forwarded using RSVP P2MP LPS or mLDP LSP in both the base router instance and in the multicast VPN (mVPN) instance. It is, however, supported when forwarding multicast packets using an IES/VPRN spoke-interface.

When this feature is enabled, the ingress data path is modified such that the result of the hash on the packet header is communicated to the egress data path for use as the value of the label field of the hash label. The egress data path appends the hash label at the bottom of the stack (BoS) and sets the S-bit to one (1).

In order to allow applications where the egress LER infers the presence of the hash label implicitly from the value of the label, the Most Significant Bit (MSB) of the result of the hash is set before
copying into the Hash Label. This means that the value of the hash label will always be in the range [524,288 - 1,048,575] and will not overlap with the signaled/static LSP and signaled/static service label ranges. This also guarantees that the hash label will not match a value in the reserved label range.

The (unmodified) result of the hash continues to be used for the purpose of ECMP and LAG spraying of packets locally on the ingress LER. Note, however, that for VLL services, the result of the hash is overwritten and the ECMP and LAG spraying will be based on service-id when ingress SAP shared queuing is not enabled. However, the hash label will still reflect the result of the hash such that an LSR can use it to perform fine grained load balancing of VLL pseudowire packets.

Packets generated in CPM and that are forwarded labeled within the context of a service (for example, OAM packets) must also include a Hash Label at the BoS and set the S-bit accordingly. The TTL of the hash label is set to a value of 0.

The user enables the signaling of the hash-label capability under a VLL spoke-sdp, a VPLS spoke-sdp or mesh-sdp, or an IES/VPRN spoke interface by adding the `signal-capability` option. In this case, the decision whether to insert the hash label on the user and control plane packets by the local PE is solely determined by the outcome of the signaling process and can override the local PE configuration. The following are the procedures:

- The 7950 SR local PE will insert the flow label interface parameters sub-TLV with F=1 in the pseudowire ID FEC element in the label mapping message for that spoke-sdp or mesh-sdp.
- If the remote PE includes this sub-TLV with F=1 or F=0, then local PE must insert the hash label in the user and control plane packets.
- If remote PE does not include this sub-TLV (for example, it does not support it, or it is supported but the user did not enable the `hash-label` option or the `signal-capability` option), then the local PE establishes the pseudowire but must not insert the hash label in the user and control packets over that spoke-sdp or mesh-sdp. If the remote PE does not support the `signal-capability` option, then there are a couple of possible outcomes:
  - If the `hash-label` option was enabled on the local configuration of the spoke-sdp or mesh-sdp at the remote PE, the pseudowire packets received by the local PE will have the hash label included. These packets must be dropped. The only way to solve this is to disable the signaling capability option on the local node which will result in the insertion of the hash label by both PE nodes.
  - If the `hash-label` option is not supported or was not enabled on the local configuration of the spoke-sdp or mesh-sdp at the remote PE, the pseudowire received by the local PE will not have the hash label included.
- The user can enable or disable the signal-capability option in CLI as needed. When doing so, the 7950 SR must withdraw the label it sent to its peer and send a new label mapping message with the new value of the F bit in the flow label interface parameters sub-TLV of the pseudowire ID FEC element.

The `no` form of this command disables the use of the hash label.

**Default**

no hash-label

**Parameters**

- `signal-capability` — Enables the signaling and negotiation of the use of the hash label between the local and remote PE nodes. The `signal-capability` option is not supported on a VPRN spoke-sdp.
igmp-snooping

Syntax  igmp-snooping
Context  config>service>vpls
        config>service>vpls>sap
        config>service>vpls>spoke-sdp
        config>service>vpls>mesh-sdp

Description  This command enables the Internet Group Management Protocol (IGMP) snooping context.

Default  none

igmp-host-tracking

Syntax  igmp-host-tracking
Context  config>service>vpls
        config>service>vpls>sap

Description  This command enables the context to configure IGMP host tracking parameters.

disable-router-alert-check

Syntax  [no] disable-router-alert-check
Context  config>service>vpls>igmp-snooping
        config>service>vpls>sap>igmp-snooping

Description  This command enables the IGMP router alert check option.
The no form of the command disables the router alert check.

expiry-time

Syntax  expiry-time expiry-time
        no expiry-time
Context  config>service>vpls>igmp-snooping
        config>service>vpls>sap>igmp-snooping

Description  This command configures the time that the system continues to track inactive hosts.
The no form of the command removes the values from the configuration.

Default  no expiry-time

Parameters  expiry-time — Specifies the time, in seconds, that this system continues to track an inactive host.

Values  1 — 65535
import

Syntax
import policy-name
no import

Context
config>service>vpls>sap>igmp-snooping

Description
This command associates an import policy to filter IGMP packets.
The no form of the command removes the values from the configuration.

Default
no import

Parameters
policy-name — Specifies the import policy name.

max-num-groups

Syntax
max-num-groups max-num-groups
no max-num-groups

Context
config>service>vpls>sap>igmp-snooping
config>service>vpls>mesh-sdp>igmp-snooping
config>service>vpls>sap>igmp-host-tracking
config>service>vpls>sap>igmp-snooping
config>service>vpls>sap>igmp-host-tracking
config>service>vpls>sap>igmp-snooping
config>service>vpls>spoke-sdp>igmp-snooping

Description
This command configures the maximum number of multicast groups allowed to be tracked.
The no form of the command removes the values from the configuration.

Default
no max-num-groups

Parameters
max-num-groups — Specifies the maximum number of multicast groups allowed to be tracked.
Values
1 — 196607

max-num-sources

Syntax
max-num-sources max-num-sources
no max-num-sources

Context
config>service>vpls>sap>igmp-host-tracking
config>service>vpls>mesh-sdp>igmp-snooping
config>service>vpls>sap>igmp-host-tracking
config>service>vpls>sap>igmp-snooping
config>service>vpls>spoke-sdp>igmp-snooping

Description
This command configures the maximum number of multicast sources allowed per group.
The no form of the command removes the value from the configuration.

Parameters
max-num-sources — Specifies the maximum number of multicast sources allowed per group.
Values
1 — 1000
### max-num-grp-sources

**Syntax**
```
max-num-grp-sources [1..32000]
no max-num-grp-sources
```

**Context**
```
config>service>vpls>sap>igmp-host-tracking
config>service>vpls>mesh-sdp>igmp-snooping
config>service>vpls>sap>igmp-host-tracking
config>service>vpls>sap>igmp-snooping
config>service>vpls>spoke-sdp>igmp-snooping
```

**Description**
This command defines the maximum number of multicast (S,G)s that can be joined on this SAP or SDP. If the node receives an IGMP join message that would exceed the configured number of (S,G)s, the request is ignored.

The **no** form of this command disables the check.

**Default**
```
no max-num-grp-sources
```

**Parameters**

- **1..32000** — Specifies the maximum number of multicast sources allowed to be tracked per group

### import

**Syntax**
```
import policy-name
no import
```

**Context**
```
config>service>vpls>sap>igmp-snooping
config>service>vpls>spoke-sdp>igmp-snooping
config>service>vpls>mesh-sdp>igmp-snooping
```

**Description**
This command specifies the import routing policy to be used for IGMP packets to be used on this SAP or SDP. Only a single policy can be imported on a single SAP or SDP at any time.

The **no** form of the command removes the policy association from the SAP or SDP.

**Default**
```
no import — No import policy is specified.
```

**Parameters**

- **policy-name** — The import policy name. Values can be string up to 32 characters long of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes. These policies are configured in the **config>router>policy-options** context. The router policy must be defined before it can be imported.

### last-member-query-interval

**Syntax**
```
last-member-query-interval tenths-of-seconds
no last-member-query-interval
```

**Context**
```
config>service>vpls>sap>igmp-snooping
config>service>vpls>spoke-sdp>igmp-snooping
config>service>vpls>mesh-sdp>igmp-snooping
```

**Description**
This command defines the last member query interval in tenths of seconds. If the node does not receive a response to a query sent by the IGMP group membership query function, the node sends another query. The default is 1.25 seconds.

The **no** form of this command reverts to the default value.

**Default**
```
1.25 seconds
```

**Parameters**

- **tenths-of-seconds** — The last member query interval in tenths of a second. Values can be string up to 32 characters long of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes. These policies are configured in the **config>router>policy-options** context. The router policy must be defined before it can be imported.
VPLS Multicast Commands

**Description**  This command configures the maximum response time used in group-specific queries sent in response to ‘leave’ messages, and is also the amount of time between 2 consecutive group-specific queries. This value may be tuned to modify the leave latency of the network. A reduced value results in reduced time to detect the loss of the last member of a group. The configured last-member-query-interval is ignored when fast-leave is enabled on the SAP.

**Default**  10

**Parameters**  
- **seconds** — Specifies the frequency, in tenths of seconds, at which query messages are sent.
  - **Values**  1 — 50

**mcac**

**Syntax**  `mcac`

**Context**  
- `config>service>vpls>mesh-sdp>snooping`
- `config>service>vpls>spoke-sdp>snooping`
- `config>service>vpls>sap>igmp-snooping`

**Description**  This command configures multicast CAC policy and constraints for this interface.

**Default**  none

**policy**

**Syntax**  `policy policy-name`

**Context**  
- `config>service>vpls>mesh-sdp>snooping>mcac`
- `config>service>vpls>spoke-sdp>snooping>mcac`
- `config>service>vpls>sap>igmp-snooping>mcac`

**Description**  This command configures the multicast CAC policy name.

**Parameters**  
- **policy-name** — The multicast CAC policy name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

**unconstrained-bw**

**Syntax**  `unconstrained-bw bandwidth mandatory-bw mandatory-bw no unconstrained-bw`

**Context**  
- `config>service>vpls>mesh-sdp>snooping>mcac`
- `config>service>vpls>spoke-sdp>snooping>mcac`
- `config>service>vpls>sap>igmp-snooping>mcac`

**Description**  This command configures the bandwidth for the interface's multicast CAC policy traffic. When disabled (no unconstrained-bw) there will be no checking of bandwidth constraints on the interface.
level. When enabled and a policy is defined, enforcement is performed. The allocated bandwidth for optional channels should not exceed the unconstrained-bw minus the mandatory-bw and the mandatory channels have to stay below the specified value for the mandatory-bw. After this interface check, the bundle checks are performed.

**Parameters**

`bandwidth` — The bandwidth assigned for interface's MCAC policy traffic, in kilo-bits per second (kbps).

**Values**

0 — 2147483647

`mandatory-bw` — Specifies the bandwidth pre-reserved for all the mandatory channels on a given interface in kilo-bits per second (kbps).

If the `bandwidth` value is 0, no mandatory channels are allowed. If `bandwidth` is not configured, then all mandatory and optional channels are allowed.

If the value of `mandatory-bw` is equal to the value of `bandwidth`, then all the unconstrained bandwidth on a given interface is allocated to mandatory channels configured through multicast CAC policy on that interface and no optional groups (channels) are allowed.

The value of `mandatory-bw` should always be less than or equal to that of `bandwidth`. An attempt to set the value of `mandatory-bw` greater than that of `bandwidth`, will result in inconsistent value error.

**Values**

0 — 2147483647

**mc-constraints**

**Syntax**

`mc-constraints`

**Context**

`config>service>vpls>sap>igmp-snooping>mcac`

**Description**

This command enables the context to configure multicast CAC constraints.

**Default**

none

**level**

**Syntax**

`level level-id bw bandwidth`

`no level level-id`

**Context**

`config>service>vpls>sap>igmp-snooping>mcac>mc-constraints`

**Description**

This command configures levels and their associated bandwidth for multicast cac policy on this interface.

**Parameters**

`level-id` — Specifies has an entry for each multicast CAC policy constraint level configured on this system.

**Values**

1 — 8

`bandwidth` — Specifies the bandwidth in kilobits per second (kbps) for the level.

**Values**

1 — 2147483647
VPLS Multicast Commands

number-down

**Syntax**  
```
number-down  number-lag-port-down
no  number-down
```

**Context**  
```
config>service>vpls>sap>igmp-snooping>mcac>mc-constraints
```

**Description**  
This command configure the number of ports down along with level for multicast cac policy on this interface.

**Default**  
not enabled

**Parameters**  
`number-lag-port-down` — If the number of ports available in the LAG is reduced by the number of ports configured in this command here then bandwidth allowed for bundle and/or interface will be as per the levels configured in this context.

**Values**  
1 — 64 (for 64-link LAG)  
1 — 32 (for other LAGs)

max-num-groups

**Syntax**  
```
max-num-groups  count
no  max-num-groups
```

**Context**  
```
config>service>vpls>sap>igmp-snooping
config>service>vpls>spoke-sdp>igmp-snooping
config>service>vpls>mesh-sdp>igmp-snooping
config>service>vpls>sap>mld-snooping
config>service>vpls>spoke-sdp>mld-snooping
config>service>vpls>mesh-sdp>mld-snooping
```

**Description**  
This command defines the maximum number of multicast groups that can be joined on this SAP or SDP. If the node receives an IGMP join message that would exceed the configured number of groups, the request is ignored.

The `no` form of this command disables the check.

**Default**  
no max-num-groups

**Parameters**  
`count` — Specifies the maximum number of groups that can be joined on this SAP or SDP.

**Values**  
1 — 1000

max-num-sources

**Syntax**  
```
max-num-sources  max-num-sources
no  max-num-sources
```

**Context**  
```
config>service>vpls>sap>igmp-snooping
```

**Description**  
This command defines the maximum number of multicast sources that can be joined on this SAP or SDP. If the node receives an IGMP join message that would exceed the configured number of
sources, the request is ignored. The no form of this command disables the check.

**Parameters**

*max-num-sources* — Specifies the maximum number of multicast sources allowed per group.

**Values**

1 — 1000

---

### mrouter-port

**Syntax**

```text
[no] mrouter-port
```

**Context**

- `config>service>vpls>sap>igmp-snooping`
- `config>service>vpls>spoke-sdp>igmp-snooping`
- `config>service>vpls>mesh-sdp>igmp-snooping`

**Description**

This command specifies whether a multicast router is attached behind this SAP or SDP. Configuring a SAP as an mrouter-port will have a double effect. Firstly, all multicast traffic received on another SAP or SDP will be copied to this SAP or SDP. Secondly, IGMP reports generated by the system as a result of someone joining or leaving a multicast group, will be sent to this SAP or SDP.

If two multicast routers exist in the network, one of them will become the active querier. While the other multicast router (non-querier) stops sending IGMP queries, it should still receive reports to keep its multicast trees up to date. To support this, the mrouter-port should be enabled on all SAPs or SDPs connecting to a multicast router.

Note that the IGMP version to be used for the reports (v1, v2 or v3) can only be determined after an initial query has been received. Until such time no reports are sent on the SAP or spoke SDP, even if mrouter-port is enabled.

If the `send-queries` command is enabled on this SAP or spoke SDP, the `mrouter-port` parameter cannot be set.

**Default**

no mrouter-port

---

### mvr

**Syntax**

```text
mvr
```

**Context**

- `config>service>vpls>igmp-snooping`
- `config>service>vpls>mld-snooping`
- `config>service>vpls>sap>igmp-snooping`

**Description**

This command enables the context to configure Multicast VPLS Registration (MVR) parameters.
query-interval

**Syntax**

```
query-interval seconds
no query-interval
```

**Context**

- `config>service>vpls>igmp-snooping`
- `config>service>vpls>sap>igmp-snooping`
- `config>service>vpls>spoke-sdp>igmp-snooping`
- `config>service>vpls>mesh-sdp>igmp-snooping`
- `config>service>vpls>mld-snooping`
- `config>service>vpls>sap>mld-snooping`
- `config>service>vpls>spoke-sdp>mld-snooping`
- `config>service>vpls>mesh-sdp>mld-snooping`

**Description**

This command configures the IGMP query interval. If the `send-queries` command is enabled, this parameter specifies the interval between two consecutive general queries sent by the system on this SAP or SDP. The configured query-interval must be greater than the configured query-response-interval. If send-queries is not enabled on this SAP or SDP, the configured query-interval value is ignored.

**Default**

125

**Parameters**

- `seconds` — The time interval, in seconds, that the router transmits general host-query messages.

<table>
<thead>
<tr>
<th>Values</th>
<th>config&gt;service&gt;vpls&gt;igmp-snooping: 1 - 65535</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>config&gt;service&gt;vpls&gt;sap&gt;igmp-snooping: 2 - 1024</td>
</tr>
</tbody>
</table>

query-src-ip

**Syntax**

```
query-src-ip ip-address
no query-src-ip
```

**Context**

- `config>service>vpls>igmp-snooping`

**Description**

This command configures the IP source address used in IGMP queries.

query-response-interval

**Syntax**

```
query-response-interval seconds
```

**Context**

- `config>service>vpls>sap>igmp-snooping`
- `config>service>vpls>spoke-sdp>igmp-snooping`
- `config>service>vpls>mesh-sdp>igmp-snooping`
- `config>service>vpls>sap>mld-snooping`
- `config>service>vpls>spoke-sdp>mld-snooping`
- `config>service>vpls>mesh-sdp>mld-snooping`

**Description**

This command configures the IGMP query response interval. If the `send-queries` command is enabled, this parameter specifies the maximum response time advertised in IGMPv2/v3 queries.
The configured query-response-interval must be smaller than the configured query-interval. If send-queries is not enabled on this SAP or SDP, the configured query-response-interval value is ignored.

**Default** 10

**Parameters**

- **seconds** — Specifies the length of time to wait to receive a response to the host-query message from the host.
  
  **Values** 1 — 1023

---

**query-src-ip**

**Syntax**

query-src-ip ipv6-address  
no query-src-ip

**Context** config>service>vpls>mld-snooping

**Description** This command configures the IP source address used in MLD queries.

---

**report-src-ip**

**Syntax**

report-src-ip address  
no report-src-ip

**Context** config>service>vpls>igmp-snooping

**Description** This parameter specifies the source IP address used when generating IGMP reports. According to the IGMPv3 standard, a zero source address is allowed in sending IGMP reports. However, for interoperability with some multicast routers, the source IP address of IGMP group reports can be configured using this command.

**Default** 0.0.0.0

**Parameters**

- **ip-address** — The source IP source address in transmitted IGMP reports.

---

**robust-count**

**Syntax**

robust-count robust-count  
no robust-count

**Context**

- config>service>vpls>igmp-snooping
- config>service>vpls>sap>igmp-snooping
- config>service>vpls>spoke-sdp>igmp-snooping
- config>service>vpls>mesh-sdp>igmp-snooping
- config>service>vpls>sap>mld-snooping
- config>service>vpls>spoke-sdp>mld-snooping
- config>service>vpls>mesh-sdp>mld-snooping
Description
If the send-queries command is enabled, this parameter allows tuning for the expected packet loss on a SAP or SDP. The robust-count variable allows tuning for the expected packet loss on a subnet and is comparable to a retry count. If this SAP or SDP is expected to be 'lossy', this parameter may be increased. IGMP snooping on this SAP or SDP is robust to (robust-count-1) packet losses.

If send-queries is not enabled, this parameter will be ignored.

Default
2

Parameters
robust-count — Specifies the robust count for the SAP or SDP.

Values
config>service>vpls>sap>igmp-snooping: 2 — 7
cfg>service>vpls>igmp-snooping: 1 — 255

mrp

Syntax
mrp

Context
config>service>vpls
config>service>vpls>mesh-sdp
config>service>vpls>sap
config>service>vpls>spoke-sdp

Description
This command configures Multiple Registration Protocol (MRP) parameters.

mvrp

Syntax
mvrp

Context
config>service>vpls

Description
This command configures MVRP parameters.

attribute-table-size

Syntax
[no] attribute-table-size value

Context
config>service>vpls>mvrp

Description
This command controls the number of attributes accepted on a per BVPLS basis. When the limit is reached, no new attributes will be registered.

If a new lower limit (smaller than the current number of attributes) from a local or dynamic IVPLS is being provisioned, a CLI warning will be issued stating that the system is currently beyond the new limit. The value will be accepted, but any creation of new attributes will be blocked under the attribute count drops below the new limit; the software will then start enforcing the new limit.

Default
maximum number of attributes

Parameters
value — Specifies the number of attributes accepted on a per BVPLS basis.
attribute-table-size

Syntax  
[no] attribute-table-size value

Context  
config>service>vpls>mrp  
config>service>vpls>mvrp

Description  
This command controls the number of attributes accepted on a per BVPLS basis. When the limit is reached, no new attributes will be registered.

If a new lower limit (smaller than the current number of attributes) from a local or dynamic IVPLS is being provisioned, a CLI warning will be issued stating that the system is currently beyond the new limit. The value will be accepted, but any creation of new attributes will be blocked under the attribute count drops below the new limit; the software will then start enforcing the new limit.

Default  
maximum number of attributes

Parameters  
value — Specifies the number of attributes accepted on a per BVPLS basis.

Values  
SR-7/SR-12: 1 — 2047  
SR-1 1 — 1023

attribute-table-high-wmark

Syntax  
[no] attribute-table-high-wmark high-water-mark

Context  
config>service>vpls>mrp  
config>service>vpls>mvrp

Description  
This command specifies the percentage filling level of the MMRP attribute table where logs and traps are sent.

Default  
95%

Parameters  
high-water-mark — Specifies the utilization of the MRP attribute table of this service at which a table full alarm will be raised by the agent.

Values  
1% — 100%

attribute-table-low-wmark

Syntax  
[no] attribute-table-low-wmark low-water-mark

Context  
config>service>vpls>mrp  
config>service>vpls>mvrp
VPLS Multicast Commands

**Description**
This command specifies the MMRP attribute table low watermark as a percentage. When the percentage filling level of the MMRP attribute table drops below the configured value, the corresponding trap is cleared and/or a log entry is added.

**Default**
90%

**Parameters**
- `low-water-mark` — Specifies utilization of the MRP attribute table of this service at which a table full alarm will be cleared by the agent.
  - **Values**
    - 1% — 100%

**flood-time**

**Syntax**
```
flood-time flood-time
no flood-time
```

**Context**
- `config>service>vpls>mrp`
- `config>service>vpls>mvrp`

**Description**
This command configures the amount of time, in seconds, after a status change in the VPLS service during which traffic is flooded. Once that time expires, traffic will be delivered according to the MMRP registrations that exist in the VPLS.

**Default**
3 seconds

**Parameters**
- `flood-time` — Specifies the MRP flood time, in seconds.
  - **Values**
    - 3 — 600

**join-time**

**Syntax**
```
[no] join-time value
```

**Context**
- `config>service>vpls>sap>mrp`
- `config>service>vpls>spoke-sdp>mrp`
- `config>service>vpls>mesh-sdp>mrp`

**Description**
This command controls the interval between transmit opportunities that are applied to the Applicant state machine. An instance of this Join Period Timer is required on a per-Port, per-MRP Participant basis. For additional information, refer to IEEE 802.1ak-2007 section 10.7.4.1.

**Default**
2

**Parameters**
- `value` — Specifies the timer value in 10th of seconds for sending join-messages.
  - **Values**
    - 1 — 10 tenths of a second
leave-time

Syntax  
[no] leave-time value

Context  
```
config>service>vpls>sap>mrp
config>service>vpls>spoke-sdp>mrp
config>service>vpls>mesh-sdp>mrp
```

Description  
This command controls the period of time that the Registrar state machine will wait in the leave state before transitioning to the MT state when it is removed. An instance of the timer is required for each state machine that is in the leave state. The Leave Period Timer is set to the value leave-time when it is started.

A registration is normally in “in” state where there is an MFIB entry and traffic is being forwarded. When a “leave all” is performed (periodically around every 10-15 seconds per SAP/SDP binding - see leave-all-time-below), a node sends a message to its peer indicating a leave all is occurring and puts all of its registrations in leave state.

The peer refreshes its registrations based on the leave all PDU it receives and sends a PDU back to the originating node with the state of all its declarations.

Refer to IEEE 802.1ak-2007 section 10.7.4.2.

Default  
30

Parameters  
value — [30-60] tenths of a second

leave-all-time

Syntax  
[no] leave-all-time value

Context  
```
config>service>vpls>sap>mrp
config>service>vpls>spoke-sdp>mrp
config>service>vpls>mesh-sdp>mrp
```

Description  
This command controls the frequency with which the LeaveAll state machine generates LeaveAll PDUs. The timer is required on a per-Port, per-MRP Participant basis. The Leave All Period Timer is set to a random value, T, in the range LeaveAllTime<T<1.5*leave-all-time when it is started. Refer to IEEE 802.1ak-2007 section 10.7.4.3.

Default  
100

Parameters  
value — [60-300] tenths of a second

mrp-policy

Syntax  
[no] mrp-policy-name

Context  
```
config>service>vpls>sap>mrp
config>service>vpls>spoke-sdp>mrp
config>service>vpls>mesh-sdp>mrp
```
**VPLS Multicast Commands**

**Description**  This command instructs MMRP to use the mrp-policy specified in the command to control which Group BMAC attributes will be declared and registered on the egress SAP/Mesh-SDP/Spoke-SDP. The Group BMACs will be derived from the ISIDs using the procedure used in the PBB solution. The Group MAC = standard OUI with the last 24 bits being the ISID value. If the policy-name refers to a non-existing mrp-policy the command should return error. Changes to a mrp-policy are allowed and applied to the SAP/SDPs under which the policy is referenced.

**Default**  no mrp-policy is defined

**Parameters**  
*policy-name* — Specifies the redirect policy name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

---

**periodic-time**

**Syntax**  
[no] periodic-time value

**Context**  
config>service>vpls>sap>mrp
config>service>vpls>spoke-sdp>mrp
config>service>vpls>mesh-sdp>mrp

**Description**  This command controls the frequency the PeriodicTransmission state machine generates periodic events if the Periodic Transmission Timer is enabled. The timer is required on a per-Port basis. The Periodic Transmitting Timer is set to one second when it is started.

**Default**  10

**Parameters**  
*value* — [10-100] tenths of a second

---

**periodic-timer**

**Syntax**  
[no] periodic-timer

**Context**  
config>service>vpls>sap>mrp
config>service>vpls>spoke-sdp>mrp
config>service>vpls>mesh-sdp>mrp

**Description**  This command enables or disables the Periodic Transmission Timer.

**Default**  disabled

---

**multicast-info-policy**

**Syntax**  
multicast-info-policy policy-name

**Context**  
config>service>vpls

**Description**  This command specifies the multicast policy name configured on this service.
per-service-hashing

**Syntax**

```
[no] per-service-hashing
```

**Context**

```
config>service>vpls
config>template>vpls-template
```

**Description**

This command enables on a per service basis, consistent per-service hashing for Ethernet services over LAG, over Ethernet tunnel (eth-tunnel) using loadsharing protection-type or over CCAG. Specifically, it enables the new hashing procedures for Epipe, VPLS, regular or PBB services.

The following algorithm describes the hash-key used for hashing when the new option is enabled:

- If the packet is PBB encapsulated (contains an I-TAG ethertype) at the ingress side, use the ISID value from the I-TAG
- If the packet is not PBB encapsulated at the ingress side
  - For regular (non-PBB) VPLS and Epipe services, use the related service ID
  - If the packet is originated from an ingress IVPLS or PBB Epipe SAP
    - If there is an ISID configured use the related ISID value
    - If there is no ISID yet configured use the related service ID
  - For BVPLS transit traffic use the related flood list id
    - Transit traffic is the traffic going between BVPLS endpoints
    - An example of non-PBB transit traffic in BVPLS is the OAM traffic
- The above rules apply regardless of traffic type
  - Unicast, BUM flooded without MMRP or with MMRP, IGMP snooped

The `no` form of this command implies the use of existing hashing options.

**Default**

`no per-service-hashing`

pim-snooping

**Syntax**

```
[no] pim-snooping
```

**Context**

```
config>service>vpls>spoke-sdp
config>service>vpls>sap
```

**Description**

This command enables PIM snooping for the VPLS service. When enabled, it is enabled for all SAPs except default SAPs. A default SAP is a SAP that has a wildcard VLAN ID, such as `sap 1/1/1:*`.

The `no` form of the command removes the PIM snooping configuration.
max-num-groups

Syntax  
max-num-groups num-groups
no max-num-groups

Context  
config>service>vpls>pim-snooping
config>service>vpls>spoke-sdp>pim-snooping
config>service>vpls>sap>pim-snooping

Description  
This command configures the maximum groups for PIM snooping.

Parameters  
num-groups — Specifies the maximum groups for PIM snooping.

Values  
1 — 16000

oper-group

Syntax  
[no] oper-group name

Context  
config>service>vpls>sap
config>service>vpls>spoke-sdp
config>service>vpls>bgp>pw-template-binding

Description  
This command associates the context to which it is configured to the operational group specified in the
name. The oper-group name must be already configured under config>service before its name is
referred to in this command.
The no form of the command removes the association.

Default  
no oper-group

Parameters  
name — A character string of maximum 32 ASCII characters identifying the group instance.

monitor-oper-group

Syntax  
[no] monitor-oper-group name

Context  
config>service>vpls>site
config>service>vpls>spoke-sdp
config>service>vpls>sap

Description  
This command specifies the operational group to be monitored by the object under which it is
configured. The oper-group name must be already configured under config>service before its name is
referred to in this command.
The no form of the command removes the association.

Default  
no oper-group

Parameters  
name — A character string of maximum 32 ASCII characters identifying the group instance.
hold-time

Syntax

```
hold-time seconds
no hold-time
```

Context

```
config>service>vpls>pim-snooping
```

Description

This command configures the duration that allows the PIM-snooping switch to snoop all the PIM states in the VPLS. During this duration, multicast traffic is flooded in the VPLS. At the end of this duration, multicast traffic is forwarded using the snooped states.

When PIM snooping is enabled in VPLS, there is a period of time when the PIM snooping switch may not have built complete snooping state. The switch cannot build states until the routers connected to the VPLS refresh their PIM messages.

This parameter is applicable only if PIM snooping is enabled.

Parameters

```
seconds — Specifies the PIM snooping hold time, in seconds
```

- **Values**
  - 0 — 300
- **Default**
  - 90

mode

Syntax

```
mode mode
```

Context

```
config>service>vpls>pim-snooping
```

Description

This command sets the PIM snooping mode to proxy or plain snooping.

Parameters

```
mode — Specifies PIM snooping mode.
```

- **Values**
  - snooping, proxy
- **Default**
  - proxy

precedence

Syntax

```
precedence precedence-value| primary
no precedence
```

Context

```
config>service>vpls>spoke-sdp
```

Description

This command configures the spoke SDP precedence.

Default

4

Parameters

```
precedence-value — Specify the spoke SDP precedence.
```

- **Values**
  - 0 — 4
- **primary** — Specifies that the precedence is primary.
VPLS Multicast Commands

pw-status-signaling

Syntax     [no] pw-status-signaling
Context    config>service>vpls>spoke-sdp
Description This command specifies the type of signaling used by this multi-segment pseudowire provider-edge for this service.

When no pw-status-signaling is enabled, a 7x50 will not include the pseudowire status TLV in the initial label mapping message of the pseudowire used for a spoke SDP. This will force both 7x50 PEs to use the pseudowire label withdrawal method for signaling pseudowire status.

If pw-status-signaling is configured, the node will include the use of the pseudowire status TLV in the initial label mapping message for the pseudowire.

propagate-mac-flush

Syntax     [no] propagate-mac-flush
Context    config>service>vpls
Description This command specifies whether MAC flush messages received from the given LDP are propagated to all spoke and mesh SDPs within the context of this VPLS service. The propagation will follow the split-horizon principle and any data-path blocking in order to avoid the looping of these messages.

Default    no propagate-mac-flush

send-queries

Syntax     [no] send-queries
Context    config>service>vpls>sap>igmp-snooping
config>service>vpls>spoke-sdp>igmp-snooping
config>service>vpls>mesh-sdp>igmp-snooping
config>service>vpls>sap>mld-snooping
config>service>vpls>spoke-sdp>mld-snooping
config>service>vpls>mesh-sdp>mld-snooping

Description This command specifies whether to send IGMP general query messages on the SAP or SDP.

When send-queries is configured, all type of queries generate ourselves are of the configured version. If a report of a version higher than the configured version is received, the report will get dropped and a new wrong version counter will get incremented. If send-queries is not configured, the version command has no effect. The version used will be the version of the querier. This implies that, for example, when we have a v2 querier, we will never send out a v3 group or group-source specific query when a host wants to leave a certain group.

Default    no send-queries
source

**Syntax**

```
[no] source ip-address
```

**Context**

```
config>service>vpls>sap>igmp-snooping>static>group
config>service>vpls>spoke-sdp>igmp-snooping>static>group
config>service>vpls>mesh-sdp>igmp-snooping>static>group
```

**Description**

This command adds a static (s,g) entry, to allow multicast traffic for a multicast group from a specified source. For a multicast group, more than one source address can be specified. Static (s,g) entries cannot be added, if a starg is previously created.

The `no` form of the command removes the source from the configuration.

**Default**

none

**Parameters**

*ip-address* — Specifies the IPv4 unicast address.

---

starg

**Syntax**

```
[no] starg
```

**Context**

```
config>service>vpls>sap>igmp-snooping>static>group
config>service>vpls>spoke-sdp>igmp-snooping>static>group
config>service>vpls>mesh-sdp>igmp-snooping>static>group
```

**Description**

This command adds a static (*,g) entry to allow multicast traffic for the corresponding multicast group from any source. This command can only be enabled if no existing source addresses for this group are specified.

The `no` form of the command removes the starg entry from the configuration.

**Default**

no starg

---

static

**Syntax**

```
static
```

**Context**

```
config>service>vpls>sap>igmp-snooping
config>service>vpls>spoke-sdp>igmp-snooping
config>service>vpls>mesh-sdp>igmp-snooping
config>service>vpls>sap>mld-snooping
config>service>vpls>spoke-sdp>mld-snooping
config>service>vpls>mesh-sdp>mld-snooping
```

**Description**

This command enables access to the context to configure static group addresses. Static group addresses can be configured on a SAP or SDP. When present either as a (*, g) or a (s,g) entry, multicast packets matching the configuration will be forwarded even if no join message was registered for the specific group.

**Default**

none
version

Syntax

```
version version
no version
```

Context

```
config>service>vpls>sap>igmp-snooping
config>service>vpls>mesh-sdp>igmp-snooping
config>service>vpls>spoke-sdp>igmp-snooping
config>service>vpls>sap>mld-snooping
config>service>vpls>spoke-sdp>mld-snooping
config>service>vpls>mesh-sdp>mld-snooping
```

Description

This command specifies the version of IGMP which is running on this SAP or SDP. This object can be used to configure a router capable of running either value. For IGMP to function correctly, all routers on a LAN must be configured to run the same version of IGMP on that LAN.

When the send-query command is configured, all type of queries generate ourselves are of the configured version. If a report of a version higher than the configured version is received, the report gets dropped and a new “wrong version” counter is incremented.

If the send-query command is not configured, the version command has no effect. The version used on that SAP or SDP will be the version of the querier. This implies that, for example, when there is a v2 querier, a v3 group or group-source specific query when a host wants to leave a certain group will never be sent.

Parameters

```
version — Specify the IGMP version.
```

Values

```
1, 2, 3
```

to-sap

Syntax

```
to-sap sap-id
no to-sap
```

Context

```
config>service>vpls>sap>igmp-snooping>mvr
```

Description

In some situations, the multicast traffic should not be copied from the MVR VPLS to the SAP on which the IGMP message was received (standard MVR behaviour) but to another SAP.

This command configures the SAP to which the multicast data needs to be copied.

Default

```
no to-sap
```

Parameters

```
sap-id — Specifies the SAP to which multicast channels should be copied. See Common CLI Command Descriptions on page 1783 for command syntax.
```

app-profile

Syntax

```
app-profile app-profile-name
no app-profile
```

Context

```
config>service>vpls>sap
```

7950 SR OS Services Guide
**Description**
This command configures the application profile name.

**Parameters**
- `app-profile-name` — Specifies an existing application profile name configured in the `config>app-assure>group>policy` context.

**arp-host**

**Syntax**
`arp-host`

**Context**
`config>service>vpls>sap`

**Description**
This command enables the context to configure ARP host parameters.

**host-limit**

**Syntax**
`host-limit max-num-hosts`
`no host-limit`

**Context**
`config>service>vpls>sap>arp-host`

**Description**
This command configures the maximum number of ARP hosts.
The `no` form of the command returns the value to the default.

**Default**
1

**Parameters**
- `max-num-hosts` — specifies the maximum number of ARP hosts allowed on this SAP.

**Values**
- 1 — 32767

**min-auth-interval**

**Syntax**
`min-auth-interval min-auth-interval`
`no min-auth-interval`

**Context**
`config>service>vpls>sap>arp-host`

**Description**
This command configures the minimum authentication interval.
The `no` form of the command returns the value to the default.

**Default**
15

**Parameters**
- `min-auth-interval` — Specifies the minimum authentical interval, in minutes.

**Values**
- 1 — 6000
arp-reply-agent

Syntax

```
arp-reply-agent [sub-ident]
no arp-reply-agent
```

Context  config>service>vpls>sap

Description

This command enables a special ARP response mechanism in the system for ARP requests destined to static or dynamic hosts associated with the SAP. The system responds to each ARP request using the hosts MAC address as the both the source MAC address in the Ethernet header and the target hardware address in the ARP header.

ARP replies and requests received on a SAP with **arp-reply-agent** enabled will be evaluated by the system against the anti-spoof filter entries associated with the ingress SAP (if the SAP has anti-spoof filtering enabled). ARPs from unknown hosts on the SAP will be discarded when anti-spoof filtering is enabled.

The ARP reply agent only responds if the ARP request enters an interface (SAP, spoke SDP or mesh-SDP) associated with the VPLS instance of the SAP.

A received ARP request that is not in the ARP reply agent table is flooded to all forwarding interfaces of the VPLS capable of broadcast except the ingress interface while honoring split-horizon constraints.

Static hosts can be defined on the SAP using the **host** command. Dynamic hosts are enabled on the system by enabling the **lease-populate** command in the SAP’s **dhcp** context. In the event that both a static host and a dynamic host share the same IP and MAC address, the VPLS ARP reply agent will retain the host information until both the static and dynamic information are removed. In the event that both a static and dynamic host share the same IP address, but different MAC addresses, the VPLS ARP reply agent is populated with the static host information.

The **arp-reply-agent** command will fail if an existing static host on the SAP does not have both MAC and IP addresses specified. Once the ARP reply agent is enabled, creating a static host on the SAP without both an IP address and MAC address will fail.

The ARP-reply-agent may only be enabled on SAPs supporting Ethernet encapsulation.

The **no** form of the command disables ARP-reply-agent functions for static and dynamic hosts on the SAP.

Default  not enabled

Parameters

**sub-ident** — Configures the arp-reply-agent to discard ARP requests received on the SAP that are targeted for a known host on the same SAP with the same subscriber identification.

Hosts are identified by their subscriber information. For DHCP subscriber hosts, the subscriber hosts, the subscriber information is configured using the optional subscriber parameter string.

When arp-reply-agent is enabled with **sub-ident**:

- If the subscriber information for the destination host exactly matches the subscriber information for the originating host and the destination host is known on the same SAP as the source, the ARP request is silently discarded.

- If the subscriber information for the destination host or originating host is unknown or undefined, the source and destination hosts are not considered to be the same subscriber. The ARP request is forwarded outside the SAP’s Split Horizon Group.
• When **sub-ident** is not configured, the arp-reply-agent does not attempt to identify the subscriber information for the destination or originating host and will not discard an ARP request based on subscriber information.

### force-l2pt-boundary

**Syntax**  
```plaintext
[no] force-l2pt-boundary
```

**Context**  
`config>service>vpls>sap`

**Description**  
Enabling force-l2pt-boundary will force that all SAPs managed by the given m-vpls instance on the corresponding port will have to have l2pt-termination enabled. This command is applicable only to SAPs created under m-vpls and this regardless the flavor of STP currently being active. It is not applicable to spoke SDPS.

The execution of this command will fail as soon as at least one of the currently managed SAPs (all SAPs falling within the specified managed-vlan-range) does not have l2pt-termination enabled, and this regardless its admin/operational status.

If force-l2pt-boundary is enabled on a given m-vpls SAP, all newly created SAPs falling into the specified managed-vlan-range will have l2pt-termination enabled per default.

Extending or adding new range into a managed-vlan-range declaration will fail as soon as there is at least one SAPs falling into the specified vlan-range does not have l2pt-termination enabled.

Disabling l2pt-termination on currently managed SAPs will fail as soon as the force-l2pt-boundary is enabled under corresponding m-vpls SAP.

### frame-relay

**Syntax**  
```plaintext
frame-relay
```

**Context**  
`config>service>vpls>sap`

**Description**  
This command enables the context to configure frame-relay parameters.

### frf-12

**Syntax**  
```plaintext
[no] frf-12
```

**Context**  
`config>service>vpls>sap>fr`

**Description**  
This command enables FRF12 headers. This must be set to disabled for this entry to be added to an MLFR bundle.

The **no** form of the command disables FRF12 headers.
ete-fragment-threshold

Syntax  

```
ete-fragment-threshold  threshold
no ete-fragment-threshold
```

Context  

```
config>service>vpls>sap>fr>frf-12
```

Description  
This command configures the FRF.12 fragmentation threshold.

The no form of the command removes the value.

Default  

```
128
```

Parameters  

```
threshold  —  Specifies  the  maximum  length  of  a  fragment  to  be  transmitted.
```

```
Values  128  —  512
```

interleave

Syntax  

```
interleave
no interleave
```

Context  

```
config>service>vpls>sap>frame-relay>frf.12
```

Description  
This command enables interleaving of high priority frames and low-priority frame fragments within a FR SAP using FRF.12 end-to-end fragmentation.

When this option is enabled, only frames of the FR SAP non expedited forwarding class queues are subject to fragmentation. The frames of the FR SAP expedited queues are interleaved, with no fragmentation header, among the fragmented frames. In effect, this provides a behavior like in MLPPP Link Fragment Interleaving (LFI).

When this option is disabled, frames of all the FR SAP forwarding class queues are subject to fragmentation. The fragmentation header is however not included when the frame size is smaller than the user configured fragmentation size. In this mode, the SAP transmits all fragments of a frame before sending the next full or fragmented frame.

The receive direction of the FR SAP supports both modes of operation concurrently, with and without fragment interleaving.

The no form of this command restores the default mode of operation.

Default  

```
no interleave
```

scheduling-class

Syntax  

```
scheduling-class  class-id
no scheduling-class
```

Context  

```
config>service>vpls>sap>frame-relay
```

Description  
This command specifies the scheduling class to use for this SAP. This object is only applicable for a SAP whose bundle type is set to MLFR.
Parameters  

- **class-id** — Specifies the scheduling class.
  
  **Values**  
  0 — 3

---

**host-connectivity-verify**

**Syntax**

```
host-connectivity-verify source-ip ip-address [source-mac ieee-address] [interval interval] [action {remove | alarm}]
```

**Context**

```
config>service>vpls
config>service>vpls>sap
```

**Description**

This command enables subscriber host connectivity verification on a given SAP within a VPLS service. This tool will periodically scan all known hosts (from dhcp-state) and perform a UC ARP request. The subscriber host connectivity verification will maintain state (connected vs. not-connected) for all hosts.

**Default**

no host-connectivity-verify

**Parameters**

- **source-ip ip-address** — Specify an unused IP address in the same network for generation of subscriber host connectivity verification packets.
- **source-mac ieee-address** — Specifies the source MAC address to be used for generation of subscriber host connectivity verification packets.
- **interval interval** — The interval, in minutes, which specifies the time interval in which all known sources should be verified. The actual rate is then dependent on number of known hosts and interval.
  
  **Values**  
  1 — 6000
  
  Note that a zero value can be used by the SNMP agent to disable host-connectivity-verify.
- **action {remove | alarm}** — Defines the action taken on a subscriber host connectivity verification failure for a given host. The remove keyword raises an alarm and removes dhcp-state and releases all allocated resources (queues, table entries, etc.). DHCP release will be signaled to corresponding DHCP server. Static host will be never removed. The alarm keyword raises an alarm indicating that the host is disconnected.
Egress Multicast Group Commands

egress-multicast-group

Syntax

- `egress-multicast-group egress-multicast-group-name`
- `no egress-multicast-group group-name`

Context

- `config>service`

Description

This command creates an egress multicast group (EMG) context. An EMG is created as an object used to group VPLS SAPs that are allowed to participate in efficient multicast replication (EMR). EMR is a method to increase the performance of egress multipoint forwarding by sacrificing some destination-based features. Eliminating the requirement to perform unique features for each destination allows the egress forwarding plane to chain together multiple destinations into a batch replication process. In order to perform this batch replication function, similar characteristics are required on each SAP within the EMG.

Only SAPs defined on Ethernet access ports are allowed into an egress-multicast-group.

In order to understand the purpose of an egress-multicast-group, an understanding of the system’s use of flooding lists is required. A flooding list is maintained at the egress forwarding plane to define a set of destinations to which a packet must be replicated. Multipoint services make use of flooding lists to enable forwarding a single packet to many destinations. Examples of multipoint services that use flooding lists are VPLS, IGMP snooping and IP multicast routing. Currently, the egress forwarding plane will only use efficient multicast replication for VPLS and IGMP snooping flooding lists.

In VPLS services, a unique flooding list is created for each VPLS context. The flooding list is used when a packet has a broadcast, multicast or unknown destination MAC address. From a system perspective, proper VPLS handling requires that a broadcast, multicast or unknown destined packet be sent to all destinations that are in the forwarding state. The ingress forwarding plane ensures the packet gets to all egress forwarding planes that include a destination in the VPLS context. It is the egress forwarding plane’s job to replicate the packet to the subset of the destinations that are reached through its interfaces and each of these destinations are included in the VPLS context’s flooding list.

For IGMP snooping, a unique flooding list is created for each IP multicast (s,g) record. This (s,g) record is associated with an ingress VPLS context and may be associated with VPLS destinations in the source VPLS instance or other VPLS instances (in the case of MVR). Again, the ingress forwarding plane ensures that an ingress IP multicast packet matching the (s,g) record gets to all egress forwarding planes that have a VPLS destination associated with the (s,g) record. The egress forwarding plane uses the flooding list owned by the (s,g) record to replicate the packet to all VPLS destinations in the flooding list. The IGMP Snooping function identifies which VPLS destinations should be associated with the (s,g) record.

With normal multicast replication, the egress forwarding plane examines which features are enabled for each destination. This includes ACL filtering, mirroring, encapsulation and queuing. The resources used to perform this per destination multicast processing are very expensive to the egress forwarding plane when high replication bandwidth is required. If destinations with similar egress functions can be grouped together, the egress forwarding plane can process them in a more efficient manner and maximize replication bandwidth.

The egress-multicast-group object is designed to allow the identification of SAPs with similar egress characteristics. When a SAP is successfully provisioned into an egress-multicast-group, the system is
ensured that it may be batched together with other SAPs in the same group at the egress forwarding plane for efficient multicast replication. A SAP that does not meet the common requirements is not allowed into the egress-multicast-group.

At the forwarding plane level, a VPLS flooding list is categorized into chainable and non-chainable destinations. Currently, the only chainable destinations are SAPs within an egress-multicast-group. The chainable destinations are further separated by egress-multicast-group association. Chains are then created following the rules below:

- A replication batch chain may only contain SAPs from the same egress-multicast-group
- A replication batch chain length may not exceed the dest-chain-limit of the egress-multicast-group to which the SAPs are members

Further subcategories are created for an IGMP (s,g) flooding list. A Layer 2 (s,g) record is created in a specific VPLS instance (the instance the (s,g) flow ingresses). SAPs within that VPLS context that join the (s,g) record are considered native SAPs within the flooding list. SAPs that join the (s,g) flooding list through the multicast VPLS registration process (MVR) from another VPLS context using the from-vpls command are considered alien SAPs. The distinction between native and alien in the list is maintained to allow the forwarding plane to enforce or suspend split-horizon-group (SHG) squelching. When the source of the (s,g) matching packet is in the same SHG as a native SAP, the packet must not be replicated to that SAP. For a SAP in another VPLS context, the source SHG of the packet has no meaning and the forwarding plane must disregard SHG matching between the native source of the packet and the alien destination. Because the SHG squelch decision is done for the whole chain based on the first SAP in the chain, all SAPs in the chain must be all native or all alien SAPs. Chains for IGMP (s,g) flooding lists are created using the following rules:

1. A replication batch chain may only contain SAPs from the same egress-multicast-group.
2. A replication batch chain may only contain all alien or all native SAPs.
3. A replication batch chain length may not exceed the dest-chain-limit of the egress-multicast-group to which the SAPs are members

When a packet associated with a flooding list is received by the egress forwarding plane, it processes the packet by evaluating each destination on the list sequentially in a replication context. If the current entry being processed in the list is a non-chained destination, the forwarding plane processes the packet for that destination and then moves on to process other packets currently in the forwarding plane before returning to process the next destination in the list. If the current entry being processed is a chained destination, the forwarding plane remains in the replication context until it has forwarded to each entry in that chain. Once the replication context finishes with the last entry in the chain, it moves on to process other packets waiting for egress processing before returning to the replication context. Processing continues in this manner until the packet has been forwarded to all destinations in the list.

Batch chain processing of a chain of SAPs improves replication efficiency by bypassing the functions that perform egress mirroring decisions on SAPs within the chain and making a single ACL filtering decision for the whole chain. Each destination in the chain may have a unique egress QoS policy and per destination queuing is still performed for each destination in the chain. Also, while each SAP in the chain must be on access ports with the same encap-type, if the encap-type is dot1q, each SAP may have a unique dot1q tag.

One caveat to each SAP having a unique egress QoS policy in the chain is that only the Dot1P marking decisions for the first SAP in the list is enforced. If the first SAP’s QoS policy forwarding class action states that the packet should not be remarked, none of the replicated packets in the chain will have the dot1P bits remarked. If the first SAP’s QoS policy forwarding class action states that the
packet should be remarked with a specific dot1P value, all the replicated packets for the remaining SAPs in the chain will have the same dot1P marking.

While the system supports 32 egress multicast groups, a single group would usually suffice. An instance where multiple groups would be needed is when all the SAPs requiring efficient multicast replication cannot share the same common requirements. In this case, an egress multicast group would be created for each set of common requirements. An egress multicast group may contain SAPs from many different VPLS instances. It should be understood that an egress multicast group is not equivalent to an egress forwarding plane flooding list. An egress multicast group only identifies which SAPs may participate in efficient multicast replication. As stated above, entries in a flooding list are populated due to VPLS destination creation or IGMP snooping events.

The no form of the command removes a specific egress multicast group. Deleting an egress multicast group will only succeed when the group has no SAP members. To remove SAP members, use the no multicast-group group-name command under each SAP’s egress context.

Parameters

**group-name** — Multiple egress multicast groups may be created on the system. Each must have a unique name. The egress-multicast-group-name is an ASCII string up to 16 characters in length and follows all the naming rules as other named policies in the system. The group’s name is used throughout the system to uniquely identify the Egress Multicast Group and is used to provision a SAP into the group.

**Default** None, each egress multicast group must be explicitly configured.

**Values** Up to 32 egress multicast groups may be created on the system.

description

**Syntax**

description description-string

no description

**Context**

config>service>egress-multicast-group

**Description**

This command defines an ASCII string associated with egress-multicast-group-name.

The no form of the command removes an existing description string from egress-multicast-group.

**Default** none

**Parameters**

description-string — The description command accepts a description-string parameter. The description-string parameter is an ASCII string of up to 80 characters in length. Only printable 127 bit ASCII characters are allowed. If the string contains spaces, the string must be specified with beginning and ending quotes.

**Values** An ASCII string up to 80 characters in length.
**dest-chain-limit**

**Syntax**

```
dest-chain-limit destinations per pass
no dest-chain-limit
```

**Context**

```
config>service>egress-multicast-group
```

**Description**

This command defines the maximum length of an egress forwarding plane efficient multicast replication chain for an egress-multicast-group. Varying the maximum length of chains created for an egress multicast group has the effect of efficient multicast batched chain replication on other packets flowing through the egress forwarding plane. While replicating for the SAPs within a replication chain, other packets are waiting for the forwarding plane to finish. As the chain length increases, forwarding latency for the other waiting packets may increase. When the chain length decreases, a loss of efficiency in the replication process will be observed.

The **no** form of the command restores the default value.

**Default**

16

**Parameters**

- destinations per pass — This parameter must be specified when executing the `dest-chain-limit` command. When executed, the command will use the number-of-destinations parameter to reorganize all efficient multicast SAP chains that contain members from the egress-multicast-group.

The `destinations per pass` parameter can be modified at any time. Be aware that when changing the maximum chain length, the system will rebuild the chains according to the new limit. When this happens, it is possible that packets will not be replicated to a destination while it is being reorganized in the flooding list’s chains. Only the chains associated with the egress-multicast-group context the command is executed in will be affected by changing the parameter.

It is expected that the optimal replication chain length will be between 10 and 16. Since so many variables affect efficient multicast (i.e. ingress packet rate, number of chains, size of replicated packets), only proper testing in the environment that replication will be performed will identify the best dest-chain-limit value for each Egress Multicast Group.

Setting the `destinations per pass` parameter to a value of 0 has the effect of removing from all egress forwarding planes all chains with members from the egress-multicast-group. Replication to each destination SAP from the group is performed using the normal method (non-efficient replication). The value 0 is not considered a normal value for dest-chain-limit and is provided for debugging purposes only. Setting the value to 0 is persistent between reboots of the system.

Setting the `destinations per pass` parameter to a value of 1 has the effect of placing each egress-multicast-group member SAP into a chain with a single SAP. The value 1 is not considered a normal value for the `dest-chain-limit` and is provided for debugging purposes only. Setting the value to 1 is persistent between reboots of the system.

**Values**

1 — 30

---

**sap-common-requirements**

**Syntax**

```
sap-common-requirements
```

**Context**

```
config>service>egress-multicast-group
```

---
**Description**
This command configures the common SAP parameter requirements. The SAP common requirements are used to evaluate each SAP for group membership. If a SAP does not meet the specified requirements, the SAP is not allowed into the egress-multicast-group. Once a SAP is a member of the group, attempting to change the parameters on the SAP will fail.

**egress-filter**

**Syntax**
```plaintext
egress-filter [ip ip-filter-id]
egress-filter [ipv6 ipv6-filter-id]
egress-filter [mac mac-filter-id]
no egress-filter [ip ip-filter-id] [ipv6 ipv6-filter-id] [mac mac-filter-id]
```

**Context**
```
cfg>service>egress-multicast-group>sap-common-requirements
```

**Description**
This command identifies the type of filter and actual filter ID that must be provisioned on the SAP prior to the SAP being made a member of the egress-multicast-group. If the SAP does not have the specified filter applied, the SAP cannot be provisioned into the group. It is important that the egress filter applied to each SAP within the egress-multicast-group be the same since the batch replication process on an efficient multicast replication chain will apply the first SAP’s ACL decision to all other SAPs on the chain. Once the SAP is made a member of the egress-multicast-group, the SAP’s egress filter cannot be changed on the SAP.

Changing the `egress-filter` parameters within the `sap-common-requirements` node automatically changes the egress filter applied to each member SAP. If the filter cannot be changed on the SAP due to resource constraints, the modification will fail.

The specified egress-filter does not contain an entry that is defined as an egress mirror-source. Once the filter is associated with the egress-multicast-group, attempting to define one of its entries as an egress mirror source will fail.

The `no` form of the command removes the egress-filter removes the egress filter from each member SAP. The `no egress-filter` command specifies that an egress filter (IP, IPv6 or MAC) is not applied to a new member SAP within the egress-multicast-group.

**Default**
`no filter`. The egress filter ID must be defined with the associated `ip` or `mac` keyword. If an egress-filter is not specified or the no egress-filter command is executed in the sap-common-requirements node, a new member SAP does not have an egress IP or MAC filter defined.

**Parameters**
- **ip ip-filter-id** — Specifies IP filter policy. The filter ID must already exist within the created IP filters.
  - **Values**
    - `1 — 65535`
- `ipv6 ipv6-filter-id` — Specifies the IPv6 filter policy. The filter ID must already exist within the created IPv6 filters.
  - **Values**
    - `1 — 65535`
- `mac mac-filter-id` — Specifies the MAC filter policy. The specified filter ID must already exist within the created MAC filters. The filter policy must already exist within the created MAC filters.
  - **Values**
    - `1 — 65535`
encap-type

Syntax  
encap-type \{dot1q | null\}

no encap-type

Context  
config>service>egress-multicast-group>sap-common-requirements

Description  
This command specifies the encapsulation type that must exist on the SAP’s access port to allow the SAP membership within the egress-multicast-group. The \texttt{config>port>ethernet>access>encap-type} command is used to define the encapsulation type for the Ethernet port. The allowed encapsulation type values are dot1q and null. If the SAP does not exist on a port with the specified encap-type, it will not be allowed into the egress-multicast-group.

If at least one SAP is currently a member of the efficient-multicast-group, the \texttt{encap-type} cannot be changed within the sap-common-requirements node. If the efficient-multicast-group does not contain any member SAPs, the \texttt{encap-type} may be changed at any time.

There is no interaction between an efficient-multicast-group and the corresponding access ports associated with its members since all SAPs must be deleted from a port before its encap-type can be changed. When the SAPs are deleted from the port, they are also automatically deleted from the efficient-multicast-group.

The \texttt{no} form of the command returns the egress-multicast-group required encapsulation type for SAPs to dot1q. If the current encap-type is set to null, the command cannot be executed when SAPs exist within the egress-multicast-group.

Default  
dot1q — For an egress-multicast-group.

null — If member SAPs are on a null encapsulated access port.

Parameters  
null — The \texttt{null} keyword is mutually exclusive with the \texttt{dot1q} keyword. When the encap-type within the sap-common-requirements is specified to be null, the encapsulation type for the access ports associated with all SAPs within the egress-multicast-group must be set to null.

dot1q — The \texttt{dot1q} keyword is mutually exclusive with the \texttt{null} keyword. When the encap-type within the sap-common-requirements is specified to be dot1q, the encapsulation type for the access ports associated with all SAPs within the egress-multicast-group must be set to dot1q.

qinq-etype

Syntax  
qinq-etype \{0x0600..0xffff\}

no qinq-etype

Context  
config>service>egress-multicast-group>sap-common-requirements

Description  
This command specifies the Ethertype used for QinQ encapsulation.

Default  
no qinq-etype

ethertype — Defines the dot1q EtherType that must be associated with a SAP’s access port when the encap-type is set to dot1q. Any valid EtherType may be specified.

Values  
[0x0600 — 0xffff]: [1536 — 65535] in decimal or hex
Egress Multicast Group Commands

**qinq-fixed-tag-value**

**Syntax**

```
qinq-fixed-tag-value tag-value
no qinq-fixed-tag-value
```

**Context**

config>service>egress-multicast-group>sap-common-requirements

**Description**

This command configures the fixed tag value used for QinQ encapsulation.

**Default**

no qinq-fixed-tag-value

**Parameters**

`tag-value` — Specifies the provisioned common value of the fixed 802.1Q tag of all the QinQ SAP's in this egress multicast group.

The value 0 is used to indicate that the actual value of the fixed tag will be defined implicitly by the corresponding tag of the first SAP added to this egress multicast group.

**Values**

0, 1 — 4094

**dot1q-etype**

**Syntax**

```
dot1q-etype [0x0600..0xffff]
no dot1q-etype
```

**Context**

config>service>egress-multicast-group>sap-common-requirements

**Description**

This command specifies the dot1q EtherType that must exist on the SAP’s access port to allow the SAP membership within the egress-multicast-group. The `config>port>ethernet>access>dot1q-etype` command is used to define the EtherType used when encapsulating a packet with a dot1q tag on the Ethernet port. Any valid EtherType is allowed on the port.

If the current encap-type for the egress-multicast-group is set to null, the dot1q-etype EtherType is ignored when evaluating SAP membership in the group. If the encap-type is set to dot1q (the default), a member SAP’s access port must be configured with the same dot1q-etype EtherType as the egress-multicast-group.

If at least one SAP is currently a member of the efficient-multicast-group, the dot1q-etype value cannot be changed within the sap-common-requirements node. If the efficient-multicast-group does not contain any member SAPs, the dot1q-etype value may be changed at any time.

If an access port currently has SAPs associated with it that are defined within an egress-multicast-group and the port is currently set to encap-type dot1q, the dot1q-etype value defined on the port cannot be changed.

The no form of the command returns the egress-multicast-group dot1q EtherType to the default value of 0x8100. If the current encap-type is set to a value other then 0x8100, the command cannot be executed when SAPs exist within the egress-multicast-group.

**Default**

The default dot1q-etype is 0x8100 for an egress-multicast-group.

**Parameters**

`ethertype` — Defines the dot1q EtherType that must be associated with a SAP’s access port when the encap-type is set to dot1q. Any valid EtherType may be specified.

**Values**

0x0600 — 0xffff 1536 — 65535 in decimal or hex

**Default**

0x8100
BGP Auto-Discovery Commands

bgp

**Syntax**
```
bgp
```

**Context**
```
config>service>vpls
```

**Description**
This command enables the context to configure the BGP related parameters for both BGP AD and BGP VPLS.

bgp-vpls

**Syntax**
```
bgp-vpls
```

**Context**
```
config>service>vpls
```

**Description**
This command enables the context to configure the BGP-VPLS parameters and addressing.

max-ve-id

**Syntax**
```
max-ve-id value
no max-ve-id
```

**Context**
```
config>service>vpls>bgp-vpls
```

**Description**
This command configures the allowed range for the VE-id value: locally configured and received in a NLRI. Configuration of a VE-id higher than the value specified in this command is not allowed.

Also upon reception of a higher VE-id in an NLRI imported in this VPLS instance (RT = configured import RT) the following action must be taken:

- a trap must be generated informing the operator of the mismatch.
- NLRI must be dropped
- no service labels are to be installed for this VE-id
- no new NLRI must be generated if a new offset is required for VE-id.

The **no** form of this command sets the max-ve-id to un-configured. The BGP VPLS status should be administratively down for “no max-ve-id” to be used.

The max-ve-id value can be changed without shutting down bgp-vpls if the newly provisioned value does not conflict with the already configured local VE-ID. If the value of the local-VE-ID is higher than the new max-ve-id value the command is rejected. The operator needs to decrease first the VE-ID before running the command.

The actions taken for other max-ve-id values are described below:

- max-ve-id value higher than all VE-IDs (local and received) is allowed and there are no effects.
BGP Auto-Discovery Commands

- max-ve-id higher than the local VE-ID but smaller than the remote VE-IDs:
  - Provisioning is allowed
  - A warning message will be generated stating that “Higher VE-ID values were received in the BGP VPLS context. Related pseudowires will be removed.”
  - The pseudowires associated with the higher VE-IDs will be removed locally.
  - Note that this is a situation that should be corrected by the operator as the pseudowire may be down just at the local PE, consuming unnecessarily core bandwidth. The higher VE-IDs should be removed or lowered.

If the max-ve-id has increased a BGP route refresh is sent to the VPLS community to get the routes which might have been rejected earlier due to max-ve-id check. Default no max-ve-id – max-ve-id is not configured. A max-ve-id value needs to be provisioned for BGP VPLS to be in “no shutdown” state.

Default no max-ve-id

Parameters value — Specifies the allowed range of [1-value] for the VE-id. The configured value must be bigger than the existing VE-ids.

Values 1-65535

ve-name

Syntax ve-name name
no ve-name

Context config>service>vpls>bgp-vpls

Description This command creates or edits a ve-name. Just one ve-name can be created per BGP VPLS instance. The no form of the command removes the configured ve-name from the bgp vpls node. It can be used only when the BGP VPLS status is shutdown. Command “no shutdown” cannot be used if there is no ve-name configured.

Default no ve-name

Parameters name — A character string identifying the VPLS Edge instance.

Values 32 ASCII chars max

ve-id

Syntax ve-id ve-id-value
no ve-id

Context config>service>vpls>bgp-vpls>ve-name

Description This command configures a ve-id. Just one ve-id can be configured per BGP VPLS instance. The VE-ID can be changed without shutting down the VPLS Instance. When the VE-ID changes, BGP is withdrawing its own previously advertised routes and sending a route-refresh to all the peers which
would result in reception of all the remote routes again. The old pseudowires are removed and new ones are instantiated for the new VE-ID value.

The no form of the command removes the configured ve-id. It can be used just when the BGP VPLS status is shutdown. Command “no shutdown” cannot be used if there is no ve-id configured.

**Default**

no ve-id

**Parameters**

value — A two bytes identifier that represents the local instance in a VPLS and is advertised through the BGP NLRI. Must be lower or equal with the max-ve-id.

**Values**

1-65535

---

shutdown

**Syntax**

[no] shutdown

**Context**

config>service>vpls>bgp-vpls

**Description**

This command administratively enables/disables the local BGP VPLS instance. On de-activation an MP-UNREACH-NLRI must be sent for the local NLRI.

The no form of the command enables the BGP VPLS addressing and the related BGP advertisement. The associated BGP VPLS MP-REACH-NLRI will be advertised in an update message and the corresponding received NLRIs must be considered to instantiate the data plane. RT, RD usage: same like in the BGP AD solution, if the values are not configured here, the value of the VPLS-id from under the bgp-ad node is used. If VPLS-id value is not configured either the MH site cannot be activated – i.e. no shutdown returns an error. Same applies if a pseudowire template is not specified under the bgp node.

**Default**

shutdown

---

bgp-ad

**Syntax**

[no] bgp-ad

**Context**

config>service>vpls

**Description**

This command configures BGP auto-discovery.

---

pw-template-binding

**Syntax**

pw-template-binding policy-id [split-horizon-group group-name] [import-rt {ext-community, ...(up to 5 max)}]  
no pw-template-bind policy-id

**Context**

config>service>vpls>bgp-ad  
config>service>vpls>bgp
**Description**  
This command binds the advertisements received with the route target (RT) that matches the configured list (either the generic or the specified import) to a specific pw-template. If the RT list is not present the pw-template is used for all of them.

The pw-template-binding applies to both BGP-AD and BGP-VPLS if these features are enabled in the VPLS.

For BGP VPLS the following additional rules govern the use of pseudowire-template:

- On transmission the settings for the L2-Info extended community in the BGP Update are derived from the pseudowire template attributes. If multiple pseudowire templates (with or without import-rt) are specified for the same VPLS instance the first pw-template entry will be used.

- On reception the values of the parameters in the L2-Info extended community of the BGP Update are compared with the settings from the corresponding pw-template. The following steps are used to determine the local pw-template:
  - The RT values are matched to determine the pw-template.
  - If multiple pw-templates matches are found from the previous steps, the first configured pw-template entry will be considered.
  - If the values used for Layer 2 MTU or C Flag do not match the pseudowire setup fails.

The tools perform commands can be used to control the application of changes in pw-template for both BGP-AD and BGP-VPLS.

The no form of the command removes the values from the configuration.

**Default**  
none

**Parameters**  

- **policy-id** — Specifies an existing policy ID.

  **Values**  
  1 — 2147483647

- **split-horizon-group**  
  group-name — The specified group-name overrides the split horizon group template settings.

- **import-rt ext-comm** — Specify communities allowed to be accepted from remote PE neighbors. An extended BGP community in the \( \text{type:x:y} \) format. The value \( x \) can be an integer or IP address. The type can be the target or origin. \( x \) and \( y \) are 16-bit integers.

  **Values**  
  
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-addr</td>
<td>a.b.c.d</td>
</tr>
<tr>
<td>comm-val</td>
<td>0 — 65535</td>
</tr>
<tr>
<td>2byte-asnumber</td>
<td>0 — 65535</td>
</tr>
<tr>
<td>ext-comm-val</td>
<td>0 — 4294967295</td>
</tr>
<tr>
<td>4byte-asnumber</td>
<td>0 — 4294967295</td>
</tr>
</tbody>
</table>

**bfd-enable**

**Syntax**  

[no] bfd-enable

**Context**  

config>service>vpls:bgp>pw-template-bindin

**Description**  
This command enables the use of bi-directional forwarding (BFD) to control the state of the associated protocol interface. By enabling BFD on a given protocol interface, the state of the protocol
interface is tied to the state of the BFD session between the local node and the remote node. The parameters used for the BFD are set via the BFD command under the IP interface.

The no form of this command removes BFD from the associated IGP/BGP protocol adjacency.

Default no bfd-enable

oper-group

Syntax oper-group group-name
no oper-group

Context config>service>vpls>sap
config>service>vpls>spoke-sdp
config>service>vpls>bgp>pw-template-binding

Description This command associates the context to which it is configured to the operational group specified in the group-name. The oper-group group-name must be already configured under config>service context before its name is referenced in this command.

The no form of the command removes the association.

Parameters group-name — Specifies a character string of maximum 32 ASCII characters identifying the group instance.

route-target

Syntax route-target {ext-community}{[export ext-community][import ext-community]}
no route-target

Context config>service>vpls>bgp-ad
config>service>vpls>bgp

Description This command configures the route target (RT) component that will be signaled in the related MP-BGP attribute to be used for BGP auto-discovery, BGP VPLS and BGP Multi-Homing if these features are configured in this VPLS service.

If this command is not used, the RT is built automatically using the VPLS ID. The ext-comm can have the same two formats as the VPLS ID, a two-octet AS-specific extended community, IPv4 specific extended community.

The following rules apply:

- if BGP AD VPLS-id is configured & no RT is configured under BGP node - RT = VPLS-ID
- if BGP AD VPLS-id is not configured then an RT value must be configured under BGP node (this is the case when only BGP VPLS is configured)
- if BGP AD VPLS-id is configured and an RT value is also configured under BGP node, the configured RT value prevails

Parameters export ext-community — Specify communities allowed to be sent to remote PE neighbors.
import ext-community — Specify communities allowed to be accepted from remote PE neighbors.

vpls-id

Syntax

vpls-id vpls-id

Context

config>service>vpls>bgp-ad

Description

This command configures the VPLS ID component that will be signaled in one of the extended community attributes (ext-comm).

Values and format (6 bytes, other 2 bytes of type-subtype will be automatically generated)

Parameters

vpls-id — Specifies a globally unique VPLS ID for BGP auto-discovery in this VPLS service.

Values

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-addr</td>
<td>a.b.c.d</td>
</tr>
<tr>
<td>comm-val</td>
<td>0 — 65535</td>
</tr>
<tr>
<td>as-number</td>
<td>1..65535</td>
</tr>
<tr>
<td>ext-comm-val</td>
<td>0..4294967295</td>
</tr>
</tbody>
</table>

vsi-export

Syntax

vsi-export policy-name [policy-name...(up to 5 max)]

no vsi-export

Context

config>service>vpls>bgp-ad
config>service>vpls>bgp

Description

This command specifies the name of the VSI export policies to be used for BGP auto-discovery, BGP VPLS and BGP Multi-Homing if these features are configured in this VPLS service. If multiple policy names are configured, the policies are evaluated in the order they are specified. The first policy that matches is applied.

The policy name list is handled by the SNMP agent as a single entity.

vsi-id

Syntax

vsi-id

Context

config>service>vpls>bgp-ad

Description

This command enables the context to configure the Virtual Switch Instance Identifier (VSI-ID).
prefix

Syntax

prefix low-order-vsi-id
no prefix

Context

config>service>vpls>bgp-ad>vsi-id

Description

This command specifies the low-order 4 bytes used to compose the Virtual Switch Instance Identifier (VSI-ID) to use for NLRI in BGP auto-discovery in this VPLS service.

If no value is set, the system IP address will be used.

Default

no prefix

Parameters

low-order-vsi-id — Specifies a unique VSI ID.

Values

0—4294967295

route-distinguisher

Syntax

route-distinguisher [ip-addr:comm-val | as-number:ext-comm-val]
no route-distinguisher

Context

config>service>vpls>bgp-ad>vsi-id
config>service>vpls:bgp

Description

This command configures the Route Distinguisher (RD) component that will be signaled in the MP-BGP NLRI for L2VPN AFI. This value will be used for BGP-AD, BGP VPLS and BGP Multi-Homing NLRI if these features are configured.

If this command is not configured, the RD is automatically built using the BGP-AD VPLS ID. The following rules apply:

• if BGP AD VPLS-id is configured & no RD is configured under BGP node - RD = VPLS-ID
• if BGP AD VPLS-id is not configured then an RD value must be configured under BGP node (this is the case when only BGP VPLS is configured)
• if BGP AD VPLS-id is configured and an RD value is also configured under BGP node, the configured RD value prevails

Values and format (6 bytes, other 2 bytes of type will be automatically generated)

Parameters

ip-addr:comm-val — Specifies the IP address.

Values

ip-addr a.b.c.d
comm-val 0 — 65535

as-number:ext-comm-val — Specifies the AS number and the

Values

as-number 1 — 65535
ext-comm-val 0 — 4294967295
BGP Auto-Discovery Commands

vsi-import

Syntax

vsi-import policy-name [policy-name...(up to 5 max)]
no vsi-import

Context

config>service>vpls>bgp-ad>vsi-id
config>service>vpls>bgp

Description

This command specifies the name of the VSI import policies to be used for BGP auto-discovery, BGP VPLS and BGP Multi-Homing if these features are configured in this VPLS service. If multiple policy names are configured, the policies are evaluated in the order they are specified. The first policy that matches is applied.

The policy name list is handled by the SNMP agent as a single entity.

bgp-evpn

Syntax

bgp-evpn
[no] bgp-evpn

Context

config>service>vpls

Description

This command enables the context to configure the BGP EVPN parameters.

mac-advertisement

Syntax

mac-advertisement
[no] mac-advertisement

Context

config>service>vpls>bgp-evpn

Description

The mac-advertisement command enables the advertisement in BGP of the learnt macs on SAPs and SDP bindings. When the mac-advertisement is disabled, the local macs will be withdrawn in BGP.

Default

mac-advertisement

mac-duplication

Syntax

mac-duplication

Context

config>service>vpls>bgp-evpn

Description

This command enables the context to configure the BGP EVPN mac duplication parameters.
detect

Syntax  detect num-moves num-moves window minutes
Context  config>service>vpls>bgp-evpn>mac-duplication
Description  Mac-duplication is always enabled. This command modifies the default behavior. Mac-duplication monitors the number of moves of a MAC address for a period of time (window).
Default  num-moves 5 window 3
Parameters  num-moves — Identifies the number of mac moves in a VPLS service. The counter is incremented when a given MAC is locally relearned in the FDB or flushed from the FDB due to the reception of a better remote EVPN route for that MAC.
           Values  3..10 minutes
           Default  3 minutes

retry

Syntax  retry minutes [no] retry
Context  config>service>vpls>bgp-evpn>mac-duplication
Description  Specifies the timer after which the MAC in hold-down state is automatically flushed and the mac-duplication process starts again. This value is expected to be equal to two times or more than that of window.
If no retry is configured, this implies that, once mac-duplication is detected, mac updates for that mac will be held down till the user intervenes or a network event (that flushes the mac) occurs.
Default  9 minutes
Parameters  minutes — I.
           Values  2 — 60 minutes

unknown-mac-route

Syntax  unknown-mac-route [no] unknown-mac-route
Context  config>service>vpls>bgp-evpn
Description  This command enables the advertisement of the unknown-mac-route in BGP. This will be coded in an EVPN mac route where the mac address is zero and the mac address length 48. By using this unknown-mac-route advertisement, the user may decide to optionally turn off the advertisement of MAC addresses learnt from saps and sdp-bindings, hence reducing the control plane overhead and the size of the FDB tables in the data center. All the receiving NVEs supporting this concept will send any unknown-unicast packet to the owner of the unknown-mac-route, as opposed to flooding the
unknown-unicast traffic to all other nodes part of the same VPLS. Note that, although the 7x50 can be configured to generate and advertise the unknown-mac-route, the 7x50 will never honor the unknown-mac-route and will flood to the vpls flood list when an unknown-unicast packet arrives to an ingress sap/sdp-binding.

Default  no unknown-mac-route

vxlan

Syntax  vxlan
Context  config>service>vpls>bgp-evpn
Description  This command enables the context to configure the VXLAN parameters when BGP EVPN is used as the control plane.

shutdown

Syntax  [no] shutdown
Context  config>service>vpls>bgp-evpn.vxlan
Description  This command enables/disables the automatic creation of VXLAN auto-bindings by BGP-EVPN.
Default  shutdown
IEEE 802.1ah Provider Backbone Bridging

In This Chapter

This chapter provides information about Provider Backbone Bridging (PBB), process overview, and implementation notes.

Topics in this chapter include:

- IEEE 802.1ah Provider Backbone Bridging (PBB) Overview on page 938
- PBB Features on page 939
  - Integrated PBB-VPLS Solution on page 939
  - PBB Technology on page 941
  - PBB Mapping to Existing VPLS Configurations on page 942
  - SAP and SDP Support on page 944
  - PBB Packet Walkthrough on page 946
  - IEEE 802.1ak MMRP for Service Aggregation and Zero Touch Provisioning on page 971
  - MMRP Support Over B-VPLS SAPs and SDPs on page 973
  - PBB and BGP-AD on page 978
  - PBB ELINE Service on page 978
  - MAC Flush on page 981
  - Access Multi-Homing for Native PBB (B-VPLS over SAP Infrastructure) on page 986
  - PBB and IGMP Snooping on page 999
  - PBB QoS on page 1000
  - PBB OAM on page 1016
- Configuration Examples on page 1018
IEEE 802.1ah Provider Backbone Bridging (PBB) Overview

IEEE 802.1ah draft standard (IEEE802.1ah), also known as Provider Backbone Bridges (PBB), defines an architecture and bridge protocols for interconnection of multiple Provider Bridge Networks (PBNs - IEEE802.1ad QinQ networks). PBB is defined in IEEE as a connectionless technology based on multipoint VLAN tunnels. IEEE 802.1ah employs Provider MSTP as the core control plane for loop avoidance and load balancing. As a result, the coverage of the solution is limited by STP scale in the core of large service provider networks.

Virtual Private LAN Service (VPLS), RFC 4762, *Virtual Private LAN Service (VPLS) Using Label Distribution Protocol (LDP) Signaling*, provides a solution for extending Ethernet LAN services using MPLS tunneling capabilities through a routed, traffic-engineered MPLS backbone without running (M)STP across the backbone. As a result, VPLS has been deployed on a large scale in service provider networks.

Alcatel-Lucent’s implementation fully supports a native PBB deployment and an integrated PBB-VPLS model where desirable PBB features such as MAC hiding, service aggregation and the service provider fit of the initial VPLS model are combined to provide the best of both worlds.
PBB Features

Integrated PBB-VPLS Solution

HVPLS introduced a service-aware device in a central core location in order to provide efficient replication and controlled interaction at domain boundaries. The core network facing provider edge (N-PE) devices have knowledge of all VPLS services and customer MAC addresses for local and related remote regions resulting in potential scalability issues as depicted in Figure 112.

In a large VPLS deployment, it is important to improve the stability of the overall solution and to speed up service delivery. These goals are achieved by reducing the load on the N-PEs and respectively minimizing the number of provisioning touches on the N-PEs.

The integrated PBB-VPLS model introduces an additional PBB hierarchy in the VPLS network to address these goals as depicted in Figure 113.
PBB encapsulation is added at the user facing PE (U-PE) to hide the customer MAC addressing and topology from the N-PE devices. The core N-PEs need to only handle backbone MAC addressing and do not need to have visibility of each customer VPN. As a result, the integrated PBB-VPLS solution decreases the load in the N-PEs and improves the overall stability of the backbone.

Alcatel-Lucent’s PBB-VPLS solution also provides automatic discovery of the customer VPNs through the implementation of IEEE 802.1ak MMRP minimizing the number of provisioning touches required at the N-PEs.

Figure 113: Large PBB-VPLS Deployment
IEEE 802.1ah specification encapsulates the customer or QinQ payload in a provider header as shown in Figure 114.

Figure 114: QinQ Payload in Provider Header Example

PBB Technology

IEEE 802.1ah specification encapsulates the customer or QinQ payload in a provider header as shown in Figure 114.

PBB adds a regular Ethernet header where the B-DA and B-SA are the backbone destination and respectively, source MACs of the edge U-PEs. The backbone MACs (B-MACs) are used by the core N-PE devices to switch the frame through the backbone.

A special group MAC is used for the backbone destination MAC (B-DA) when handling an unknown unicast, multicast or broadcast frame. This backbone group MAC is derived from the I-service instance identifier (ISID) using the rule: a standard group OUI (01-1E-83) followed by the 24 bit ISID coded in the last three bytes of the MAC address.

The BVID (backbone VLAN ID) field is a regular DOT1Q tag and controls the size of the backbone broadcast domain. When the PBB frame is sent over a VPLS pseudo-wire (pseudowire), this field may be omitted depending on the type of pseudowire used.

The following ITAG (standard Ether-type value of 0x88E7) has the role of identifying the customer VPN to which the frame is addressed through the 24 bit ISID. Support for service QoS is provided through the priority (3 bit I-PCP) and the DEI (1 bit) fields.
PBB Mapping to Existing VPLS Configurations

The IEEE model for PBB is organized around a B-component handling the provider backbone layer and an I-component concerned with the mapping of the customer/provider bridge (QinQ) domain (MACs, VLANs) to the provider backbone (B-MACs, B-VLANs): for example, the I-component contains the boundary between the customer and backbone MAC domains.

Alcatel-Lucent’s implementation is extending the IEEE model for PBB to allow support for MPLS pseudowires using a chain of two VPLS context linked together as depicted in Figure 115.

![Figure 115: PBB Mapping to VPLS Constructs](image)

A VPLS context is used to provide the backbone switching component. The white circle marked B, referred to as backbone-VPLS (B-VPLS), operates on backbone MAC addresses providing a core multipoint infrastructure that may be used for one or multiple customer VPNs. Alcatel-Lucent’s B-VPLS implementation allows the use of both native PBB and MPLS infrastructures.

Another VPLS context (I-VPLS) can be used to provide the multipoint I-component functionality emulating the ELAN service (refer to the triangle marked “I” in Figure 115). Similar to B-VPLS, I-VPLS inherits from the regular VPLS the pseudowire (SDP bindings) and native Ethernet (SAPs) handoffs accommodating this way different types of access: for example, direct customer link, QinQ or HVPLS.
In order to support PBB ELINE (point-to-point service), the use of an Epipe as I-component is allowed. All Ethernet SAPs supported by a regular Epipe are also supported in the PBB Epipe.
SAP and SDP Support

PBB B-VPLS

- SAPs
  - Ethernet DOT1Q and QinQ are supported — This is applicable to most PBB use cases, for example, one backbone VLAN ID used for native Ethernet tunneling. In the case of QinQ, a single tag x is supported on a QinQ encapsulation port for example (1/1/1:x.* or 1/1/1:x.0).
  - Ethernet null is supported — This is supported for a direct connection between PBB PEs, for example, no BVID is required.
  - Default SAP types are blocked in the CLI for the B-VPLS SAP.
- The following rules apply to the SAP processing of PBB frames:
  - For “transit frames” (not destined to a local BMAC), there is no need to process the ITAG component of the PBB frames. Regular Ethernet SAP processing is applied to the backbone header (BMACs and BVID).
  - If a local I-VPLS instance is associated with the B-VPLS, “local frames” originated/terminated on local I-VPLS(s) are PBB encapsulated/de-encapsulated using the pbb-etype provisioned under the related port or SDP component.
- SDPs
  - For MPLS, both mesh and spoke-SDPs with split horizon groups are supported.
  - Similar to regular pseudowire, the outgoing PBB frame on an SDP (for example, B-pseudowire) contains a BVID qtag only if the pseudowire type is Ethernet VLAN. If the pseudowire type is ‘Ethernet’, the BVID qtag is stripped before the frame goes out.

PBB I-VPLS

- Port Level
  - All existing Ethernet encapsulation types are supported (for example, null, dot1q, qinq).
- SAPs
  - The I-VPLS SAPs can co-exist on the same port with SAPs for other business services, for example, VLL, VPLS SAPs.
  - All existing Ethernet encapsulation are supported: null, dot1q, qinq.
- **SDPs**
  - GRE and MPLS SDP are spoke-sdp only. Mesh SDPs can just be emulated by using the same split horizon group everywhere.

Existing SAP processing rules still apply for the I-VPLS case; the SAP encapsulation definition on Ethernet ingress ports defines which VLAN tags are used to determine the service that the packet belongs to:

- Null encap defined on ingress — Any VLAN tags are ignored and the packet goes to a default service for the SAP;
- Dot1q encap defined on ingress — only first VLAN tag is considered;
- QinQ encap defined on ingress — both VLAN tags are considered; wildcard support for the inner VLAN tag
- For dot1q/qinQ encapsulations, traffic encapsulated with VLAN tags for which there is no definition is discarded.
- Note that any VLAN tag used for service selection on the I-SAP is stripped before the PBB encapsulation is added. Appropriate VLAN tags are added at the remote PBB PE when sending the packet out on the egress SAP.
PBB Packet Walkthrough

This section describes the walkthrough for a packet that traverses the B-VPLS and I-VPLS instances using the example of a unicast frame between two customer stations as depicted in the following network diagram Figure 116.

The station with CMAC (customer MAC) X wants to send a unicast frame to CMAC Y through the PBB-VPLS network. A customer frame arriving at PBB-VPLS U-PE1 is encapsulated with the PBB header. The local I-VPLS FIB on U-PE1 is consulted to determine the destination BMAC of
the egress U-PE for CMAC Y. In our example, B2 is assumed to be known as the B-DA for Y. If CMAC Y is not present in the U-PE1 forwarding database, the PBB packet is sent in the B-VPLS using the standard group MAC address for the ISID associated with the customer VPN. If the uplink to the N-PE is a spoke pseudowire, the related PWE3 encapsulation is added in front of the B-DA.

Next, only the Backbone Header in green is used to switch the frame through the green B-VPLS/VPLS instances in the N-PEs. At the receiving U-PE2, the CMAC X is learned as being behind BMAC B1; then the PBB encapsulation is removed and the lookup for CMAC Y is performed. In the case where a pseudowire is used between N-PE and U-PE2, the pseudowire encapsulation is removed first.

---

**PBB Control Planes**

PBB technology can be deployed in a number of environments. Natively, PBB is an Ethernet data plane technology that offers service scalability and multicast efficiency.

Environment:

- MPLS (mesh and spoke SDPs)
- Ethernet SAPs

Within these environments, SR OS offers a number of optional control planes:

- Shortest Path Bridging MAC (SPBM) (SAPs and spoke SDPs); see Shortest Path Bridging MAC Mode (SPBM) on page 948
- Rapid Spanning Tree Protocol (RSTP) optionally with MMRP (SAPs and spoke SDPs); see MMRP Support Over B-VPLS SAPs and SDPs on page 973.
- Multiple Spanning Tree Protocol (MSTP) optionally with MMRP (SAPs and spoke SDPs); see Multiple Spanning Tree on page 563.
- Multiple MAC registration Protocol (MMRP) alone (SAPs, spoke and mesh SDPs); see IEEE 802.1ak MMRP for Service Aggregation and Zero Touch Provisioning on page 971.

In general a control plane is required on Ethernet SAPs, or SDPs where there could be physical loops. Some network configurations of Mesh and Spoke SDPs can avoid physical loops and no control plane is required.

The choice of control plane is based on the requirement of the networks. SPBM for PBB offers a scalable link state control plane without BMAC flooding and learning or MMRP. RSTP and MSTP offer Spanning tree options based on BMAC flooding and learning. MMRP is used with flooding and learning to improve multicast.
Shortest Path Bridging MAC Mode (SPBM)

Shortest Path Bridging (SPB) enables a next generation control plane for PBB based on IS-IS that adds the stability and efficiency of link state to unicast and multicast services. Specifically this is an implementation of SPBM (SPB MAC mode). Current SR OS PBB B-VPLS offers point to point and multipoint to multipoint services with large scale. PBB B-VPLS is deployed in both Ethernet and MPLS networks supporting Ethernet VLL and VPLS services. SPB removes the flooding and learning mode from the PBB Backbone network and replaces MMRP for ISID Group Mac Registration providing flood containment. SROS SPB provides true shortest path forwarding for unicast and efficient forwarding on a single tree for multicast. It supports selection of shortest path equal cost tie-breaking algorithms to enable diverse forwarding in an SPB network.

Flooding and Learning Versus Link State

SPB brings a link state capability that improves the scalability and performance for large networks over the xSTP flooding and learning models. Flooding and learning has two consequences. First, a message invoking a flush must be propagated, second the data plane is allowed to flood and relearn while flushing is happening. Message based operation over these data planes may experience congestion and packet loss.

Table 13: B-VPLS Control Planes

<table>
<thead>
<tr>
<th>PBB B-VPLS Control Plane</th>
<th>Flooding and Learning</th>
<th>Multipath</th>
<th>Convergence time</th>
</tr>
</thead>
<tbody>
<tr>
<td>xSTP</td>
<td>Yes</td>
<td>MSTP</td>
<td>xSTP + MMRP</td>
</tr>
<tr>
<td>G.8032</td>
<td>Yes</td>
<td>Multiple Ring instances</td>
<td>Eth-OAM based + MMRP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Ring topologies only</td>
<td></td>
</tr>
<tr>
<td>SPB-M</td>
<td>No</td>
<td>Yes –ECT based</td>
<td>IS-IS link state (incremental)</td>
</tr>
</tbody>
</table>

Link state operates differently in that only the information that truly changes needs to be updated. Traffic that is not affected by a topology change does not have to be disturbed and does not experience congestion since there is no flooding. SPB is a link state mechanism that uses restoration to reestablish the paths affected by topology change. It is more deterministic and reliable than RSTP and MMRP mechanisms. SPB can handle any number of topology changes and as long as the network has some connectivity, SPB will not isolate any traffic.
SPB for B-VPLS

The SROS model supports PBB Epipes and I-VPLS services on the B-VPLS. SPB is added to B-VPLS in place of other control planes (see Table 13). SPB runs in a separate instance of IS-IS. SPB is configured in a single service instance of B-VPLS that controls the SPB behavior (via IS-IS parameters) for the SPB IS-IS session between nodes. Up to four independent instances of SPB can be configured. Each SPB instance requires a separate control B-VPLS service. A typical SPB deployment uses a single control VPLS with zero, one or more user B-VPLS instances. SPB is multi-topology (MT) capable at the IS-IS LSP TLV definitions however logical instances offer the nearly the same capability as MT. The SROS SPB implementation always uses MT topology instance zero. Area addresses are not used and SPB is assumed to be a single area. SPB must be consistently configured on nodes in the system. SPB Regions information and IS-IS hello logic that detect mismatched configuration are not supported.

SPB Link State PDUs (LSPs) contains BMACs, I-SIDs (for multicast services) and link and metric information for an IS-IS database. Epipe I-SIDs are not distributed in SROS SPB allowing high scalability of PBB Epipes. I-VPLS I-SIDs are distributed in SROS SPB and the respective multicast group addresses are automatically populated in forwarding in a manner that provides automatic pruning of multicast to the subset of the multicast tree that supports I-VPLS with a common I-SID. This replaces the function of MMRP and is more efficient than MMRP so that in the future SPB will scale to a greater number of I-SIDs.

SPB on SROS can leverage MPLS networks or Ethernet networks or combinations of both. SPB allows PBB to take advantage of multicast efficiency and at the same time leverage MPLS features such as resiliency.

Control B-VPLS and User B-VPLS

Control B-VPLS are required for the configuration of the SPB parameters and as a service to enable SPB. Control B-VPLS therefore must be configured everywhere SPB forwarding is expected to be active even if there are no terminating services. SPB uses the logical instance and a Forwarding ID (FID) to identify SPB locally on the node. The FID is used in place of the SPB VLAN identifier (Base VID) in IS-IS LSPs enabling a reference to exchange SPB topology and addresses. More specifically, SPB advertises B-MACs and I-SIDs in a B-VLAN context. Since the service model in SROS separates the VLAN Tag used on the port for encapsulation from the VLAN ID used in SPB the SPB VLAN is a logical concept and is represented by configuring a FID. B-VPLS SAPs use VLAN Tags (SAPs with Ethernet encapsulation) that are independent of the FID value. The encapsulation is local to the link in SR/ESS so the SAP encapsulation has be configured the same between neighboring switches. The FID for a given instance of SPB between two neighbor switches must be the same. The independence of VID encapsulation is inherent to SROS PBB B-VPLS. This also allows spoke SDP bindings to be used between neighboring SPB instances without any VID tags. The one exception is mesh SDPs are not supported but arbitrary mesh topologies are supported by SROS SPB.
Figure 117 illustrates two switches where an SPB control B-VPLS configured with FID 1 and uses a SAP with 1/1/1:5 therefore using a VLAN Tag 5 on the link. The SAP 1/1/1:1 could also have been be used but in SROS the VID does not have to equal FID. Alternatively an MPLS PW (spoke SDP binding) could be for some interfaces in place of the SAP. Figure 117 illustrates a control VPLS and two user B-VPLS. The User B-VPLS must share the same topology and are required to have interfaces on SAPs/Spoke SDPs on the same links or LAG groups as the B-VPLS. To allow services on different B-VPLS to use a path when there are multiple paths a different ECT algorithm can be configured on a B-VPLS instance. In this case, the user B-VPLS still fate shared the same topology but they may use different paths for data traffic; see Shortest Path and Single Tree on page 952.

Figure 117: Control and User B-VPLS with FIDs

Each user B-VPLS offers the same service capability as a control B-VPLS and are configured to “follow” or fate share with a control B-VPLS. User B-VPLS must be configured as active on the whole topology where control B-VPLS is configured and active. If there is a mismatch between the topology of a user B-VPLS and the control B-VPLS, only the user B-VPLS links and nodes that are in common with the control B-VPLS will function. The services on any B-VPLS are independent of a particular user B-VPLS so a mis-configuration of one of the user B-VPLS will not affect other B-VPLS. For example if a SAP or spoke SDP is missing in the user B-VPLS any traffic from that user B-VPLS that would use that interface, will be missing forwarding information and traffic will be dropped only for that B-VPLS. The computation of paths is based only on the control B-VPLS topology.

User B-VPLS instances supporting only unicast services (PBB-Epipes) may share the FID with the other B-VPLS (control or user). This is a configuration short cut that reduces the LSP advertisement size for B-VPLS services but results in the same separation for forwarding between the B-VPLS services. In the case of PBB-Epipes only BMACs are advertised per FID but BMACs
are populated per B-VPLS in the FIB. If I-VPLS services are to be supported on a B-VPLS that B-VPLS must have an independent FID.
Shortest Path and Single Tree

IEEE 802.1aq standard SPB uses a source specific tree model. The standard model is more computationally intensive for multicast traffic since in addition to the SPF algorithm for unicast and multicast from a single node, an all pairs shortest path needs to be computed for other nodes in the network. In addition, the computation must be repeated for each ECT algorithm. While the standard yields efficient shortest paths, this computation is overhead for systems where multicast traffic volume is low. Ethernet VLL and VPLS unicast services are popular in PBB networks and the SROS SPB design is optimized for unicast delivery using shortest paths. Ethernet supporting unicast and multicast services are commonly deployed in Ethernet transport networks. SROS SPB Single tree multicast (also called shared tree or *,G) operates similarly today. The difference is that SPB multicast never floods unknown traffic.

The SR OS implementation of SPB with shortest path unicast and single tree multicast, requires only two SPF computations per topology change reducing the computation requirements. One computation is for unicast forwarding and the other computation is for multicast forwarding.

A single tree multicast requires selecting a root node much like RSTP. Bridge priority controls the choice of root node and alternate root nodes. The numerically lowest Bridge Priority is the criteria for choosing a root node. If multiple nodes have the same Bridge Priority, then the lowest Bridge Identifier (System Identifier) is the root.

In SPB the source-bmac can override the chassis-mac allowing independent control of tie breaking. The shortest path unicast forwarding does not require any special configuration other than selecting the ECT algorithm by configuring a B-VPLS use a FID with low-path-id algorithm or high-path-id algorithm to tie break between equal cost paths. Bridge priority allows some adjustment of paths. Configuring link metrics adjusts the number of equal paths.

To illustrate the behavior of the path algorithms a sample network is shown in Figure 118.

![Figure 118: Sample Partial Mesh network](image_url)
Assume that Node A is the lowest Bridge Identifier and the Multicast root node and all links have equal metrics. Also, assume that Bridge Identifiers are ordered such that Node A has a numerically lower Bridge identifier than Node B, and Node B has lower Bridge Identifier than Node C, etc. Unicast paths are configured to use shortest path tree (SPT). Figure 119 shows the shortest paths computed from Node A and Node E to Node F. There are only two shortest paths from A to F. A choice of low-path-id algorithm uses Node B as transit node and a path using high-path-id algorithm uses Node D as transit node. The reverse paths from Node F to A are the same (all unicast paths are reverse path congruent). For Node E to Node F there are three paths E-A-B-F, E-A-D-F, and E-C-D-F. The low-path-id algorithm uses path E-A-B-F and the high-path-id algorithm uses E-C-D-F. These paths are also disjoint and are reverse path congruent. Note that any nodes that are directly connected in this network have only one path between them (not shown for simplicity).

Figure 119: Unicast Paths for Low-path-id and High-path-id

For Multicast paths the algorithms used are the same low-path-id or high-path-id but the tree is always a single tree using the root selected as described earlier (in this case Node A). Figure 120 illustrates the multicast paths for low-path-id and high-path-id algorithm.
Figure 120: Multicast Paths for Low-path-id and High-path-id

All nodes in this network use one of these trees. Note that the path for multicast to/from Node A is the same as unicast traffic to/from Node A for both low-path-id and high-path-id. However, the multicast path for other nodes is now different from the unicast paths for some destinations. For example, Node E to Node F is now different for high-path-id since the path must transit the root Node A. In addition, the Node E multicast path to C is E-A-C even though E has a direct path to Node C. A rule of thumb is that the node chosen to be root should be a well-connected node and have available resources. In this example, Node A and Node D are the best choices for root nodes.

The distribution of I-SIDs allows efficient pruning of the multicast single tree on a per I-SID basis since only MFIB entries between nodes on the single tree are populated. For example, if Nodes A, B and F share an I-SID and they use the low-path-id algorithm only those three nodes would have multicast traffic for that I-SID. If the high-path-id algorithm is used traffic from Nodes A and B must go through D to get to Node F.
Data Path and Forwarding

The implementation of SPB on SROS uses the PBB data plane. There is no flooding of BMAC based traffic. If a BMAC is not found in the FDB, traffic is dropped until the control plane populates that BMAC. Unicast BMAC addresses are populated in all FDBs regardless of I-SID membership. There is a unicast FDB per B-VPLS both control B-VPLS and user BVPLS. B-VPLS instances that do not have any I-VPLS, have only a default multicast tree and do not have any multicast MFIB entries.

The data plane supports an ingress check (reverse path forwarding check) for unicast and multicast frames on the respective trees. Ingress check is performed automatically. For unicast or multicast frames the BMAC of the source must be in the FDB and the interface must be valid for that BMAC or traffic is dropped. The PBB encapsulation (See PBB Technology) is unchanged from current SROS. Multicast frames use the PBB Multicast Frame format and SPBM distributes I-VPLS I-SIDs which allows SPB to populate forwarding only to the relevant branches of the multicast tree. Therefore, SPB replaces both spanning tree control and MMRP functionality in one protocol.

By using a single tree for multicast the amount of MFIB space used for multicast is reduced. (Per source shortest path trees for multicast are not currently offered on SROS.) In addition, a single tree reduces the amount of computation required when there is topology change.

SPB Ethernet OAM

Ethernet OAM works on Ethernet services and use a combination of unicast with learning and multicast addresses (REF to OAM section). SPB on SROS supports both unicast and multicast forwarding, but with no learning and unicast and multicast may take different paths. In addition, SROS SPB control plane offers a wide variety of show commands. The SPB IS-IS control plane takes the place of many Ethernet OAM functions. SPB IS-IS frames (Hello and PDU etc) are multicast but they are per SPB interface on the control B-VPLS interfaces and are not PBB encapsulated.

All Client Ethernet OAM is supported from I-VPLS interfaces and PBB Epipe interfaces across the SPB domain. Client OAM is the only true test of the PBB data plane. The only forms of Eth-OAM supported directly on SPB B-VPLS are Virtual MEPS (vMEPs). Only CCM is supported on these vMEPs; vMEPs use a S-TAG encapsulation and follow the SPB multicast tree for the given B-VPLS. Each MEP has a unicast associated MAC to terminate various ETH-CFM tools. However, CCM messages always use a destination Layer 2 multicast using 01:80:C2:00:00:3x (where x = 0..7). vMEPs terminate CCM with the multicast address. Unicast CCM can be configured for point to point associations or hub and spoke configuration but this would not be typical (when unicast addresses are configured on vMEPs they are automatically distributed by SPB in IS-IS).
Up MEPs on services (I-VPLS and PBB Epipes) are also supported and these behave as any service OAM. These OAM use the PBB encapsulation and follow the PBB path to the destination.

Link OAM or 802.1ah EFM is supported below SPB as standard. This strategy of SPB IS-IS and OAM gives coverage.

### Table 14: SPB Ethernet OAM Operation Summary

<table>
<thead>
<tr>
<th>OAM Origination</th>
<th>Data Plane Support</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>PBB-Epipe or Customer CFM on PBB Epipe</td>
<td>Fully Supported</td>
<td></td>
</tr>
<tr>
<td>Up MEPs on PBB Epipe</td>
<td>Unicast PBB frames encapsulating unicast/multicast</td>
<td>Transparent operation. Uses Encapsulated PBB with Unicast B-MAC address</td>
</tr>
<tr>
<td>I-VPLS or Customer CFM on I-VPLS</td>
<td>Fully Supported</td>
<td>Transparent operation</td>
</tr>
<tr>
<td>Up MEPs on I-VPLS</td>
<td>Unicast/Multicast PBB frames determined by OAM type</td>
<td>Uses Encapsulated PBB frames with Multicast/Unicast BMAC address</td>
</tr>
<tr>
<td>vMEP on B-VPLS Service</td>
<td>CCM only. S-Tagged Multicast Frames</td>
<td>Ethernet CCM only. Follows the Multicast tree. Unicast addresses may be configured for peer operation.</td>
</tr>
</tbody>
</table>

In summary SPB offers an automated control plane and optional Eth-CFM/Eth-EFM to allow monitoring of Ethernet Services using SPB. B-VPLS services PBB Epipes and I-VPLS services support the existing set of Ethernet capabilities.

### SPB Levels

Levels are part of IS-IS. SPB supports Level 1 within a control B-VPLS. Future enhancements may make use of levels.
SPBM to Non-SPBM Interworking

By using static definitions of B-MACs and ISIDs interworking of PBB Epipes and I-VPLS between SPBM networks and non SPBM PBB networks can be achieved.

Static MACs and Static ISIDs

To extend SPBM networks to other PBB networks, static MACs and ISIDs can be defined under SPBM SAPs/SDPs. The declaration of a static MAC in an SPBM context allows a non-SPBM PBB system to receive frames from an SPBM system. These static MACs are conditional on the SAP/SDP operational state. (Currently this is only supported for SPBM since SPBM can advertise these BMACs and ISIDs without any requirement for flushing.) The BMAC (and BMAC to ISID) must remain consistent when advertised in the IS-IS database.

The declaration of static-isids allows an efficient connection of ISID based services. The ISID is advertised as supported on the local nodal BMAC and the static BMACs which are the true destinations for the ISIDs are also advertised. When the I-VPLS learn the remote BMAC they will associated the ISID with the true destination BMAC. Therefore if redundancy is used the BMACs and ISIDs that are advertised must be the same on any redundant interfaces.

If the interface is an MC-LAG interface the static MAC and ISIDs on the SAPs/SDPs using that interface are only active when the associated MC-LAG interface is active. If the interface is a spoke SDP on an active/standby pseudo wire (PW) the ISIDs and BMACs are only active when the PW is active.

Epipe Static Configuration

For Epipe only, the BMACs need to be advertised. There is no multicast for PBB epipes. Unicast traffic will follow the unicast path shortest path or single tree. By configuring remote BMACs Epipes can be setup to non SPBM systems. A special conditional static-mac is used for SPBM PBB B-VPLS SAPs/SDPs that are connected to a remote system. In the diagram ISID 500 is used for the PBB Epipe but only conditional MACs A and B are configured on the MC-LAG ports. The B-VPLS will advertise the static MAC either always or optionally based on a condition of the port forwarding.
I-VPLS Static Config

I-VPLS static config consists of two components: static-mac and static ISIDs that represent a remote BMAC-ISID combination.

The static-MACs are configured as with Epipe, the special conditional static-mac is used for SPBM PBB B-VPLS SAPs/SDPs that are connected to a remote system. The B-VPLS will advertise the static MAC either always or optionally based on a condition of the port forwarding.

The static-isids are created under the B-VPLS SAP/SDPs that are connected to a non-SPBM system. These ISIDs are typically advertised but may be controlled by ISID policy.

For I-VPLS ISIDs the ISIDs are advertised and multicast MAC are automatically created using PBB-OUI and the ISID. SPBM supports the pruned multicast single tree. Unicast traffic will follow the unicast path shortest path or single tree. Multicast/and unknown Unicast follow the pruned single tree for that ISID.
SPBM ISID Policies

Note that ISID policies are an optional aspect of SPBM which allow additional control of ISIDs for I-VPLS. PBB services using SPBM automatically populate multicast for I-VPLS and static-isids. Improper use of isid-policy can create black holes or additional flooding of multicast.

To enable more flexible multicast, ISID policies control the amount of MFIB space used by ISIDs by trading off the default Multicast tree and the per ISID multicast tree. Occasionally customers want services that use I-VPLS that have multiple sites but use primarily unicast. The ISID policy can be used on any node where an I-VPLS is defined or static ISIDs are defined.

The typical use is to suppress the installation of the ISID in the MFIB using use-def-mcast and the distribution of the ISID in SPBM by using no advertise-local.

The use-def-mcast policy instructs SPBM to use the default B-VPLS multicast forwarding for the ISID range. The ISID multicast frame remains unchanged by the policy (the standard format with the PBB OUI and the ISID as the multicast destination address) but no MFIB entry is allocated. This causes the forwarding to use the default BVID multicast tree which is not pruned. When this policy is in place it only governs the forwarding locally on the current B-VPLS.

The advertise local policy ISID policies are applied to both static ISIDs and I-VPLS ISIDs. The policies define whether the ISIDs are advertised in SPBM and whether the use
the local MFIB. When ISIDs are advertised they will use the MFIB in the remote nodes. Locally the use of the MFIB is controlled by the use-def-mcast policy.

The types of interfaces are summarized in Table 15.

Table 15: SPBM ISID Policies Table

<table>
<thead>
<tr>
<th>Service Type</th>
<th>ISID Policy on B-VPLS</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Epipe</td>
<td>No effect</td>
<td>PBB Epipe ISIDs are not advertised or in MFIB</td>
</tr>
<tr>
<td>I-VPLS</td>
<td>None:</td>
<td>I-VPLS uses dedicated (pruned) multicast tree. ISIDs are advertised.</td>
</tr>
<tr>
<td></td>
<td>Uses ISID Multicast tree.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Advertised ISIDs of I-VPLS.</td>
<td></td>
</tr>
<tr>
<td>I-VPLS (for Unicast)</td>
<td>use-def-mcast</td>
<td>I-VPLS uses default Multicast. Policy only required where ISIDs are defined. ISIDs not advertised. MUST be consistently defined on all nodes with same ISIDs.</td>
</tr>
<tr>
<td></td>
<td>no advertise-local</td>
<td></td>
</tr>
<tr>
<td>I-VPLS (for Unicast)</td>
<td>use-def-mcast</td>
<td>I-VPLS uses default Multicast. Policy only required where ISIDs are defined. ISIDs advertised and pruned tree used elsewhere. May be inconsistent for an ISID.</td>
</tr>
<tr>
<td></td>
<td>advertise-local</td>
<td></td>
</tr>
<tr>
<td>Static ISIDs for I-VPLS interworking</td>
<td>None: (recommended)</td>
<td>I-VPLS uses dedicated (pruned) multicast tree. ISIDs are advertised.</td>
</tr>
<tr>
<td></td>
<td>Uses ISID Multicast tree</td>
<td></td>
</tr>
<tr>
<td>Static ISIDs for I-VPLS interworking (defined locally)</td>
<td>use-def-mcast</td>
<td>I-VPLS uses default Multicast. Policy only required where ISIDs are configured or where I-VPLS is located.</td>
</tr>
<tr>
<td>No MFIB for any ISIDs. Policy defined on all nodes.</td>
<td>use-def-mcast</td>
<td>Each B-VPLS with the policy will not install MFIB. Policy defined on all switches ISIDs are defined. ISIDs advertised and pruned tree used elsewhere. May be inconsistent for an ISID.</td>
</tr>
<tr>
<td></td>
<td>no advertise-local</td>
<td></td>
</tr>
</tbody>
</table>
ISID Policy Control

Static ISID Advertisement

Static ISIDs are advertised between using the SPBM Service Identifier and Unicast Address sub-TLV in IS-IS when there is no ISID policy. This TLV advertises the local B-MAC and one or more ISIDs. The BMAC used is the source-bmac of the Control/User VPLS. Typically remote BMACs (the ultimate source-bmac) and the associated ISIDs are configured as static under the SPBM interface. This allows all remote BMACs and all remote ISIDs can be configured once per interface.

I-VPLS for Unicast Service

If the service is using unicast only an I-VPLS still uses MFIB space and SPBM advertises the ISID. By using the default multicast tree locally, a node saves MFIB space. By using the no advertise-local SPBM will not advertise the ISIDs covered by the policy. Note the actual PBB multicast frames are the same regardless of policy. Unicast traffic is the not changed for the ISID policies.

The Static BMAC configuration is allowed under Multi-Chassis LAG (MC-LAG) based SAPs and active/standby PW SDPs.

Unicast traffic will follow the unicast path shortest path or single tree. By using the ISID policy Multicast/and unknown Unicast traffic (BUM) follows the default B-VPLS tree in the SPBM domain. This should be used sparingly for any high volume of multicast services.
Default Behaviors

When static ISIDs are defined the default is to advertise the static ISIDs when the interface parent (SAP or SDP) is up.

If the advertisement is not desired, an ISID policy can be created to prevent advertising the ISID.

- **use-def-mcast**: If a policy is defined with use-def-mcast the local MFIB will not contain an Multicast MAC based on the PBB OUI+ ISID and the frame will be flooded out the local tree. This applies to any node where the policy is defined. On other nodes if the ISID is advertised the ISID will use the MFIB for that ISID.

- **No advertise-local**: If a policy of no advertise-local is defined the ISIDs in the policy will not be advertised. This combination should be used everywhere there is an I-VPLS with the ISID or where the Static ISID is defined to prevent black holes. If an ISID is to be moved from advertising to no advertising it is advisable to use **use-def-mcast** on all the nodes for that ISID which will allow the MFIB to not be installed and will start using the default multicast tree at each node with that policy. Then the no advertise-local option can be used.

Each Policy may be used alone or in combination.
Example Network Configuration

Figure 124: Sample Network

Figure 124 shows an example network showing four nodes with SPB B-VPLS. The SPB instance is configured on the B-VPLS 100001. B-VPLS 100001 uses FID 1 for SPB instance 1024. All BMACs and I-SIDs are learned in the context of B-VPLS 100001. B-VPLS 100001 has an i-vpls 10001 service, which also uses the I-SID 10001. B-VPLS 100001 is configured to use VID 1 on SAPs 1/2/2 and 1/2/3 and while the VID does not need to be the same as the FID the VID does however need to be the same on the other side (Dut-B and Dut-C).

A user B-VPLS service 100002 is configured and it uses B-VPLS 10001 to provide forwarding. It fate shares the control topology. In Figure 124, the control B-VPLS uses the low-path-id algorithm and the user B-VPLS uses high-path-id algorithm. Note that any B-VPLS can use any algorithm. The difference is illustrated in the path between Dut A and Dut D. The short dashed line through Dut-B is the low-path-id algorithm and the long dashed line thought Dut C is the high-path-id algorithm.
Sample Configuration for Dut-A

Dut-A:
Control B-VPLS:*A:Dut-A>config>service>vplsl# pwc

Present Working Context :

<User B-VPLS:>
*A:Dut-A>config>service>vplsl# pwc

Present Working Context :

<User B-VPLS:>
*A:Dut-A>config>service>vplsl# pwc
exit
sap 1/2/3:1.2 create
exit
no shutdown
------------------------------------------
I-VPLS:
configure service
  vpls 10001 customer 1 i-vpls create
  service-mtu 1492
  pbb
    backbone-vpls 100001
    exit
  exit
  stp
    shutdown
  exit
  sap 1/2/1:1000.1 create
  exit
  no shutdown
  exit
  vpls 10002 customer 1 i-vpls create
  service-mtu 1492
  pbb
    backbone-vpls 100002
    exit
  exit
  stp
    shutdown
  exit
  sap 1/2/1:1000.2 create
  exit
  no shutdown
  exit
  exit
Show Commands Outputs

The `show base` commands output a summary of the instance parameters under a control B-VPLS. The `show` command for a user B-VPLS indicates the control B-VPLS. Note that the base parameters except for Bridge Priority and Bridge ID must match on neighbor nodes.

*A:Dut-A# show service id 100001 spb base

<table>
<thead>
<tr>
<th>Service SPB Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin State : Up</td>
</tr>
<tr>
<td>ISIS Instance : 1024</td>
</tr>
<tr>
<td>Bridge Priority : 8</td>
</tr>
<tr>
<td>FID : 1</td>
</tr>
<tr>
<td>Fwd Tree Top Ucast : spf</td>
</tr>
<tr>
<td>Bridge Id : 80:00:00:10:00:01:00:01</td>
</tr>
<tr>
<td>Mcast Desig Bridge : 80:00:00:10:00:01:00:01</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ISIS Interfaces</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface                        Level CircID  Oper State   L1/L2 Metric</td>
</tr>
<tr>
<td>-----------------------------------------</td>
</tr>
<tr>
<td>sap:1/2:2:1:1.1                      L1    65536 Up           10/-</td>
</tr>
<tr>
<td>sap:1/2:3:1:1.1                      L1    65537 Up           10/-</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>FID ranges using ECT Algorithm</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-99 low-path-id</td>
</tr>
<tr>
<td>100-100 high-path-id</td>
</tr>
<tr>
<td>101-4095 low-path-id</td>
</tr>
</tbody>
</table>

The `show adjacency` command displays the system ID of the connected SPB B-VPLS neighbors and the associated interfaces to connect those neighbors.

*A:Dut-A# show service id 100001 spb adjacency

<table>
<thead>
<tr>
<th>ISIS Adjacency</th>
</tr>
</thead>
<tbody>
<tr>
<td>System ID Usage State Hold Interface MT Enab</td>
</tr>
<tr>
<td>-----------------------------------------</td>
</tr>
<tr>
<td>Dut-B L1 Up 19 sap:1/2/2:1:1.1 No</td>
</tr>
<tr>
<td>Dut-C L1 Up 21 sap:1/2/3:1:1.1 No</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Adjacencies : 2</th>
</tr>
</thead>
</table>

Details about the topology can be displayed with the `database` command. There is a detail option that displays the contents of the LSPs.

*A:Dut-A# show service id 100001 spb database

<table>
<thead>
<tr>
<th>ISIS Database</th>
</tr>
</thead>
<tbody>
<tr>
<td>LSP ID Sequence Checksum Lifetime Attributes</td>
</tr>
</tbody>
</table>

Displaying Level 1 database

<table>
<thead>
<tr>
<th>Dut</th>
<th>Type</th>
<th>MAC</th>
<th>Ver.</th>
<th>Metric</th>
<th>L1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dut-A.00-00</td>
<td>0xc</td>
<td>0xbaba</td>
<td>1103</td>
<td>L1</td>
<td></td>
</tr>
<tr>
<td>Dut-B.00-00</td>
<td>0x13</td>
<td>0xe780</td>
<td>1117</td>
<td>L1</td>
<td></td>
</tr>
<tr>
<td>Dut-C.00-00</td>
<td>0x13</td>
<td>0x85a</td>
<td>1117</td>
<td>L1</td>
<td></td>
</tr>
<tr>
<td>Dut-D.00-00</td>
<td>0xe</td>
<td>0x174a</td>
<td>1119</td>
<td>L1</td>
<td></td>
</tr>
</tbody>
</table>

Level (1) LSP Count : 4

The `show routes` command illustrates the next hop if for the MAC addresses both unicast and multicast. The path to 00:10:00:01:00:04 (Dut-D) illustrates the low-path-id algorithm id. For FID one the neighbor is Dut-B and for FID 100 the neighbor is Dut-C. Since Dut-A is the root of the multicast single tree the multicast forwarding is the same for Dut-A. However, unicast and multicast routes will differ on most other nodes. Also the I-SIDs exist on all of the nodes so I-SID base multicast follows the multicast tree exactly. If the I-SID had not existed on Dut-B or Dut-D then for FID 1 there would be no entry. Note only designated nodes (root nodes) show metrics. Non designated nodes will not show metrics.

*A:* Dut-A# show service id 100001 spb routes

<table>
<thead>
<tr>
<th>Fid</th>
<th>MAC</th>
<th>Ver.</th>
<th>Metric</th>
<th>NextHop If</th>
<th>SysID</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>00:10:00:01:00:02</td>
<td>10</td>
<td>10</td>
<td>sap:1/2/2:1.1</td>
<td>Dut-B</td>
</tr>
<tr>
<td>1</td>
<td>00:10:00:01:00:03</td>
<td>10</td>
<td>10</td>
<td>sap:1/2/3:1.1</td>
<td>Dut-C</td>
</tr>
<tr>
<td>1</td>
<td>00:10:00:01:00:04</td>
<td>10</td>
<td>20</td>
<td>sap:1/2/2:1.1</td>
<td>Dut-B</td>
</tr>
<tr>
<td>100</td>
<td>00:10:00:02:00:02</td>
<td>10</td>
<td>10</td>
<td>sap:1/2/2:1.1</td>
<td>Dut-B</td>
</tr>
<tr>
<td>100</td>
<td>00:10:00:02:00:03</td>
<td>10</td>
<td>10</td>
<td>sap:1/2/3:1.1</td>
<td>Dut-C</td>
</tr>
<tr>
<td>100</td>
<td>00:10:00:02:00:04</td>
<td>10</td>
<td>20</td>
<td>sap:1/2/3:1.1</td>
<td>Dut-C</td>
</tr>
</tbody>
</table>

Fwd Tree: multicast

<table>
<thead>
<tr>
<th>Fid</th>
<th>MAC</th>
<th>Ver.</th>
<th>Metric</th>
<th>NextHop If</th>
<th>SysID</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>00:10:00:01:00:02</td>
<td>10</td>
<td>10</td>
<td>sap:1/2/2:1.1</td>
<td>Dut-B</td>
</tr>
<tr>
<td>1</td>
<td>00:10:00:01:00:03</td>
<td>10</td>
<td>10</td>
<td>sap:1/2/3:1.1</td>
<td>Dut-C</td>
</tr>
<tr>
<td>1</td>
<td>00:10:00:01:00:04</td>
<td>10</td>
<td>20</td>
<td>sap:1/2/2:1.1</td>
<td>Dut-B</td>
</tr>
<tr>
<td>100</td>
<td>00:10:00:02:00:02</td>
<td>10</td>
<td>10</td>
<td>sap:1/2/2:1.1</td>
<td>Dut-B</td>
</tr>
<tr>
<td>100</td>
<td>00:10:00:02:00:03</td>
<td>10</td>
<td>10</td>
<td>sap:1/2/3:1.1</td>
<td>Dut-C</td>
</tr>
<tr>
<td>100</td>
<td>00:10:00:02:00:04</td>
<td>10</td>
<td>20</td>
<td>sap:1/2/3:1.1</td>
<td>Dut-C</td>
</tr>
</tbody>
</table>
No. of MAC Routes: 12

ISID Route Table

<table>
<thead>
<tr>
<th>Fid</th>
<th>ISID</th>
<th>Ver.</th>
<th>NextHop If</th>
<th>SysID</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>10001</td>
<td>10</td>
<td>sap:1/2/2:1.1</td>
<td>Dut-B</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>sap:1/2/3:1.1</td>
<td>Dut-C</td>
</tr>
<tr>
<td>100</td>
<td>10002</td>
<td>10</td>
<td>sap:1/2/2:1.1</td>
<td>Dut-B</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>sap:1/2/3:1.1</td>
<td>Dut-C</td>
</tr>
</tbody>
</table>

No. of ISID Routes: 2

The `show service spb fdb` command shows the programmed unicast and multicast source MACs in SPB-managed B-VPLS service.

*A:Dut-A# show service id 100001 spb fdb*

User service FDB information

<table>
<thead>
<tr>
<th>MacAddr</th>
<th>UCast Source</th>
<th>State</th>
<th>MCast Source</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:10:00:01:00:02 1/2/2:1.1</td>
<td>ok</td>
<td>1/2/2:1.1</td>
<td>ok</td>
<td></td>
</tr>
<tr>
<td>00:10:00:01:00:03 1/2/3:1.1</td>
<td>ok</td>
<td>1/2/3:1.1</td>
<td>ok</td>
<td></td>
</tr>
<tr>
<td>00:10:00:01:00:04 1/2/2:1.1</td>
<td>ok</td>
<td>1/2/2:1.1</td>
<td>ok</td>
<td></td>
</tr>
</tbody>
</table>

Entries found: 3

*A:Dut-A# show service id 100002 spb fdb*

User service FDB information

<table>
<thead>
<tr>
<th>MacAddr</th>
<th>UCast Source</th>
<th>State</th>
<th>MCast Source</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:10:00:02:00:02 1/2/2:1.2</td>
<td>ok</td>
<td>1/2/2:1.2</td>
<td>ok</td>
<td></td>
</tr>
<tr>
<td>00:10:00:02:00:03 1/2/3:1.2</td>
<td>ok</td>
<td>1/2/3:1.2</td>
<td>ok</td>
<td></td>
</tr>
<tr>
<td>00:10:00:02:00:04 1/2/2:1.2</td>
<td>ok</td>
<td>1/2/2:1.2</td>
<td>ok</td>
<td></td>
</tr>
</tbody>
</table>

Entries found: 3

The `show service spb mfib` command shows the programmed multicast ISID addresses Macs in SPB-managed B-VPLS service shows the multicast ISID pbb group mac addresses in SPB-managed B-VPLS. Note that other types of *,G multicast traffic is sent over the multicast tree and these MACs are not shown. OAM traffic that uses multicast (for example vMEP CCM) will take this path for example.

*A:Dut-A# show service id 100001 spb mfib*
User service MFIB information

<table>
<thead>
<tr>
<th>MacAddr</th>
<th>ISID</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>01:1E:83:00:27:11</td>
<td>10001</td>
<td>Ok</td>
</tr>
</tbody>
</table>

Entries found: 1

*A:Dut-A# show service id 100002 spb mfib

User service MFIB information

<table>
<thead>
<tr>
<th>MacAddr</th>
<th>ISID</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>01:1E:83:00:27:12</td>
<td>10002</td>
<td>Ok</td>
</tr>
</tbody>
</table>

Entries found: 1
Debug Commands

• debug service id <svcId> spb
• debug service id <svcId> spb adjacency
• debug service id <svcId> spb interface
• debug service id <svcId> spb l2db
• debug service id <svcId> spb lsdb
• debug service id <svcId> spb packet <detail>
• debug service id <svcId> spb spf

Tools Commands

• tools perform service id <svcId> spb run-manual-spf
• tools dump service id spb
• tools dump service id spb default-multicast-list
• tools dump service id spb forwardingpath

Clear Commands

• clear service id <svcId> spb
• clear service id <svcId> spb adjacency
• clear service id <svcId> spb database
• clear service id <svcId> spb spf-log
• clear service id <svcId> spb statistics
IEEE 802.1ak MMRP for Service Aggregation and Zero Touch Provisioning

IEEE 802.1ah supports an M:1 model where multiple customer services, represented by ISIDs, are transported through a common infrastructure (B-component). Alcatel-Lucent’s PBB implementation supports the M:1 model allowing for a service architecture where multiple customer services (I-VPLS or Epipe) can be transported through a common B-VPLS infrastructure as depicted in Figure 125.

The B-VPLS infrastructure represented by the white circles is used to transport multiple customer services represented by the triangles of different colors. This service architecture minimizes the number of provisioning touches and reduces the load in the core PEs: for example, G and H use less VPLS instances and pseudowire.

In a real life deployment, different customer VPNs do not share the same community of interest – for example, VPN instances may be located on different PBB PEs. The M:1 model depicted in Figure 126 requires a per VPN flood containment mechanism so that VPN traffic is distributed just to the B-VPLS locations that have customer VPN sites: for example, flooded traffic originated in the blue I-VPLS should be distributed just to the PBB PEs where blue I-VPLS instances are present – PBB PE B, E and F.
Per customer VPN distribution trees need to be created dynamically throughout the BVPLS as new customer I-VPLS instances are added in the PBB PEs.

Alcatel-Lucent’s PBB implementation employs the IEEE 802.1ak Multiple MAC Registration Protocol (MMRP) to dynamically build per I-VPLS distribution trees inside a certain B-VPLS infrastructure.

IEEE 802.1ak Multiple Registration Protocol (MRP) – Specifies changes to IEEE Std 802.1Q that provide a replacement for the GARP, GMRP and GVRP protocols. MMRP application of IEEE 802.1ak specifies the procedures that allow the registration/de-registration of MAC addresses over an Ethernet switched infrastructure.

In the PBB case, as I-VPLS instances are enabled in a certain PE, a group BMAC address is by default instantiated using the standard based PBB Group OUI and the ISID value associated with the I-VPLS.

When a new I-VPLS instance is configured in a PE, the IEEE 802.1ak MMRP application is automatically invoked to advertise the presence of the related group B-MAC on all active B-VPLS SAPs and SDP bindings.

When at least two I-VPLS instances with the same ISID value are present in a B-VPLS, an optimal distribution tree is built by MMRP in the related B-VPLS infrastructure as depicted in Figure 126.

![Figure 126: Flood Containment Requirement in M:1 Model](image-url)
MMRP Support Over B-VPLS SAPs and SDPs

MMRP is supported in B-VPLS instances over all the supported BVPLS SAPs and SDPs, including the primary and standby pseudowire scheme implemented for VPLS resiliency.

When a B-VPLS with MMRP enabled receives a packet destined to a specific group BMAC, it checks its own MFIB entries and if the group BMAC does not exist, it floods it everywhere. This should never happen as this kind of packet will be generated at the I-VPLS/PBB PE when a registration was received for a local I-VPLS group BMAC.

I-VPLS Changes and Related MMRP Behavior

This section describes the MMRP behavior for different changes in IVPLS.

1. When an ISID is set for a certain I-VPLS and a link to a related B-VPLS is activated (for example, through the `config>service>vpls>backbone-vpls vpls id:isid` command), the group BMAC address is declared on all B-VPLS virtual ports (SAPs or SDPs).
2. When the ISID is changed from one value to a new one, the old group BMAC address is undeclared on all ports and the new group BMAC address is declared on all ports in the B-VPLS.
3. When the I-VPLS is disassociated with the B-VPLS, the old group BMAC is no longer advertised as a local attribute in the B-VPLS if no other peer B-VPLS PEs have it declared.
4. When an I-VPLS goes operationally down (either all SAPs/SDPs are down) or the I-VPLS is shutdown, the associated group BMAC is undeclared on all ports in the B-VPLS.
5. When the I-VPLS is deleted, the group BMAC should already be un-declared on all ports in the B-VPLS because the I-VPLS has to be shutdown in order to delete it.

Limiting the Number of MMRP Entries on a Per B-VPLS Basis

The MMRP exchanges create one entry per attribute (group BMAC) in the B-VPLS where MMRP protocol is running. When the first registration is received for an attribute, an MFIB entry is created for it.

Alcatel-Lucent’s implementation allows the user to control the number of MMRP attributes (group BMACs) created on a per B-VPLS basis. Control over the number of related MFIB entries in the B-VPLS FIB is inherited from previous releases through the use of the `config>service>vpls>mfib-table-size table-size` command. This ensures that no B-VPLS will take up all the resources from the total pool.
Optimization for Improved Convergence Time

Assuming that MMRP is used in a certain B-VPLS, under failure conditions the time it takes for the B-VPLS forwarding to resume may depend on the data plane and control plane convergence plus the time it takes for MMRP exchanges to settle down the flooding trees on a per ISID basis.

In order to minimize the convergence time, Alcatel-Lucent’s PBB implementation offers the selection of a mode where B-VPLS forwarding reverts for a short time to flooding so that MMRP has enough time to converge. This mode can be selected through configuration using the `configure>service>vpl> bvpls>mrp>flood-time value` command where `value` represents the amount of time in seconds that flooding will be enabled. Refer to the PBB Command Reference on page 1025 for command syntax and usage.

If this behavior is selected, the forwarding plane reverts to B-VPLS flooding for a configurable time period, for example, for a few seconds, then it reverts back to the MFIB entries installed by MMRP.

The following B-VPLS events initiate the switch from per I-VPLS (MMRP) MFIB entries to “B-VPLS flooding”:

- Reception or local triggering of a TCN
- B-SAP failure
- Failure of a B-SDP binding
- Pseudowire activation in a primary/standby HVPLS resiliency solution
- SF/CPM switchover due to STP reconvergence

Controlling MRP Scope using MRP Policies

MMRP advertises the Group BMACs associated with ISIDs throughout the whole BVPLS context regardless of whether a specific IVPLS is present in one or all the related PEs or BEBs. When evaluating the overall scalability the resource consumption in both the control and data plane must be considered:

- Control plane - MMRP processing and number of attributes advertised
- Data plane – one tree is instantiated per ISID or Group BMAC attribute

In a multi-domain environment, for example multiple MANs interconnected through a WAN, the BVPLS and implicitly MMRP advertisement may span across domains. The MMRP attributes will be flooded throughout the BVPLS context indiscriminately, regardless of the distribution of IVPLS sites.
The solution described in this section limits the scope of MMRP control plane advertisements to a specific network domain using MRP Policy. ISID-based filters are also provided as a safety measure for BVPLS data plane.

Figure 127: Inter-Domain Topology

Figure 127 depicts the case of an Inter-domain deployment where multiple metro domains (MANs) are interconnected through a wide area network (WAN). A BVPLS is configured across these domains running PBB M:1 model to provide infrastructure for multiple IVPLS services. MMRP is enabled in the BVPLS to build per IVPLS flooding trees. In order to limit the load in the core PEs or PBB BCBs, the local IVPLS instances must use MMRP and data plane resources only in the MAN regions where they have sites. A solution to the above requirements is depicted in Figure 128. The case of native PBB metro domains inter-connected via a MPLS core is used in this example. Other technology combinations are possible.

Figure 128: Limiting the Scope of MMRP Advertisements
An MRP policy can be applied to the edge of MAN1 domain to restrict the MMRP advertisements for local ISIDs outside local domain. Or the MRP policy can specify the inter-domain ISIDs allowed to be advertised outside MAN1. The configuration of MRP policy is similar with the configuration of a filter. It can be specified as a template or exclusively for a specific endpoint under service mrp object. An ISID or a range of ISID(s) can be used to specify one or multiple match criteria that will be used to generate the list of Group MACs to be used as filters to control which MMRP attributes can be advertised. An example of a simple mrp-policy that allows the advertisement of Group BMACs associated with ISID range 100-150 is given below:

```
*A:ALA-7>config>service>mrp# info
----------------------------------------------
mrp-policy "test" create
   default-action block
   entry 1 create
      match
         isid 100 to 150
      exit
      action allow
      exit
   exit
----------------------------------------------
```

A special action end-station is available under mrp-policy entry object to allow the emulation on a specific SAP/PW of an MMRP end-station. This is usually required when the operator does not want to activate MRP in the WAN domain for interoperability reasons or if it prefers to manually specify which ISID will be interconnected over the WAN. In this case the MRP transmission will be shutdown on that SAP/PW and the configured ISIDs will be used the same way as an IVPLS connection into the BVPLS, emulating a static entry in the related BVPLS MFIB. Also if MRP is active in the BVPLS context, MMRP will declare the related GBMAC(s) continuously over all the other BVPLS SAP/PW(s) until the mrp-policy end-station action is removed from the mrp-policy assigned to that BVPLS context.

The MMRP usage of the mrp-policy will ensure automatically that traffic using Group BMAC will not be flooded between domains. There could be though small transitory periods when traffic originated from PBB BEB with unicast BMAC destination may be flooded in the BVPLS context as unknown unicast in the BVPLS context for both IVPLS and PBB Epipe. To restrict distribution of this traffic for local PBB services a new ISID match criteria is added to existing mac-filters. The mac-filter configured with ISID match criterium can be applied to the same interconnect endpoint(s), BVPLS SAP or PW, as the mrp-policy to restrict the egress transmission any type of frames that contain a local ISID. An example of this new configuration option is described below:

```
A:ALA-7>config>filter# info
----------------------------------------------
mac-filter 90 create
description "filter-wan-man"
type isid
scope template
eentry 1 create
   description "drop-local-isid"
      match
```

Page 976  7950 SR  OS Services Guide
isid from 100 to 1000
exit
action drop
exit

These filters will be applied as required on a per B-SAP or B-PW basis just in the egress direction. The ISID match criteria is exclusive with any other criteria under mac-filter. A new mac-filter type attribute is defined to control the use of ISID match criteria and must be set to isid to allow the use of isid match criteria. The ISID tag is identified using the PBB ethertype provisioned under config>port>ethernet>pbb-etype.
PBB and BGP-AD

BGP auto-discovery is supported only in the BVPLS to automatically instantiate the BVPLS pseudowires and SDPs as described in BGP Auto-Discovery for LDP VPLS on page 607.

PBB ELINE Service

ELINE service is defined in PBB (IEEE 802.1ah) as a point-to-point service over the B-component infrastructure. Alcatel-Lucent’s implementation offers support for PBB ELINE through the mapping of multiple Epipe services to a Backbone VPLS infrastructure.

The use of Epipe scales the ELINE services as no MAC switching, learning or replication is required in order to deliver the point-to-point service.

All packets ingressing the customer SAP/spoke-SDP are PBB encapsulated and unicasted through the B-VPLS “tunnel” using the backbone destination MAC of the remote PBB PE.

All the packets ingressing the B-VPLS destined for the Epipe are PBB de-encapsulated and forwarded to the customer SAP/spoke-SDP.

A PBB ELINE service support the configuration of a SAP or non-redundant spoke-SDP.

Non-Redundant PBB Epipe Spoke Termination

This feature provides the capability to use non-redundant pseudowire connections on the access side of a PBB Epipe, where previously only SAPs could be configured.
Support Service and Solution Combinations

The following considerations apply when Ethernet tunnels are configured under a VPLS service:

- Only ports in access or hybrid mode can be configured as eth-tunnel path members. The member ports can be located on the same or different IXCMs or XMAs.
- Dot1q and QinQ ports are supported as eth-tunnel path members.
- The same port cannot be used as member in both a LAG and an Ethernet-tunnel.
- A mix of regular and multiple eth-tunnel SAPs and PWs can be configured in the same BVPLS.
- Split horizon groups in BVPLS are supported on eth-tunnel SAPs. The use of split horizon groups allows the emulation of a VPLS model over the native Ethernet core, eliminating the need for P-MSTP.
- STP and MMRP are not supported in a BVPLS using eth-tunnel SAPs.
- Both PBB ELINE (Epipe) and ELAN (IVPLS) services can be transported over a BVPLS using Ethernet-tunnel SAPs.
- MC-LAG access multi-homing into PBB services is supported in combination with Ethernet tunnels:
  - MC-LAG SAPs can be configured in IVPLS or Epipe instances mapped to a BVPLS that uses eth-tunnel SAPs
  - Blackhole Avoidance using native PBB MAC flush/MAC move solution is also supported
- Support is also provided for BVPLS with P-MSTP and MMRP control plane running as ships-in-the-night on the same links with the Ethernet tunneling which is mapped by a SAP to a different BVPLS.
  - Epipes must be used in the BCBs to support scalable point-to-point tunneling between the eth-tunnel endpoints when management VPLS is used.
Periodic MAC Notification

Virtual BMAC learning frames (for example, the frames sent with the source MAC set to the virtual BMAC) can be sent periodically, allowing all BCBs/BEBs to keep the virtual BMAC in their Layer 2 forwarding database.

This periodic mechanism is useful in the following cases:

- A new BEB is added after the current mac-notification method has stopped sending learning frames.
- When a new combination of [MC-LAG:SAP|A/S PW]+[PBB-Epipe]+[associated B-VPLS]+[at least one B-SDP|B-SAP] becomes active. Note that the current mechanism only sends learning frames when the first such combination becomes active.
- A BEB containing the remote endpoint of a dual-homed PBB-epipe is rebooted.
- When traffic is not seen for the MAC ageing timeout (assuming that the new periodic sending interval is less than the ageing timeout).
- When there is uni-directional traffic.

In each of the above cases, all of the remote BEB/BCBs will learn the virtual MAC in the worse case after the next learning frame is sent.

In addition, this will allow all of the above when to be used in conjunction with discard-unknown in the B-VPLS. Currently, if discard-unknown is enabled in all related B-VPLSes (to avoid any traffic flooding), all above cases could experience an increased traffic interruption, or a permanent loss of traffic, as only traffic towards the dual homed PBB-epipe can restart bi-directional communication. For example, it will reduce the traffic outage when:

The PBB-Epipe virtual MAC is flushed on a remote BEB/BCB due to the failover of an MC-LAG or A/S pseudowires within the customer’s access network, for example, in between the dual homed PBB-Epipe peers and their remote tunnel endpoint.

There is a failure in the PBB core causing the path between the two BEBs to pass through a different BCB.

It should be noted that this will not help in the case where the remote tunnel endpoint BEB fails. In this case traffic will be flooded when the remote BMAC ages out if discard-unknown is disabled. If discard-unknown is enabled, then the traffic will follow the path to the failed BEB but will eventually be dropped on the source BEB when the remote BMAC ages out on all systems.

In order to scale the implementation it is expected that the timescale for sending the periodic notification messages is much longer than that used for the current notification messages.
MAC Flush

PBB Resiliency for B-VPLS Over Pseudowire Infrastructure

The following VPLS resiliency mechanisms are also supported in PBB VPLS:

- Native Ethernet resiliency supported in both I-VPLS and B-VPLS contexts
- Distributed LAG, MC-LAG, RSTP
- MSTP in a management VPLS monitoring (B- or I-) SAPs and pseudowire
- BVPLS service resiliency, loop avoidance solutions – Mesh, active/standby pseudowires and multi-chassis endpoint
- IVPLS service resiliency, loop avoidance solutions – Mesh, active/standby pseudowires (PE-rs only role), BGP Multi-homing

To support these resiliency options, extensive support for blackhole avoidance mechanisms is required.

Porting existing VPLS LDP MAC Flush in PBB VPLS

Both the I-VPLS and B-VPLS components inherit the LDP MAC flush capabilities of a regular VPLS to fast age the related FIB entries for each domain: CMACs for I-VPLS and BMACs for B-VPLS. Both types of LDP MAC flush are supported for I-VPLS and B-VPLS domains:

- **flush-all-but-mine** - flush on positive event, for example:
  - Pseudowire activation — VPLS resiliency using active/standby pseudowire
  - Reception of a STP TCN
- **flush-all-from-me** - flush on negative event, for example:
  - SAP failure – link down or MC-LAG out-of-sync
  - Pseudowire or Endpoint failure

In addition, only for the B-VPLS domain, changing the backbone source MAC of a B-VPLS will trigger a LDP MAC flush-all-from-me to be sent in the related active topology. At the receiving PBB PE, a BMAC flush automatically triggers a flushing of the CMACs associated with the old source BMAC of the B-VPLS.
PBB Blackholing Issue

In the PBB VPLS solution, a B-VPLS may be used as infrastructure for one or more I-VPLS instances. B-VPLS control plane (LDP Signaling or P-MSTP) replaces I-VPLS control plane throughout the core. This is raising an additional challenge related to blackhole avoidance in the I-VPLS domain as described in this section.

**PBB Blackholing Issue** — Assuming that the link between PE A1 and node 5 is active, the remote PEs participating in the orange VPN (for example, PE D) will learn the CMAC X associated with backbone MAC A1. Under failure of the link between node 5 and PE A1 and activation of link to PE A2, the remote PEs (for example, PE D) will black-hole the traffic destined for customer MAC X to BMAC A1 until the aging timer expires or a packet flows from X to Y through the PE A2. This may take a long time (default aging timer is 5 minutes) and may affect a large number of flows across multiple I-VPLSes.

A similar issue will occur in the case where node 5 is connected to A1 and A2 I-VPLS using active/standby pseudowires. For example, when node 5 changes the active pseudowire, the remote PBB PE will keep sending to the old PBB PE.

Another case is when the QinQ access network dual-homed to a PBB PE uses RSTP or MVPLS with MSTP to provide loop avoidance at the interconnection between the PBB PEs and the QinQ SWs. In the case where the access topology changes, a TCN event will be generated and propagated throughout the access network. Similarly, this change needs to be propagated to the remote PBB PEs to avoid blackholing.

A solution is required to propagate the I-VPLS events through the backbone infrastructure (B-VPLS) in order to flush the customer MAC to BMAC entries in the remote PBB. As there are no IVPLS control plane exchanges across the PBB backbone, extensions to B-VPLS control plane are required to propagate the I-VPLS MAC flush events across the B-VPLS.

---

**LDP MAC Flush Solution for PBB Blackholing**

In the case of an MPLS core, B-VPLS uses T-LDP signaling to set up the pseudowire forwarding. The following I-VPLS events must be propagated across the core B-VPLS using LDP MAC flush-all-but-mine or flush-all-from-me indications:

For flush-all-but-mine indication (“positive flush”):

- TCN event in one or more of the I-VPLS or in the related M-VPLS for the MSTP use case.
- Pseudowire/SDP binding activation with Active/Standby pseudowire (standby, active or down, up)
- Reception of an LDP MAC withdraw “flush-all-but-mine” in the related I-VPLS
For **flush-all-from-me** indication (“negative flush”)

- MC-LAG failure - does not require send-flush-on-failure to be enabled in I-VPLS
- Failure of a local SAP – requires send-flush-on-failure to be enabled in I-VPLS
- Failure of a local pseudowires/SDP binding – requires send-flush-on-failure to be enabled in I-VPLS
- Reception of an LDP MAC withdraw flush-all-from-me in the related I-VPLS

In order to propagate the MAC flush indications triggered by the above events, the PE that originates the LDP MAC withdraw message must be identified. In regular VPLS “mine”/“me” is represented by the pseudowire associated with the FEC and the T-LDP session on which the LDP MAC withdraw was received. In PBB, this is achieved using the B-VPLS over which the signaling was propagated and the BMAC address of the originator PE.

Alcatel-Lucent PBB-VPLS solution addresses this requirement by inserting in the BVPLS LDP MAC withdraw message a new PBB-TLV (type-length-value) element. The new PBB TLV contains the source BMAC identifying the originator (“mine”/“me”) of the flush indication and the ISID list identifying the I-VPLS instances affected by the flush indication.

There are a number of advantages to this approach. Firstly, the PBB-TLV presence indicates this is a PBB MAC Flush. As a result, all PEs containing only the B-VPLS instance will automatically propagate the LDP MAC withdraw in the B-VPLS context respecting the split-horizon and active link topology. There is no flushing of the B-VPLS FIBs throughout the core PEs. Subsequently, the receiving PBB VPLS PEs uses the BMAC and ISID list information to identify the specific I-VPLS FIBs and the CMAC entries pointing to the source BMAC included in the PBB TLV.

An example of processing steps involved in PBB MAC Flush is depicted in Figure 129 for the case when a Topology Change Notification (TCN) is received on PBB PE 2 from a QinQ access in the I-VPLS domain.
The received TCN may be related to one or more I-VPLS domains. This will generate a MAC Flush in the local I-VPLS instance(s) and if configured, it will originate a PBB MAC `flush-all-but-mine` throughout the related B-VPLS context(s) represented by the white circles 1-8 in our example.

A PBB-TLV is added by PE2 to the regular LDP MAC `flush-all-but-mine`. BMAC2, the source BMAC associated with B-VPLS on PE2 is carried inside the PBB TLV to indicate who “mine” is. The ISID list identifying the I-VPLS affected by the TCN is also included if the number of affected I-VPLS is 100 or less. No ISID list is included in the PBB-TLV if more than 100 ISIDs are affected. If no ISID list is included, then the receiving PBB PE will flush all the local I-VPLS instances associated with the B-VPLS context identified by the FEC TLV in the LDP MAC withdraw message. This is done to speed up delivery and processing of the message.

Recognizing the PBB MAC flush, the B-VPLS only PEs 3, 4, 5 and 6 refrain from flushing their B-VPLS FIB tables and propagate the MAC flush message regardless of their “propagate-mac-flush” setting.

When LDP MAC withdraw reaches the terminating PBB PEs 1 and 7, the PBB-TLV information is used to flush from the I-VPLS FIBs all CMAC entries except those associated with the originating BMAC BM2. If specific I-VPLS ISIDs are indicated in the PBB TLV, then the PBB PEs will flush only the CMAC entries from the specified I-VPLS except those mapped to the
originating BMAC. Flush-all-but-mine indication is not propagated further in the I-VPLS context to avoid information loops.

The other events that trigger Flush-all-but-mine propagation in the B-VPLS (pseudowire/SDP binding activation, Reception of an LDP MAC Withdraw) are handled similarly. The generation of PBB MAC flush-all-but-mine in the B-VPLS must be activated explicitly on a per I-VPLS basis with the command `send-bvpls-flush all-but-mine`. The generation of PBB MAC flush-all-from-me in the B-VPLS must be activated explicitly on a per I-VPLS basis with the command `send-bvpls-flush all-from-me`.
Access Multi-Homing for Native PBB (B-VPLS over SAP Infrastructure)

Alcatel-Lucent PBB implementation allows the operator to use a native Ethernet infrastructure as the PBB core. Native Ethernet tunneling can be emulated using Ethernet SAPs to interconnect the related B-VPLS instances. This kind of solution might fit certain operational environments where Ethernet services was provided in the past using QinQ solution. The drawback is that no LDP signaling is available to provide support for Access Multi-homing for Epipe (pseudowire Active/Standby status) or I-VPLS services (LDP MAC Withdraw). An alternate solution is required.

A PBB network using Native Ethernet core is depicted in Figure 130. MC-LAG is used to multi-home a number of edge switches running QinQ to PBB BEBs.

![Figure 130: Access Dual-Homing into PBB BEBs - Topology View](Figure 130)

The interrupted line from the MC-LAG represents the standby, inactive link; the solid line is the active link. The BEBs are dual-homed to two core switches BCB1 and BCB2 using native Ethernet SAPs on the B-VPLS side. Multi-point B-VPLS with MSTP for loop avoidance can be used as the PBB core tunneling. Alternatively point-to-point, G.8031 protected Ethernet tunnels can be also used to interconnect B-VPLS instances in the BEBs as described in the PBB over G.8031 protected Ethernet tunnels.
Alcatel-Lucent implementation provides a solution for both PBB ELINE (Epipe) and ELAN (IVPLS) services that avoids PBB blackholing when the active ES11-BEB1 link fails. It also provides a consistent behavior for both service type and for different backbone types: for example, native Ethernet, MPLS, or a combination. Only MC-LAG is supported initially as the Access-Multi-homing mechanism.

Solution Description for I-VPLS Over Native PBB Core

The use case described in the previous section is addressed by enhancing the existing native PBB solution to provide for blackhole avoidance.

The topology depicted in Figure 131 describes the details of the solution for the I-VPLS use case. Although the native PBB use case is used, the solution works the same for any other PBB infrastructure: for example, G.8031 Ethernet tunnels, pseudowire/MPLS, or a combination.
ES1 and ES2 are dual-homed using MC-LAG into two BEB devices: ES1 to BEB C and BEB D, ES2 to BEB A and BEB B. MC-LAG P11 on BEB C and P9 on BEB A are active on each side.

In the service context, the triangles are I-VPLS instances while the small circles are B-VPLS components with the related, per BVPLS source BMACs indicated next to each BVPLS instances. P-MSTP or RSTP may be used for loop avoidance in the multi-point BVPLS. For simplicity, only the active SAPs (BEB P2, P4, P6 and P8) are shown in the diagram.

In addition to the source BMAC associated with each BVPLS, there is an additional BMAC associated with each MC-LAG supporting multi-homed I-VPLS SAPs. The BEBs that are in a multi-homed MC-LAG configuration share a common B-MAC on the related MC-LAG interfaces. For example, a common BMAC C1 is associated in this example with ports P11 and P12 participating in the MC-LAG between BEB C and BEB D while BMAC A1 is associated with ports P9 and P10 in the MC-LAG between BEB A and BEB B. While BMAC C1 is associated through the I-VPLS SAPs with both BVPLS instances in BEB C and BEB D, it is actively used for forwarding to I-VPLS SAPs only on BEB C containing the active link P11.

MC-LAG protocol keeps track of which side (port or LAG) is active and which is standby for a given MC-LAG grouping and activates the standby in case the active one fails. The source BMAC C1 and A1 are used for PBB encapsulation as traffic arrives at the IVPLS SAPs on P11 and P9 respectively. MAC Learning in the BVPLS instances installs MAC FIB entries in BCB-E and BEB A as depicted in Figure 131.

Active link (P11) or access node (BEB C) failures are activating through MC-LAG protocol the standby link (P12) participating in the MC-LAG on the pair MC-LAG device (BEB D).

Figure 132 depicts the case of access link failure.
On failure of the active link P11 on BEB C the following processing steps apply:

- MC-LAG protocol activates the standby link P12 on the pair BEB D.
- BMAC C1 becomes active on BEB D and any traffic received on BEB D with destination BMAC C1 is forwarded on the corresponding I-VPLS SAPs on P12.
- BEB D determines the related B-VPLS instance(s) associated with all the I-VPLS SAP(s) mapped to P12, the newly activated MC-LAG link(s)/LAG component(s).
- Subsequently, BEB D floods in the related B-VPLS instance(s) an Ethernet CFM-like message using C1 as source BMAC. A vendor CFM opcode is used followed by an Alcatel-Lucent OUI.
- As a result, all the FIB entries in BCBs or BEBs along the path will be automatically updated to reflect the move of BMAC C1 to BEB D.
- Note that in this particular configuration the entries on BEB A do not need to be updated saving MAC Flush operation.
• In other topologies, it is possible that the BMAC C1 FIB entries in the B-VPLS instance on the remote BEBs (like BEB A) will need to move between B-SAPs. This will involve a move of all CMAC using as next hop BMAC C1 and the new egress linecard.

Identical procedure is used when the whole BEB C fails.
Solution Description for PBB Epipe over G.8031 Ethernet Tunnels

This section discusses the Access Multi-Homing solution for PBB ELINE over an infrastructure of G.8031 Ethernet tunnels. Although a specific use case is used, the solution works the same for any other PBB infrastructure: for example, native PBB, pseudowire/MPLS, or a combination.

The PBB ELINE service and the related BVPLS infrastructure are depicted in Figure 133.

![Figure 133: Access Multi-Homing Solution for PBB Epipe](image)

The ELINE instances are connected through the B-VPLS infrastructure. Each B-VPLS is interconnected to the BEBs in the remote pair using the G.8031, Ethernet Protection Switched (EPS) tunnels. Only the active Ethernet paths are shown in the network diagram to simplify the explanation. Split Horizon Groups may be used on EPS tunnels to avoid running MSTP/RSTP in the PBB core.

The same BMAC addressing scheme is used as in the ELAN case: a BMAC per B-VPLS and additional BMACs associated with each MC-LAG connected to an Epipe SAP. The BMACs associated with the active MC-LAG are actively used for forwarding into B-VPLS the traffic ingressing related Epipe SAPs.
MC-LAG protocol keeps track of which side is active and which is standby for a given MC-LAG grouping and activates the standby link in a failure scenario. The source BMACs C1 and A1 are used for PBB encapsulation as traffic arrives at the Epipe SAPs on P11 and P9, respectively. MAC Learning in the B-VPLS instances installs MAC FIB entries in BEB C and BEB A as depicted in Figure 133. The highlighted Ethernet tunnel (EPS) will be used to forward the traffic between BEB A and BEB C.

Active link (P11) or access node (BEB C) failures are activating through MC-LAG protocol, the standby link (P12) participating in the MC-LAG on the pair MC-LAG device (BEB D). The failure of BEB C is depicted in Figure 134. The same procedure applies for the link failure case.

The following process steps apply:

- BEB D will lose MC-LAG communication with its peer BEB C - no more keep-alives from BEB C or next-hop tracking may kick in.
- BEB D assumes BEB C is down and activates all shared MC-LAG links, including P12.
- BMAC C1 becomes active on BEB D and any traffic received on BEB C with destination BMAC C1 is forwarded on the corresponding Epipe SAPs on P12.
- BEB D determines the related B-VPLS instance(s) associated with all the Epipe SAP(s) mapped to P12, the newly activated MC-LAG link(s)/LAG component(s).
Subsequently, BEB D floods in the related B-VPLS instance(s) the same Ethernet CFM message using C1 as source BMAC.

As a result, the FIB entries in BEB A and BEB B will be automatically updated to reflect the move of BMAC C1 from EP1 to EP2 and from EP3 to EP4, respectively.

Note that the same process is executed for all the MC-LAGs affected by BEB C failure so BEB failure will be the worst case scenario.

---

### Dual-Homing into PBB Epipe - Local Switching Use Case

When the service SAPs were mapped to MC-LAGs belonging to the same pair of BEBs in earlier releases, an IVPLS had to be configured even if there were just two SAPs active at any point in time. Since then, the PBB Epipe model has been enhanced to support configuring in the same Epipe instance two SAPs and a BVPLS uplink as depicted in Figure 135.

![Figure 135: Solution for Access Dual-Homing with Local Switching for PBB Eline/Epipe](al_0161.png)

The PBB Epipe represented by the yellow diamond on BEB1 points through the BVPLS uplink to the BMAC associated with BEB2. The destination BMAC can be either the address associated with the green BVPLS on BEB2 or the BMAC of the SAP associated with the pair MC-LAG on BEB2 (preferred option).

The Epipe information model is expanded to accommodate the configuration of two SAPs (I-SAPs) and of a BVPLS uplink in the same time. For this configuration to work in an Epipe environment, only two of them will be active in the forwarding plane at any point in time, specifically:

- SAP1 and SAP2 when both MC-LAG links are active on the local BEB1 (see Figure 135)
PBB Features

• The Active SAP and the BVPLS uplink if one of the MC-LAG links is inactive on BEB1
  → PBB tunnel will be considered as a backup path only when the SAP is operationally down.
  → If the SAP is administratively down, then all traffic will be dropped.
• Although the CLI allows configuration of two SAPs and a BVPLS uplink in the same PBB Epipe, the BVPLS uplink is inactive as long as both SAPs are active.
  → Traffic received through PBB tunnel is dropped if BVPLS uplink is inactive.
• The same rules apply to BEB2.
BGP Multi-homing for I-VPLS

This section describes the application of BGP multi-homing to I-VPLS services. BGP multi-homing for I-VPLS uses the same mechanisms as those used when BGP multi-homing is configured in a non-PBB VPLS service, which are described in detail in section BGP Multi-Homing for VPLS on page 620.

The multi-homed sites can be configured with either a SAP or spoke-SDP, and support both split-horizon groups and fate-sharing by the use of oper-groups.

When the B-VPLS service is using LDP signaled pseudowires, blackhole protection is supported after a multi-homing failover event when send-flush-on-failure and send-bvpls-flush flush-all-from-me is configured within the I-VPLS. This causes the system on which the site object fails to send a MAC flush all-from-me message so that customer MACs are flushed on the remote backbone edge bridges using a flush-all-from-me message. The message sent includes a PBB TLV which contains the source BMAC identifying the originator (“mine”/”me”) of the flush indication and the ISID list identifying the I-VPLS instances affected by the flush indication, see section LDP MAC Flush Solution for PBB Blackholing on page 982.

The VPLS preference sent in BGP multi-homing updates will be always be set to zero, however, if a non-zero value is received in a valid BGP multi-homing update it will be used to influence the designated forwarder (DF) election.
Access Multi-Homing over MPLS for PBB Epipes

It is possible to connect backbone edge bridges (BEBs) configured with PBB Epipes to an edge device using active/standby pseudowires over an MPLS network. This is shown in Figure 136.

In this topology, the edge device (CE1) is configured with multiple Epipes to provide virtual lease line (VLL) connectivity across a PBB network. CE1 uses active/standby pseudowires (PWs) which terminate in PBB Epipe services on BEB1 and BEB2 and are signaled accordingly using the appropriate pseudowire status bits.

Traffic is sent from CE1 on the active pseudowires into the PBB epipe services, then onto the remote devices through the B-VPLS service. It is important that traffic sent to CE1 is directed to the BEB that is attached to the active pseudowire connected to CE1. To achieve this, a virtual backbone MAC (vBMAC) is associated with the services on CE1.

The vBMAC is announced into the PBB core by the BEB connected to the active pseudowire using SPBM configured in the B-VPLS services; hence SPBM is mandatory. In Figure 136, the vBMAC would be announced by BEB1; if the pseudowires failed over to BEB2, BEB1 would stop announcing the vBMAC and BEB2 will start announcing it.

The remote services are configured to use the vBMAC as the backbone destination MAC (backbone-dest-mac) which results in traffic being sent to the desired BEB.

The vBMAC is configured under the SDP used to connect to the edge device’s active/standby pseudowires using the command source-bmac-lsb. This command defines a sixteen (16) bit value which overrides the sixteen least-significant-bits of source backbone MAC (source-bmac) to
create the vBMAC. The operator must ensure that the vBMACs match on the two peering BEBs for a corresponding SDP.

The PBB Epipe pseudowires are identified to be connected to an edge device active/standby pseudowire using the spoke-sdp parameter use-sdp-bmac. Enabling this parameter will cause traffic forwarded from this spoke-SDP into the B-VPLS domain to use the vBMAC as its source MAC address when both this, and the control pseudowire, are in the active state on this BEB. Note that PBB Epipe pseudowires connected to edge device’s non-active/standby pseudowires are still able to use the same SDP.

To cater for the case where there are multiple edge device active/standby pseudowires using a given SDP, one pseudowire must be identified to be the control pseudowire (using the source-bmac-lsb parameter control-pw-vc-id). The state of the control pseudowire determines the announcing of the vBMAC by SPBM into the B-VPLS based on the following conditions:

- The source-bmac-lsb and control-pw-vc-id have both been configured.
- The spoke SDP referenced by the control-pw-vc-id has use-sdp-bmac configured.
- The spoke SDP referenced by the control-pw-vc-id is operationally up and the “Peer Pw Bits” do not include pwFwdingStandby.
- If multiple B-VPLS services are used with different SPBM Forward IDs (FIDs), the vBMAC is advertised into any FID which has a PBB Epipe with a spoke SDP configured with use-sdp-bmac that is using an SDP with source-bmac-lsb configured (regardless of whether the PBB Epipe spoke SDP defined as the control pseudowire is associated with the B-VPLS).

It is expected that pseudowires configured using an SDP with source-bmac-lsb and with the parameter use-sdp-bmac are in the same state (up, down, active, standby) as the control pseudowire. If this is not the case, the following scenarios are possible (based on Figure 136):

- If any non-control pseudowires are active on BEB2 and standby on BEB1, then this will continue to allow bi-directional traffic for the related services as the return traffic to CE1 will be sent to BEB1, specifically to the BEB announcing the vBMAC. As the non-control PW is in standby state it will be used to send this traffic to the edge device. If this operation is not desired, it is possible to prevent traffic being sent on a standby PW using the standby-signaling-slave parameter under the spoke SDP definition.
- If any non-control pseudowires are active on BEB2 but down on BEB1, then only unidirectional traffic is possible. The return traffic to CE1 will be sent to BEB1, as it is announcing the vBMAC but the pseudowire on BEB1 is down for this service.

Alarms are raised to track if, on the BEB with the control pseudowire in the standby/down state, any non-control pseudowires go active. Specifically, there will be an alarm when the first non-control pseudowire becomes active and another alarm when the last non-control pseudowire becomes standby/down.
If both control pseudowires are active (neither in standby) then both BEBs would announce the vBMAC – this would happen if the edge device was a 7x50 using an Epipe service without standby-signaling-master configured. Traffic from remote BEBs on any service related to the vBMAC would be sent to the nearest SPBM BEB and it would depend on the state of the pseudowires on each BEB as to whether it could reach the edge device. Similarly, the operator must ensure that the corresponding service pseudowires on each BEB are configured as the control pseudowire, otherwise SPBM might advertise the vBMAC from both BEBs resulting in the same consequences.

All traffic received from the edge device on a pseudowire into a PBB Epipe, on the BEB with the active control pseudowire, is forwarded by the B-VPLS using the vBMAC as the source backbone MAC, otherwise the source-bmac is used.

The control pseudowire can be changed dynamically without shutting down the spoke SDPs, SDP or withdrawing the SPBM advertisement of the vBMAC; this allows a graceful change of the control pseudowire. Clearly, any change should be performed on both BEBs as closely in time as possible to avoid an asymmetric configuration, ensuring that the new control pseudowire is in the same state as the current control pseudowire on both BEBs during the change.

The following are not supported:

- Active/standby pseudowires within the PBB Epipe are not supported, consequently the following are not supported:
  - The configuration of endpoints.
  - The configuration of precedence under the spoke-SDP.
- The use of PW switching.
- BGP-MH support, namely configuring the pseudowires to be part of a multi-homed site.
- Network-domains.
- Support for the following tunneling technologies
  - RFC 3107
  - GRE
  - L2TPv3
  - MPLS-TP
PBB and IGMP Snooping

IGMP snooping feature provided for regular VPLS is supported similarly in the PBB IVPLS context to provide for efficient multicast replication in the customer domain. The difference from regular VPLS is the handling of IGMP messages arriving from the BVPLS side over a BVPLS SAP/SDP.

The first IGMP join message received over the local BVPLS will add all the BVPLS SAP/SDP components into the related multicast table associated with the IVPLS context. This is in line with the PBB model where the BVPLS infrastructure emulates a backbone LAN to which every IVPLS is connected by one virtual link.

When the querier is connected to a remote IVPLS instance, over the BVPLS infrastructure, its location is identified by the BVPLS SDP/SAP on which the query was received and also by the source BMAC address used in the PBB header for the query message, the BMAC associated with the BVPLS instance on the remote PBB PE.
PBB QoS

For PBB encapsulation, the configuration used for DE and dot1p in SAP and SDP policies applies to the related bits in both backbone dot1q (BTAG) and ITAG fields.

The following QoS processing rules apply for PBB B-VPLS SAPs and SDPs:

**B-VPLS SAP ingress**

- If dot1p, DE based classification is enabled, the BTAG fields will be used by default to evaluate the internal forwarding class (fc) and discard profile if there is a BTAG field. The 802.1ah ITAG will be used only if the BTAG is absent (null SAP).
- If either one of the dot1p or DE based classification is not explicitly enabled or the packets are untagged then the default fc and profile is assigned.

**B-VPLS SAP egress**

- If the sap-egress policy for the SAP contains an fc to dot1p/de mapping, this entry is used to set the dot1p and DE bits from the BTAG of the frame going out from the SAP. The same applies for the ITAG on frames originated locally from an I-VPLS. The mapping does not have any effect on the ITAG of frames transiting the B-VPLS.
- If no explicit mapping exists, the related dot1p DE bits are set to zero on both ITAG and BTAG if the frame is originated locally from an I-VPLS. If the frame is transiting the B-VPLS the ITAG stays unchanged, the BTAG is set according to the type of ingress SAP.
  - If the ingress SAP is tagged, the values of the dot1p, DE bits are preserved in the BTAG going out on the egress SAP.
  - If the ingress SAP is untagged, the dot1p, DE bits are set to zero in the BTAG going out on the egress SAP.

**B-VPLS SDP (network) ingress policy**

- QoS policies for dot1p and DE bits apply only for the outer VLAN ID: this is the VLAN ID associated with the link layer and not the PBB BTAG. As a result, the dot1p DE bits will be checked if an outer VLAN ID exists in the packets ingressing the SDP. If that VLAN ID is absent, nothing above the pseudowire SL will be checked - for example, no dot1p bits in the BTAG or ITAG will be checked. It is expected that the EXP bits will be used to transport QoS information across the MPLS backbone and into the PEs.

**B-VPLS SDP (network) egress policy**

- When building PBB packets originating from a local I-VPLS, the BTAG and ITAG values (dot1p, DE bits) will be set according to the network egress policy. The same applies for newly added BTAG (VLAN mode pseudowires) in a packet transiting the B-VPLS (SAP/
SDP to SDP). Note that if either dot1p or DE based classification is not explicitly enabled in the CLI, the values from the default fc to dot1p, DE mapping are assumed.

- Dot1p, DE bits for existing BTAGs will remain unchanged - for example, applicable to packets transiting the B-VPLS and going out on SDP.

---

**Transparency of Customer QoS Indication through PBB Backbone**

Similar to PW transport, operators want to allow their customers to preserve all eight Ethernet COS markings (three dot1p bits) and the discard eligibility indication (DE bit) while transiting through a PBB backbone.

This means any customer COS marking on the packets inbound to the ingress SAP must be preserved when going out on the egress SAP at the remote PBB PE even if the customer VLAN tag is used for SAP identification at the ingress.

A solution to the above requirements is depicted in Figure 137.

![Figure 137: PCP, DE Bits Transparency in PBB](image)

The PBB BVPLS is represented by the blue pipe in the middle with its associated COS represented through both the service (I-tag) and tunnel COS (BVID dot1p+DE or PW EXP bits).

The customer COS is contained in the orange dot1q VLAN tags managed in the customer domains. There may be one (CVID) or two (CVID, SVID) tags used to provide service classification at the SAP. IVPLS or PBB Epipe instances (orange triangles) are used to provide a Carrier-of-Carrier service.

As the VLAN tags are stripped at the ingress SAP and added back at the egress SAP, the PBB implementation must provide a way to maintain the customer QoS marking. This is done using a force-qtag-forwarding configuration on a per IVPLS/Epipe basis under the node specifying the uplink to the related BVPLS. When force-qtag-forwarding is enabled, a new VLAN tag is added.
right after the CMAC addresses using the configured QTAG. The dot1p, DE bits from the specified outer/inner customer QTAG will be copied in the newly added tag.

Once the force-qtag-forwarding is enabled in one IVPLS/PBB Epipe instance, it will be enabled in all of the related instances.

At the remote PBB PE/BEB on the egress SAPs or SDPs, the first QTAG after the CMAC addresses will be removed and its dot1p, DE bits will be copied in the newly added customer QTAGs.

---

**Configuration Examples**

This section gives usage examples for the new commands under PBB Epipe or IVPLS instances.

**PBB IVPLS usage:**

```bash
configure service vpls 100 ivpls
  sap 1/1/1:101
  pbb
    backbone-vpls 10 isid 100
    force-qtag-forwarding
```

**PBB Epipe Usage:**

```bash
configure service epipe 200
  sap 1/1/1:201
  pbb
    tunnel 10 backbone-dest-mac ab-bc-cd-ef-01-01 isid 200
    force-qtag-forwarding
```
Details Solution Description

Figure 137 depicts a specific use case. Keeping the same topology - an ingress PBB PE, a PBB core and an egress PBB PE - let us consider the generic use case where:

1. the packet arrives on the ingress PBB PE on an I-SAP or an I-SDP binding/PW and it is assigned to a PBB service instance (Epipe/IVPLS)
2. goes next through a PBB core (native Ethernet B-SAPs or PW/MPLS based B-SDP)
3. lastly, egresses at another PBB PE through a PBB service instance on either an I-SAP or I-SDP binding/PW.

Similar to the Ethernet-VLAN VC Type, the following packet processing steps apply for different scenarios.

- **Ingress PE, ingress I-SAP case** with force-qtag-forwarding enabled under PBB Epipe or IVPLS
  
The QTAG is inserted automatically right after CMAC addresses; an ethertype value of 8100 is used.
  
  → **Case 1**: SAP type = null/dot1q default (1/1/1 or 1/1/1.*) so there is no service delimiting tag used and stripped on the ingress side.
    - VLAN and Dot1p+DE bits on the inserted QTAG are set to zero regardless of ingress QoS policy
  
  → **Case 2**: SAP type = dot1q or qinq default (1/1/1.100 or 1/1/1.100.*) so there is a service delimiting tag used and stripped.
    - The service delimiting QTAG (dot1p + DE bits and VLAN) is copied as is in the inserted QTAG.
  
  → **Case 3**: SAP type = qinq (1/1/1.100.10) so there are two service delimiting tags used and stripped.
    - The service delimiting QTAG (VLAN and dot1p + DE bits) is copied as is from the inner tag in the inserted QTAG.

- **Ingress PE, ingress I-SDP/PW case** with force-qtag-forwarding enabled under PBB Epipe or IVPLS
The QTAG is inserted automatically right after CMAC addresses; an ethertype value of 8100 is used.

→ **Case 1**: SDP vc-type = Ethernet (force-vlan-vc-forwarding= not supported for I-PW) so there is no service delimiting tag stripped on the ingress side.
   - VLAN and Dot1p+DE bits on the inserted QTAG are set to zero regardless of ingress QoS policy

→ **Case 2**: SDP vc-type = Ethernet VLAN so there is a service delimiting tag stripped.
   - VLAN and Dot1p + DE bits on the inserted QTAG are preserved from the service delimiting tag.

PBB packets are tunneled through the core the same way for native ETH/MPLS cases.
• **Egress PE, egress I-SAP case** with force-qtag-forwarding enabled under PBB Epipe or VPLS
  
  → The egress QoS policy (FC->dot1p+DE bits) is used to determine the QoS settings of the added QTAGs. If it required to preserve the ingress QoS, no egress policy should be added.
    
    − If QinQ SAP is used, at least qinq-mark-top-only option must be enabled to preserve the CTAG.
  
  → The “core QTAG” (core = received over the PBB core, 1st after CMAC addresses) is always removed after QoS information is extracted.
    
    − If no force-qtag-forwarding is used at egress PE, the inserted QTAG is maintained.
  
  → If egress SAP is on the ingress PE, then the dot1p+DE value is read directly from the procedures described in Ingress PE, ingress I-SAP and Ingress PE, ingress I-SDP/PW cases. The use cases below still apply.
  
  → **Case 1**: SAP type = null/dot1q default (2/2/2 or 2/2/2.*) so there is no service delimiting tag added on the egress side.
    
    − Dot1p+DE bits and the VLAN value contained in the QTAG are ignored.
  
  → **Case 2**: SAP type = dot1q/qinq default (3/1/1.300 or 3/1/1.300.*) so a service delimiting tag is added on egress
    
    − The FC->dot1p, DE bit entries in the SAP egress QoS policy are applied.
    
    − If there are no such entries, then the values of the dot1p+DE bits from the stripped QTAG are used.
  
  → **Case 3**: SAP type = qinq (3/1/1.300.30) so two service delimiting tags are added on egress
    
    − The FC->dot1p, DE bit entries in the SAP egress QoS policy are applied.
    
    − If the **qinq-mark-top-only** command under **vpls>sap>egress** is not enabled (default), the policy is applied to both service delimiting tags.
    
    − If the qinq-mark-top-only command is enabled, the policy is applied only to the outer service delimiting tag.
    
    − On the tags where the egress QoS policies do not apply the values of the dot1p+DE bits from the stripped QTAG are used.
• **Egress PE, egress I-SDP case** with force-qtag-forwarding enabled under PBB Epipe or IVPLS
  
  → **Case 1**: I-SDP vc-type = Ethernet VLAN so there is service delimiting tag added after PW encapsulation.
    - The dot1p+DE bits from the QTAG received over the PBB core side are copied to the QTAG added on the I-SDP.
    - The VLAN value in the QTAG might change to match the provisioned value for the I-SDP configuration.
  
  → **Case 2**: I-SDP vc-type = Ethernet (force-vlan-vc-forwarding=not supported for I-SDPs) so there is no service delimiting tag added on egress PW
    - The QTAG received over the PBB core is stripped and the QoS information is lost.
Egress B-SAP per ISID Shaping

This feature allows users to perform egress data path shaping of packets forwarded within a B-VPLS SAP. The shaping is performed within a more granular context within the SAP. The context for a B-SAP is an ISID.

B-SAP Egress ISID Shaping Configuration

Users can enable the per-ISID shaping on the egress context of a B-VPLS SAP by configuring an encapsulation group, referred to as `encap-group` in CLI, under the QoS sub-context, referred to as `encap-defined-qos`.

```
config>service>vpls>sap>egress>encap-defined-qos>encap-group
```

The group name is unique across all member types. The `isid` type is currently the only option.

The user adds or removes members to the `encap-group`, one at a time or as a range of contiguous values. However, when the `qos-per-member` option is enabled, members must be added or removed one at a time. These members are also referred to as ISID contexts.

```
config>service>vpls>sap>egress>encap-defined-qos>encap-group
```

Once a group is created, the user assigns a SAP egress QoS policy, and optionally a scheduler policy or aggregate rate limit, using the following commands:

```
config>service>vpls>sap>egress>encap-defined-qos>encap-group>qos sap_egress_policy-id
config>service>vpls>sap>egress>encap-defined-qos>encap-group>scheduler-policy scheduler_policy-name
config>service>vpls>sap>egress>encap-defined-qos>encap-group>agg-rate-limit kilobits-per-second
```
Note that a SAP egress QoS policy must first be assigned to the created encap-group before the user can add members to this group. Conversely, the user cannot perform the `no qos` command until all members are deleted from the **encap-group**.

An explicit or the default SAP egress QoS policy will continue to be applied to the entire B-SAP but this will serve to create the set of egress queues which will be used to store and forward a packet which does not match any of the defined ISID values in any of the encap-groups for this SAP.

Only the queue definition and fc-to-queue mapping from the encap-group SAP egress QoS policy is applied to the ISID members. All other parameters configurable in a SAP egress QoS policy must be inherited from egress QoS policy applied to the B-SAP.

Furthermore, any other CLI option configured in the egress context of the B-SAP will continue to apply to packets matching a member of any encap-group defined in this B-SAP.

Note also that the SAP egress QoS policy must not contain an active policer or an active queue-group queue or the application of the policy to the encap-group will be failed. A policer or a queue-group queue is referred to as active if one or more FC map to it in the QoS policy. Conversely, the user will not be allowed to assign a FC to a policer or a queue-group queue once the QoS policy is applied to an encap-group.

The **qos-per-member** keyword allows the user to specify that a separate queue set instance and scheduler/agg-rate-limit instance will be created for each ISID value in the encap-group. By default, shared instances will be created for the entire encap-group.

Note that when the B-SAP is configured on a LAG port, the ISID queue instances defined by all the encap-groups applied to the egress context of the SAP will be replicated on each member link of the LAG. The set of scheduler/agg-rate-limit instances will be replicated per link or per XMA depending if the `adapt-qos` option is set to link mode or distribute mode. This is the same behavior as that applied to the entire B-SAP in the current implementation.
Provisioning Model

The main objective of this proposed provisioning model is to separate the definition of the QoS attributes from the definition of the membership of an encap-group. The user can apply the same SAP egress QoS policy to a large number of ISID members without having to configure the QoS attributes for each member.

The following are conditions of the provisioning model:

- A SAP egress policy ID must be assigned to an **encap-group** before any member can be added regardless of the setting of the **qos-per-member** option.
- When **qos-per-member** is specified in the **encap-group** creation, the user must add or remove ISID members one at a time. The command is failed if a range is entered.
- When **qos-per-member** is specified in the **encap-group** creation, the sap-egress QoS policy ID and the scheduler policy name cannot be changed unless the group membership is empty. However, the **agg-rate-limit** parameter value can be changed or the command removed (**no agg-rate-limit**).
- When **qos-per-member** is not specified in the **encap-group** creation, the user may add or remove ISID members as a singleton or as a range of contiguous values.
- When **qos-per-member** is not specified in the **encap-group** creation, the sap-egress QoS policy ID and the scheduler policy name or **agg-rate-limit** parameter value may be changed at anytime. Note however that the user cannot still remove the SAP egress QoS policy (**no qos**) while there are members defined in the encap-group.
- The QoS policy or the scheduler policy itself may be edited and modified while members are associated with the policy.
- There will be a maximum number of ISID members allowed in the lifetime of an encap-group.

Operationally, the provisioning consists of the following steps:

1. Create an encap-group.
2. Define and assign a SAP egress QoS policy to the encap-group. This step is mandatory else the user is allowed to add members to the **encap-group**.
3. Manage membership for the encap-group using the **member** command (or SNMP equivalent).
   - Supports both range and singleton ISIDs
   - Cannot add an ISID if it already exists on the SAP in another encap-group
     - The **member** command is all-or-nothing. No ISID in a range is added if one fails
     - It the first ISID that fails in the error message is identified.
     - Must first remove the ISID using **no member** command.
→ Specifying an ISID in a group that already exists within the group is a no-op (no failure)
→ If insufficient queues or scheduler policies or FC-to-Queue lookup table space exist to support a new member or a modified membership range, the entire member command is failed

4. Define and assign a scheduling policy or agg-rate-limit for the encap-group. This step is optional.

Logically, the encap-group membership operation can be viewed as three distinct functions:

1. Creation or deletion of new queue sets and optionally scheduler/agg-rate-limit at QoS policy association time.
2. Mapping or un-mapping the member ISID to either the group queue set and scheduler (group QoS) or the ISID specific queue set and scheduler (qos-per-member).
3. Modifying the groups objective membership based on newly created or expanded ranges or singletons based on the membership operation.
Egress Queue Scheduling

Figure 138 displays an example of egress queue scheduling.

The queuing and scheduling re-uses existing scheduler policies and port scheduler policy with the difference that a separate set of FC queues are created for each defined ISID context according to the encap-group configured under the egress context of the B-SAP. This is in addition to the set of queues defined in the SAP egress QoS policy applied to the egress of the entire SAP.

The user type in Figure 138 maps to a specific encap-group defined for the B-SAP in CLI. The operator has the flexibility of scheduling many user types by assigning different scheduling parameters as follows:
• A specific scheduler policy to each encap-group with a root scheduler which shapes the aggregate rate of all queues in the ISID context of the encap-group and provides strict priority scheduling to its children.

  A second tier scheduler can be used as a WFQ scheduler to aggregate a subset of the ISID context FC queues. Alternatively, the operator can apply an aggregate rate limit to the ISID context instead of a scheduler policy.

• A specific priority level when parenting the ISID queues or the root of the scheduler policy serving the ISID queues to the port scheduler.

• Ability to use the weighted scheduler group to further distribute the bandwidth to the queues or root schedulers within the same priority level according to configured weights.

In order to make the shaping of the ISID context reflect the SLA associated with each user type, it is required to subtract the operator’s PBB overhead from the Ethernet frame size. For that purpose, a packet byte-offset parameter is added to the context of a queue.

```plaintext
cfg>qos>sap-egress>queue>packet-byte-offset {add bytes | subtract bytes}
```

When a packet-byte-offset value is applied to a queue instance, it adjusts the immediate packet size. This means that the queue rates, like the operational PIR and CIR, and queue bucket updates use the adjusted packet size. In addition, the queue statistics will also reflect the adjusted packet size. Scheduler policy rates, which are data rates, will use the adjusted packet size.

The port scheduler max-rate and priority level rates and weights, if a Weighted Scheduler Group is used, are always “on-the-wire” rates and thus use the actual frame size. The same applies to the agg-rate-limit on a SAP, a subscriber, or a Multi-Service Site (MSS) when the queue is port-parented.

When the user enables frame-based-accounting in a scheduler policy or queue-frame-based-accounting with agg-rate-limit in a port scheduler policy, the queue rate is capped to a user-configured “on-the-wire” rate but the packet-byte-offset value is still in effect as explained above.
**B-SAP per-ISID Shaping Configuration Example**

The following CLI configuration for B-SAP per-ISID shaping achieves the specific use case shown in Figure 138 on page 1011.

```
config
go
    port-scheduler-policy "bvpls-backbone-port-scheduler"
group scheduler-group1 create
    rate 1000
    level 3 rate 1000 group scheduler-group1 weight w1
    level 4 rate 1000 group scheduler-group1 weight w4
    level 5 rate 1000 cir-rate 100
    level 7 rate 5000 cir-rate 5000
    level 8 rate 500 cir-rate 500
exit

    scheduler-policy "user-type1"
    tier 1
    scheduler root
    port-parent level 8 rate pir1 weight w-pir1 cir-level 8 cir-rate cir1 cir-weight w-cir1
    exit
    tier 3
    scheduler wfq
    rate pir1
    parent root
    exit
    exit
exit

    scheduler-policy "user-type2"
    tier 1
    scheduler root
    port-parent level 7 rate pir2 weight w-pir2 cir-level 7 cir-rate cir2 cir-weight w-cir2
    exit
    tier 3
    scheduler wfq
    rate pir2
    parent root
    exit
    exit
exit

    scheduler-policy "b-sap"
    tier 1
    scheduler root
    port-parent level 5 rate pir5 weight w-pir5 cir-level 1 cir-rate cir5 cir-weight w-cir5
    exit
    tier 3
    scheduler wfq
    rate pir5
    parent root
    exit
    exit
exit
```
sap-egress 100 // user type 1 QoS policy
queue 1
  parent wfq weight x level 3 cir-weight x cir-level 3
  packet-byte-offset subtract bytes 22
queue 2
  packet-byte-offset subtract bytes 22
  parent wfq weight y level 3 cir-weight y cir-level 3
queue 3
  packet-byte-offset subtract bytes 22
  parent wfq weight z level 3 cir-weight z cir-level 3
queue 4
  parent root level 8 cir-level 8
  packet-byte-offset subtract bytes 22
fc be queue 1
fc l2 queue 2
fc h2 queue 3
fc ef queue 4
exit

sap-egress 200 // user type 2 QoS policy
queue 1
  parent wfq weight x level 3 cir-weight x cir-level 3
  packet-byte-offset subtract bytes 26
queue 2
  parent wfq weight y level 3 cir-weight y cir-level 3
  packet-byte-offset subtract bytes 26
queue 3
  parent wfq weight z level 3 cir-weight z cir-level 3
  packet-byte-offset subtract bytes 26
queue 4
  parent root level 8 cir-level 8
  packet-byte-offset subtract bytes 26
fc be queue 1
fc l2 queue 2
fc h2 queue 3
fc ef queue 4
exit

sap-egress 300 // User type 3 QoS policy
queue 1
  port-parent level 4 rate pir3 weight w-pir3 cir-level
  4 cir-rate cir3 cir-weight w-cir3
  packet-byte-offset subtract bytes 22
fc be queue 1
exit

sap-egress 400 // User type 4 QoS policy
queue 1
  port-parent level 3 rate pir4 weight w-pir4 cir-level
  3 cir-rate cir4 cir-weight w-cir4
  packet-byte-offset subtract bytes 22
fc be queue 1
exit

sap-egress 500 // B-SAP default QoS policy
queue 1
  parent wfq weight x level 3 cir-weight x cir-level 3
queue 2
  parent wfq weight y level 3 cir-weight y cir-level 3
queue 3
    parent wfq weight z level 3 cir-weight z cir-level 3
queue 4
    parent root level 8 cir-level 8
fc be queue 1
fc 12 queue 2
fc h2 queue 3
fc ef queue 4
exit
exit
exit
config
    service
    vpls 100 bvpls
        sap 1/1/1:100
        egress
            encap-defined-qos
            encap-group type1-grouped type isid
            member 1 to 10
                qos 100
                scheduler-policy user-type1
                exit
        encap-group type1-separate type isid qos-per-member
            member 16
                qos 100
                scheduler-policy user-type1
                exit
    encap-group type2-grouped type isid
        member 21 to 30
            qos 200
            scheduler-policy user-type2
            exit
    encap-group type2-separate type isid qos-per-member
        member 36
            qos 200
            scheduler-policy user-type2
            exit
        encap-group type3-grouped type isid
            member 41 to 50
                qos 300
                exit
            encap-group type4-grouped type isid
                member 61 to 70
                    qos 400
                    scheduler-policy b-sap
                    exit
                    exit
                    exit
                    exit
exit
exit
exit
PBB OAM

Alcatel-Lucent’s PBB implementation support both MPLS and native Ethernet tunneling. In the case of an MPLS, SDP bindings are used as the B-VPLS infrastructure while T-LDP is used for signaling. As a result, the existing VPLS, MPLS diagnostic tools are supported in both I-VPLS and B-VPLS domains as depicted in Figure 139.

![PBB OAM View for MPLS Infrastructure](image)

**Figure 139: PBB OAM View for MPLS Infrastructure**

When an Ethernet switching backbone is used for aggregation between PBB PEs, a SAP is used as the B-VPLS uplink instead of an SDP. No T-LDP signalling is available.

The existing IEEE 802.1ag implemented for regular VPLS SAPs may be used to troubleshoot connectivity at I-VPLS and B-VPLS layers.
**Mirroring**

There are no restrictions for mirroring in I-VPLS or B-VPLS.

---

**OAM Commands**

All VPLS OAM commands may be used in both I-VPLS and B-VPLS instances.

**I-VPLS**

- The following OAM commands are meaningful only towards another I-VPLS service instance (spoke-SDP in I-VPLS):
  - LSP-ping, LSP-trace, SDP-ping, SDP-MTU
- The following I-VPLS OAM exchanges are transparently transported over the B-VPLS core:
  - SVC-ping, MAC-ping, MAC-trace, MAC-populate, MAC-purge, CPE-ping (towards customer CPE), 802.3ah EFM, SAA
- PBB uplinks using MPLS/SPP: there are no PBB specific OAM commands.

**B-VPLS**

- In case of Ethernet switching backbone (B-SAPs on B-VPLS), 802.1ag OAM is supported on B-SAP, operating on:
  - The customer level (C-SA/C-DA and C-type layer)
  - The tunnel level (B-SA/B-DA and B-type layer)

---

**CFM Support**

There is no special 802.1ag CFM (Connectivity Fault Management) support for PBB. B-component and I-components run their own maintenance domain and levels. CFM for I-components run transparently over the PBB network and will appear as directly connected.
Configuration Examples

Use the CLI syntax displayed to configure PBB.

**PBB using G.8031 Protected Ethern**

BEB1 to BCB1 L3: 3/1/1 - Member port of LAG-emulation ET1
BEB1 to BCB2:4/1/1 – terminate ET3

*A:7750_ALU>config>eth-tunnel 1
  description "LAG-emulation to BCB1 ET1"
  protection-type loadsharing
  ethernet
    mac 00:11:11:11:11:12
    encap-type dot1q
  exit
  ccm-hold-time down 5 up 10 // 50 ms down, 1 sec up
  lag-emulation
    access adapt-qos distribute
    path-threshold 1
  exit
  path 1
    member 1/1/1
    control-tag 0
    eth-cfm
      ...
    exit
    no shutdown
  exit
  path 2
    member 2/1/1
    control-tag 0
    eth-cfm
      ...
    exit
    no shutdown
  exit
  path 3
    member 3/1/1
    control-tag 0
    eth-cfm
      ...
    exit
    no shutdown
  exit
  no shutdown
--------------------------------------------------

*A:7750_ALU>config>eth-tunnel 3
  description "G.8031 tunnel ET3"
  protection-type 8031_1to1
  ethernet
    mac 00:11:11:11:11:11
    encap-type dot1q
  exit
ccm-hold-time down 5 // 50 ms down, no up hold-down
path 1
  member 1/1/1
  control-tag 5
  precedence primary
  eth-cfm
    mep 2 domain 1 association 1
ccm-enable
    control-mep
    no shutdown
  exit
exit
no shutdown
exit

path 2
  member 4/1/1
  control-tag 5
  eth-cfm
    mep 2 domain 1 association 2
ccm-enable
    control-mep
    no shutdown
  exit
exit
no shutdown
exit
no shutdown

# Service config

* A:7750_ALU> config> service vpls 1 customer 1 m-vpls b-vpls create
description "m-VPLS for multipoint traffic"
stp
  mst-name "BVPLS"
  mode p-mstp
  mst-instance 10
    mst-priority 4096
    vlan-range 100-199
  exit
  mst-instance 20
    mst-priority 8192
    vlan-range 200-299
  exit
no shutdown
exit

sap eth-tunnel-1 create // BSAP0 to BCB E
sap 4/1/1:0 create // physical link to BCB F (NOTE 0 or 0.*)
  // indicate untagged for m-VPLS)
  exit
no shutdown

# Service config: one of the same-fate SAP over
# loadsharing tunnel

A:7750_ALU> config service vpls 100 customer 1 b-vpls create
  sap eth-tunnel-1:1 create // to BCB E
  // must specify tags for each path for loadsharing
  eth-tunnel
path 1 tag 100
path 2 tag 100
path 3 tag 100
exit
no shutdown ...
sap 3/1/1:200 // to BCBF ...

A:7750_ALU>config service vpls 1000 customer 1 i-vpls create
    pbb backbone-vpls 100 isid 1000
    sap 4/1/1:200 // access SAP to QinQ

# Service config: one of epipes into b-VPLS protected tunnel
# as per R7.0 R4

A:7750_ALU>config service service vpls 3 customer 1 b-vpls create
    sap eth-tunnel-3 create
...

CLI Syntax:
port 1/1/1
    ethernet
        encap-type dot1q
port 2/2/2
    ethernet
        encap-type dot1q
config eth-tunnel 1
    path 1
        member 1/1/1
        control-tag 100
        precedence primary
        eth-cfm
            mep 51 domain 1 association 1 direction down
            ccm-enable
            low-priority-defect allDef
            mac-address 00:AE:AE:AE:AE:AE
        control-mep
        no shutdown
        no shutdown
    path 2
        member 2/2/2
        control-tag 200
        eth-cfm
            mep
                mep 52 domain 1 association 2 direction down
                ccm-enable
                low-priority-defect allDef
                mac-address 00:BE:BE:BE:BE:BE

...
control-mep
no shutdown
no shutdown

config service vpls 1 b-vpls
  sap eth-tunnel-1
config service epipe 1000
  pbb-tunnel 1 backbone-dest-mac remote-beb
  sap 3/1/1:400.10

**MC-LAG Multihoming for Native PBB**

This section describes a configuration example for BEB C configuration given the following assumptions:

- BEB C and BEB D are MC-LAG peers
- B-VPLS 100 on BEB C and BEB D
- VPLS 1000 on BEB C and BEB D
- MC-LAG 1 on BEB C and BEB D

**CLI Syntax:**

```
service pbb
  source-bmac ab-ac-ad-ef-00-00
port 1/1/1
  ethernet
    encap-type qinq
lag 1
  port 1/1/1 priority 20
  lacp active administrative-key 32768
redundancy
  multi-chassis
  peer 1.1.1.3 create
    source-address 1.1.1.1
  mc-lag
    lag 1 lacp-key 1 system-id 00:00:00:01:01:01
    system-priority 100
    source-bmac-1sb use-lacp-key

service vpls 100 bvpls
  sap 2/2/2:100 // bvid 100
  mac-notification
  no shutdown

service vpls 101 bvpls
  sap 2/2/2:101 // bvid 101
  mac-notification
  no shutdown
```
/ no per BVPLS source-bmac configuration, the chassis one (ab-ac-ad-ef-00-00) is used

service vpls 1000 ivpls
    backbone-vpls 100
    sap lag-1:1000 //automatically associates the SAP with ab-ac-ad-ef-00-01 (first 36 bits from BVPLS 100 sbmac+16bit source-bmac-lsb)

service vpls 1001 ivpls
    backbone-vpls 101
    sap lag-1:1001 //automatically associates the SAP with ab-ac-ad-ef-00-01 (first 36 bits from BVPLS 101 sbmac+16bit source-bmac-lsb)
Access Multi-Homing over MPLS for PBB Epipes

This section gives an example configuration for BEB1 from Figure 136.

*A:BEB1>config>service# info

-- ---------------------------------------------------------------

pbb
  source-bmac 00:00:00:00:11:11
  mac-name "remote-BEB" 00:44:44:44:44
  exit
sdp 1 mpls create
  far-end 1.1.1.4
  idp
  keep-alive
  shutdown
  exit
  source-bmac-lsb 33:33 control-pw-vc-id 100
  no shutdown
  exit
vpls 10 customer 1 b-vpls create
  service-mtu 1532
  stp
    shutdown
  exit
  spb 1024 fid 1 create
    no shutdown
  exit
  sap 1/1/1:10 create
    spb create
    no shutdown
    exit
  exit
  sap 1/1/5:10 create
    spb create
    no shutdown
    exit
  exit
  no shutdown
  exit
epipe 100 customer 1 create
  pbb
    tunnel 10 backbone-dest-mac "remote-BEB" isid 100
    exit
  spoke-sdp 1:100 create
    use-sdp-bmac
    no shutdown
    exit
  no shutdown
  exit
epipe 101 customer 1 create
  pbb
    tunnel 10 backbone-dest-mac "remote-BEB" isid 101
    exit
  spoke-sdp 1:101 create
    use-sdp-bmac
    no shutdown
    exit
The SDP control pseudowire information can be seen using this command:

*A:BEB1# show service sdp 1 detail

Service Destination Point (Sdp Id : 1) Details

Sdp Id 1 - 1.1.1.4

Description : (Not Specified)
SDP Id : 1
SDP Source : manual
Src B-MAC LSB : 33-33
Ctrl PW VC ID : 100
Ctrl PW Active : Yes

The configuration of a pseudowire to support remote active/standby PBB Epipe operation can be seen using this command:

*A:BEB1# show service id 100 sdp 1:100 detail

Service Destination Point (Sdp Id : 1:100) Details

Sdp Id 1:100 - (1.1.1.4)

Description : (Not Specified)
SDP Id : 1:100
Type : Spoke
Src B-MAC LSB : 33-33
Ctrl PW VC ID : 100
Ctrl PW Active : Yes
Use SDP B-MAC : True
PBB Command Reference

Command Hierarchies

• Global Commands on page 1025
• SAP Commands on page 1026
• Mesh SDP Commands on page 1027
• Spoke SDP Commands on page 1027
• Show Commands on page 1029
• Clear Commands on page 1029
• Debug Commands on page 1030

Global Commands

```_Config
 — service
  — [no] vpls service-id [customer customer-id] [vpn vpn-id] [m-vpls] [b-vpls] [i-vpls] [create]
  — [no] spb instance [fid value] [create]
  — [no] shutdown
  — level level-number
    — bridge-priority value
    — ect-algorithm name fid-range fid-range
    — forwarding-tree-topology [st spf]
  — lsp-lifetime seconds
  — no lsp-lifetime
  — lsp-wait lsp-wait [lsp-initial-wait [lsp-second-wait]]
  — overload [timeout seconds]
  — no overload
  — overload-on-boot [timeout seconds]
  — no overload-on-boot
  — [no] spf-wait spf-wait [spf-initial-wait [spf-second-wait]]
  — spbm-control-vpls mgmt vpls svc id fid val
  — no spbm-control-vpls
  — mrp
    — [no] attribute-table-high-wmark high-water-mark
    — [no] attribute-table-low-wmark low-water-mark
    — [no] attribute-table-size max-attributes
    — flood-time flood-time
    — no flood-time
    — [no] shutdown

_Config
 — service
  — pbb
    — mac-name name ieee-address
    — no mac-name
```
--- source-bmac ieee-address
--- no source-bmac

config
--- service
--- [no] vpls service-id [customer customer-id] [b-vpls] [create]
--- pbb
--- [no] force-qtag-forwarding
--- source-bmac ieee-address
--- no source-bmac
--- [no] use-sap-bmac
--- mac-notification
--- [no] count value
--- [no] interval value
--- renotify value
--- no renotify

config
--- service
--- [no] vpls service-id [customer customer-id] [i-vpls] [create]
--- pbb
--- backbone-vpls service-id [isid isid]
--- no backbone-vpls
--- igmp-snooping
--- [no] mrouter-dest mac-name
--- [no] sap sap-id
--- igmp-snooping
--- [no] mrouter-port
--- [no] sdp sd-id:vc-id
--- igmp-snooping
--- [no] mrouter-port
--- [no] stp
--- [no] force-qtag-forwarding
--- [no] send-bvpls-flush {[all-from-me] | [all-but-mine]}

config
--- service
--- epipe service-id [customer customer-id] [create] [vpn vpn-id] [vc-switching]
--- no epipe service-id
--- pbb
--- [no] force-qtag-forwarding

SAP Commands

config
--- service
--- [no] vpls service-id [customer customer-id] [vpn vpn-id] [mvpls] [b-vpls|i-vpls] [create]
--- sap sap-id [split-horizon-group group-name] [create]
--- no sap sap-id
--- mrp
--- [no] join-time value
Mesh SDP Commands

config
  service
    — [no] vpls service-id [customer customer-id] [vpn vpn-id] [mvpls] [b-vpls|i-vpls] [create]
    — mesh-sdp sdid;vc-id [vc-type {ether | vlan}]
    — no mesh-sdp sdid;vc-id
    — mrp
      — [no] join-time value
      — [no] leave-all-time value
      — [no] leave-time value
      — [no] mrp-policy policy-name
      — [no] periodic-time value
      — [no] periodic-timer

Spoke SDP Commands

config
  service
    — [no] vpls service-id [customer customer-id] [vpn vpn-id] [mvpls] [b-vpls|i-vpls] [create]
    — spoke-sdp sdid;vc-id [vc-type {ether | vlan}] [split-horizon-group group-name]
    — no spoke-sdp sdid;vc-id
    — mrp
      — [no] join-time value
      — [no] leave-all-time value
      — [no] leave-time value
      — [no] mrp-policy policy-name
      — [no] periodic-time value
      — [no] periodic-timer
    — [no] spb create
      — [no] shutdown
      — lsp-pacing-interval milliseconds
      — no lsp-pacing-interval
      — retransmit-interval seconds
— **no retransmit-interval**
— **metric** value
— **no metric**
  — **hello-interval** seconds
  — **no hello-interval**
  — **hello-multiplier** multiplier
  — **no hello-multiplier**

### BGP-MH for I-VPLS Commands

```plaintext
config
  — service
    — vpls service-id [customer customer-id] [vpn vpn-id] [m-vpls | b-vpls | i-vpls] [create]
    — no vpls service-id
      — site name [create]
      — no site name
        — boot-timer seconds
        — no boot-timer
        — failed-threshold [1..1000]
        — failed-threshold all
        — [no] mesh-sdp-binding
        — monitor-oper-group name
        — no monitor-oper-group
        — sap sap-id
        — no sap
        — [no] shutdown
        — site-activation-timer seconds
        — no site-activation-timer
        — site-id value
        — no site-id
        — split-horizon-group group-name
        — no split-horizon-group
        — spoke-sdp sdp-id:vc-id
        — no spoke-sdp
```
Show Commands

```
show
  - eth-cfm
    - association [ma-index] [detail]
    - cfm-stack-table [port port-id [vlan vlan-id]] | sdp sd-p-id[vc-id] [level 0..7] [direction up|down]
    - domain [md-index] [association ma-index | all-associations [detail]]
    - mep mep-id domain md-index association ma-index [loopback] [linktrace]
  - service
    - id service-id
      - i-vpls
        - mrp-policy mac [ieee-address]
        - mrp
      - spb
        - adjacency [detail]
        - base
        - database
        - fate-sharing
        - fid [fid] fate-sharing
        - fid [fid] user-service
        - fid [fid] fdb
        - fid [fid] mfib [group-mac <ieee-address>]
        - fid [fid] mfib [isid <isid>]
        - hostname
        - interface
        - mfib [detail]
        - routes
        - spf
        - spf-log
        - status
      - mrp-policy [mrp-policy]
      - mrp-policy mrp-policy [association]
      - mrp-policy mrp-policy [entry entry-id]
  - pbb
    - base
    - mac-name [detail]
```

Clear Commands

clear

```
clear
  - service
    - statistics
      - id service-id
        - counters
        - mesh-sdp sd-p-id[vc-id] {all | counters | stp | mrp}
        - mrp
        - spoke-sdp sd-p-id[vc-id] {all | counters | stp | mrp}
        - stp
        - spb
          - adjacency [detail]
          - database
          - spf-log
          - status
```
— sap sap-id {all | counters | stp | l2pt | mrp}

Debug Commands

debu

— service

— id service-id

— [no] mrp

— all-events
— [no] applicant-sm
— [no] leave-all-sm
— [no] mmrp-mac ieee-address
— [no] mrpdu
— [no] periodic-sm
— [no] registrant-sm
— [no] sap sap-id
— [no] sdp sdp-id:vc-id
— [no] spb

— [no] adjacency {sap sap-id | spoke-sdp sdp-id:vc-id | nbr-system-id}
— [no] interface { sap <sap-id> | spoke-sdp <sdp-id:vc-id>}
— [no] l2db
— [no] sdb {system-id | lsp-id}
— [no] packet { pttop-hello l1-hello l1-psnp l1-csnp l1-lsp}

detail
— [no] spf { system-id }
VPLS Service Commands

vpls

Syntax     vpls service-id customer customer-id vpn vpn-id [m-vpls] [b-vpls | i-vpls] [create]
no vpls service-id

Context     config>service

Description  This command creates or edits a Virtual Private LAN Services (VPLS) instance. The vpls command is used to create or maintain a VPLS service. If the service-id does not exist, a context for the service is created. If the service-id exists, the context for editing the service is entered.

A VPLS service connects multiple customer sites together acting like a zero-hop, layer 2 switched domain. A VPLS is always a logical full mesh.

When a service is created, the create keyword must be specified if the create command is enabled in the environment context. When a service is created, the customer keyword and customer-id must be specified and associates the service with a customer. The customer-id must already exist having been created using the customer command in the service context. Once a service has been created with a customer association, it is not possible to edit the customer association. The service must be deleted and recreated with a new customer association.

Once a service is created, the use of the customer customer-id is optional for navigating into the service configuration context. Attempting to edit a service with the incorrect customer-id specified will result in an error.

More than one VPLS service may be created for a single customer ID.

By default, no VPLS instances exist until they are explicitly created.

The no form of this command deletes the VPLS service instance with the specified service-id. The service cannot be deleted until all SAPs and SDPs defined within the service ID have been shutdown and deleted, and the service has been shutdown.

service-id — The unique service identification number identifying the service in the service domain.
    This ID must be unique to this service and may not be used for any other service of any type. The service-id must be the same number used for every SR OS router on which this service is defined.

Values     1 — 2147483648

customer customer-id — Specifies the customer ID number to be associated with the service. This parameter is required on service creation and optional for service editing or deleting.

Values     1 — 2147483647
VPLS Service Commands

**vpn vpn-id** — Specifies the VPN ID number which allows you to identify virtual private networks (VPNs) by a VPN identification number.

**Values**

- 1 — 2147483647

**Default**

null (0)

**m-vpls** — Specifies a management VPLS.

**b-vpls | i-vpls** — Creates a backbone-vpls or ISID-vpls for use with PBB

### eth-tunnel

**Syntax**

```
eth-tunnel tunnel-id
```

**Context**

```
cfg>service>vpls
```

**Description**

This command associates a BVPLS SAP with the global Ethernet tunnel object specified by tunnel-id. Only one-to-one mapping between SAP and Ethernet tunnel is supported in the initial implementation. The global eth-tunnel tunnel-id with at least a member port must be configured in advance for the command to be successful. A SAP will be instantiated using the active path components (member port and control-tag) for VPLS forwarding. The last member port in the Ethernet Tunnel cannot be deleted if there is a SAP configured on that eth-tunnel. This command is only available in the BVPLS context.

The **no** form of this command removes the sap from the Ethernet tunnel object.

**Default**

no sap is specified

**Parameters**

- **tunnel-id** — Specifies the value of the Ethernet tunnel identifier to be used for the SAP.

  **Values**

  1-64

### spb

**Syntax**

```
[no] spb instance [fid value] [create]
```

**Context**

```
cfg>service>vpls <instance> b-vpls
```

**Description**

This command enables Shortest Path Bridging (SPB) on a B-VPLS instance. SPB uses IS-IS that supports multiple instances, therefore an instance must be specified. The declaration of SPB in this context is the control configuration for the SPB. This is an SPB management interface and it manages the configuration for IS-IS. Various parameters that define this SPB instance are configured under this SPB instance. Several of the parameters are shared with other B-VPLS service instances using SPB.

SPB enables an instance of IS-IS protocol with the no shutdown command. Alternatively, the IS-IS protocol instance under SPB is disabled with the shutdown command in the `config>service>vpls <instance> b-vpls` context.

A Forwarding Identifier (FID) is optionally specified which is an abstraction of the B-VID used for forwarding in SPB. When no FID is configured the control VPLS is advertised with FID value 1.
When a FID value is specified, the control VPLS is advertised and associated with the FID value specified. The default algorithm for any FID declared or implicit is low-path-id. When a FID is specified, the ect-algorithm can be specified for the FID and changed only when there are no VPLS, SAPs or SDP bindings associated with the FID. The FID for a control instance cannot be changed once created. To change a FID the SPB component would have to be shutdown, deleted and recreated with a new FID.

Default  

Parameters  

instance-id — Specifies the instance ID for an SPB IS-IS instance.  

Values  1024–2047 (4 available)  

Default  1024  

FID — Specifies FID value.  

Values  1-4095  

Default  1  

Note: SPB operates with disable-learning, disable aging and discard-unknown. The state of these commands is ignored when SPB is configured.

spb

Syntax  

[no] spb [create]  

Context  

cfg>service>vpls <instance> b-vpls>sap>spb>  
cfg>service>vpls <instance> b-vpls>spoke-sdp>spb>  

Description  

This command enables Shortest Path Bridging (SPB) on SAP or Spoke SDP. The B-VPLS may be a control B-VPLS or user B-VPLS. Since SPB uses IS-IS that supports multiple instances, SPB inherits the instance from the control B-VPLS.  

SPB at this context level is enabled immediately. SPB enables an instance of IS-IS protocol with the no shutdown command. Alternatively, the IS-IS protocol instance under SPB is disabled with the shutdown command in the config>service>vpls <instance> b-vpls>spb context.

Default  

no spb

spbm-control-vpls

Syntax  

spbm-control-vpls service-id fid fid  

no spbm-control-vpls  

Context  

cfg>service>vpls service-id b-vpls>  

Description  

This command associates a user B-VPLS with a particular control B-VPLS and a FID. The ECT algorithm and the behavior of unicast and multicast come from the association to the FID.  

A Forwarding Identifier (FID) is specified which is an abstraction of the B-VID used for forwarding in SPB. The ect-algorithm is associated with the FID and can be changed only when there are no
VPLS, SAPs or SDP bindings associated with the FID. The FID must be independent from the FID assigned to other services.

none

shutdown

Syntax

[no] shutdown

Context

config>service>vpls <instance> b-vpls>spb>
config>service>vpls <instance> b-vpls>sap>spb>
config>service>vpls <instance> b-vpls>spoke-sdp>spb>

Description
This command administratively disables an entity. When disabled, an entity does not change, reset, or remove any configuration settings or statistics.

The operational state of the entity is disabled as well as the operational state of any entities contained within.

The no form of this command administratively enables an entity.

SPB Interface — In the config>service>vpls <instance> b-vpls>spb> context, the command disables the IS-IS interface. By default, the IS-IS interface is disabled, shutdown.

lsp-lifetime

Syntax

lsp-lifetime seconds
no lsp-lifetime

Context

config>service>vpls <instance> b-vpls>spb

Description
This command sets the time, in seconds, SPB wants the LSPs it originates to be considered valid by other routers in the domain. This is a control B-VPLS command.

Each LSP received is maintained in an LSP database until the lsp-lifetime expires unless the originating router refreshes the LSP. By default, each router refreshes its LSP’s every 20 minutes (1200 seconds) so other routers will not age out the LSP.

The LSP refresh timer is derived from this formula: lsp-lifetime/2

The no form of the command reverts to the default value.

Default
1200 — LSPs originated by SPB should be valid for 1200 seconds (20 minutes).

Parameters

seconds — The time, in seconds, that SPB wants the LSPs it originates to be considered valid by other routers in the domain.

Values
350 — 65535

lsp-wait
Syntax  lsp-wait [lsp-initial-wait [lsp-second-wait]]

Context  config>service>vpls <instance> b-vpls>spb

Description  This command is used to customize the throttling of SPB LSP-generation. Timers that determine when to generate the first, second and subsequent LSPs can be controlled with this command. Subsequent LSPs are generated at increasing intervals of the second lsp-wait timer until a maximum value is reached. This is a control B-VPLS command.

Parameters  

- **lsp-max-wait** — Specifies the maximum interval in seconds between two consecutive occurrences of an LSP being generated.
  
  **Values** 1 — 120
  
  **Default** 5

- **lsp-initial-wait** — Specifies the initial LSP generation delay in seconds.
  
  **Values** 0 — 100
  
  **Default** 0

- **lsp-second-wait** — Specifies the hold time in seconds between the first and second LSP generation.
  
  **Values** 1 — 100
  
  **Default** 1

overload

Syntax  overload [timeout seconds]

no overload

Context  config>service>vpls <instance> b-vpls>spb

Description  This command administratively sets the SPB to operate in the overload state for a specific time period, in seconds, or indefinitely. During normal operation, the router may be forced to enter an overload state due to a lack of resources. When in the overload state, the router is only used if the destination is reachable by SPB and will not used for other transit traffic.

If a time period is specified, the overload state persists for the configured length of time. If no time is specified, the overload state operation is maintained indefinitely.

The overload command can be useful in circumstances where SPB is overloaded or used prior to executing a shutdown command to divert traffic around the switch.

The no form of the command causes the router to exit the overload state.

**Default**  no overload

Parameters  

- **seconds** — The time, in seconds, that this router must operate in overload state.
  
  **Values** 60 — 1800
  
  **Default**  Infinity (overload state maintained indefinitely)
**overload-on-boot**

**Syntax**

overload-on-boot [timeout seconds]

no overload-on-boot

**Context**

config>service>vpls <instance> b-vpls>spb>

**Description**

When the router is in an overload state, SPB the B-VPLS is used only if there is no other SPB B-VPLS to reach the destination. This command configures the IGP upon bootup in the overload state until one of the following events occur:

- The timeout timer expires.
- A manual override of the current overload state is entered with the `config>service>vpls instance>b-vpls>spb>no overload` command.

The no form of the command does not affect the overload-on-boot function.

If no timeout is specified, SPB IS-IS goes into overload indefinitely after a reboot. After the reboot, the SPB IS-IS status displays a permanent overload state:

```
L1 LSDB Overload : Manual on boot (Indefinitely in overload)
```

This state can be cleared with the `config>service>vpls instance>b-vpls>spb>no overload` command.

When specifying a timeout value, SPB IS-IS goes into overload for the configured timeout after a reboot. After the reboot, SPB IS-IS status displays the remaining time the system stays in overload:

```
L1 LSDB Overload : Manual on boot (Overload Time Left : 17)
```

The overload state can be cleared before the timeout expires with `config>service>vpls instance>b-vpls>spb>no overload` command.

The no form of the command removes the overload-on-boot functionality from the configuration.

**Default**

no overload-on-boot

**Parameters**

seconds — The time, in seconds, that this router must operate in overload state.

**Values**

60 — 1800

**Default**

Infinity (overload state maintained indefinitely)

**spf-wait**

**Syntax**

[no] spf-wait spf-wait [spf-initial-wait [spf-second-wait]]

**Context**

config>service>vpls <instance> b-vpls>spb>

**Description**

This command defines the maximum interval between two consecutive SPF calculations in seconds. Timers that determine when to initiate the first, second and subsequent SPF calculations after a topology change occurs can be controlled with this command.

Subsequent SPF runs (if required) occur at exponentially increasing intervals of the spf-second-wait interval. For example, if the spf-second-wait interval is 1000, then the next SPF will run after 2000 milliseconds, and then next SPF will run after 4000 milliseconds, etc., until it reaches the spf-wait value. The SPF interval remains at the spf-wait value until there are no more SPF runs scheduled in
that interval. After a full interval without any SPF runs, the SPF interval drops back to spf-initial-wait.

**Default**

no spf-wait

**Parameters**

- **spf-wait** — Specifies the maximum interval in seconds between two consecutive spf calculations.
  - **Values**:
    - 1 — 120
  - **Default**: 10

- **spf-initial-wait** — Specifies the initial SPF calculation delay in milliseconds after a topology change.
  - **Values**:
    - 10 — 100000
  - **Default**: 1000

- **spf-second-wait** — Specifies the hold time in milliseconds between the first and second SPF calculation.
  - **Values**:
    - 1 — 100000
  - **Default**: 1000

### level

**Syntax**

```
level level-number
```

**Context**

```
config>service>vpls <instance> b-vpls>spb
```

**Description**

This command creates the context to configure SPB Level 1 or Level 2 area attributes. This is IS-IS levels. Only Level 1 can be configured.

A Level 1 adjacency can be established only with other Level 1 B-VPLS. A Level 2 adjacency can be established only with other Level 2 B-VPLS. Currently there is no support for level 1 and level 2 in the same instance of SPB.

**Default**

level 1

**Parameters**

- **level-number** — The SPB level number.
  - **Values**: 1, 2

### bridge-priority

**Syntax**

```
bridge-priority value
```

**Context**

```
config>service>vpls <instance> b-vpls>spb>level level-number
```

**Description**

This command configures the four bit bridge priority for Shortest Path Bridging. This value is added to the 6 byte bridge identifier (which is the system-id) in the top four bits of a two byte field. Note the actual value will be bit shifted 12 bits left effective putting this in the high bits of the 16 bits added to system ID.

The bridge priority is important in choosing the Root Bridge for the single tree algorithm (lowest value = best). Bridge priority also factors into the tie breaker for SPF algorithms as described in the
SPB standard. The bridge-identifier (system-id) of the control B-VPLS determines the tiebreaker when the bridge-priorities are equal.

**Values**

- **0 — 15**

**Default**

- **8**

### ect-algorithm

**Syntax**

```
ект-algorithm name fid-range fid-range
```

**Context**

```
config>service>vpls <instance> b-vpls>spb>level level-number
```

**Description**

This command configures the ect-algorithm associated with a FID. Names are:

- low-path-id
- high-path-id

The algorithm for low-path-id chooses the path with the lowest metric and uses the sum of each Bridge-ID to break-ties (in this case preferring the lowest bridge identifiers).

The algorithm for high-path-id choose the path with the lowest metric and the sum of each Bridge-ID (after each one is modified by the algorithm mask) to break-ties (in this case preferring the highest bridge identifiers).

A Forwarding Identifier (FID) is an abstraction of the IEEE 802.1 SPB Base VID and represents the VLAN (B-VPLS) in IS-IS LSPs. B-VPLS services with the same FID share B-MACs and I-SIDs. (the SAP encapsulation VLAN tag may be set to the same value as the FID or to any other valid VLAN tag). One or more FIDs can be associated with an ECT-algorithm by using the FID range. User B-VPLS services may share the same FID as the control B-VPLS or use independent FIDs where each FID has an assigned ect-algorithm. B-VPLS services with i-vpls services must have an independent FID. B-VPLS services with only PBB Epipes may share FIDs with other B-VPLS services including the control B-VPLS service.

The ect-algorithm is associated with the FID and can only be changed only when there are no VPLS, SAPs or SDP bindings associated with the FID. The FID must be independent from the FID assigned to other services.

**Default**

- low-path-id

**Parameters**

- **name** — low-path-id, high-path-id
- **fid-range** — Range of Forwarding Identifier values.

**Values**

- **1 — 4095**

### forwarding-tree-topology

**Syntax**

```
forwarding-tree-topology unicast [st|spf]
```

**Context**

```
config>service>vpls <instance> b-vpls>spb>level level-number
```
**Description**
This command sets the unicast forwarding to follow the shortest path tree defined by the ECT algorithm shortest path forwarding (spf) or to follow a single tree (st). Shortest path trees make use of more link resources.

Multicast traffic is defaulted to follow the single tree topology. A single tree unicast would make Multicast and uncast follow the same path.

**Default**
spf

**lsp-pacing-interval**

**Syntax**
lsp-pacing-interval milliseconds
no lsp-pacing-interval

**Context**
config>service>vpls <instance> b-vpls>sap>spb>
config>service>vpls <instance> b-vpls>spoke-sdp>spb>

**Description**
This command configures the interval between SPB LSP PDUs sent from this interface. This command is valid only for interfaces on control B-VPLS.

To avoid bombarding adjacent neighbors with excessive data, pace the Link State Protocol Data Units (LSP’s). If a value of zero is configured, no LSP’s are sent from the interface.

The no form of the command reverts to the default value.

**Default**
100 — LSPs are sent in 100 millisecond intervals.

**Parameters**
milliseconds — The interval in milliseconds that SPB IS-IS LSP’s can be sent from the interface expressed as a decimal integer.

0 — 65535

**retransmit-interval**

**Syntax**
retransmit-interval seconds
no retransmit-interval

**Context**
config>service>vpls <instance> b-vpls>sap>spb>
config>service>vpls <instance> b-vpls>spoke-sdp>spb>

**Description**
This command configures the minimum time between LSP PDU retransmissions on a point-to-point interface. This command is valid only for interfaces on control B-VPLS.

The no form of the command reverts to the default value.

**Default**
100

**Parameters**
seconds — The interval in seconds that SPB IS-IS LSPs can be sent on the interface.

Values 1 — 65535

**metric**
Syntax  \texttt{metric value} \\
No metric \\
\textbf{Context} \texttt{config}\textgreater service\textgreater vpls \textless instance\textgreater b-vpls\textgreater sap\textgreater spb\textgreater level \\
\texttt{config}\textgreater service\textgreater vpls \textless instance\textgreater b-vpls\textgreater spoke-sdp\textgreater spb\textgreater level \\
\textbf{Description} This configures metric for this SPB interface SAP/spoke-sdp. This command is valid only for interfaces on control B-VPLS. \\
\textbf{Values} \begin{itemize} \\
\item 1 — 16,777,215 \\
\end{itemize} \\
\textbf{Default} 1000 \\

\textbf{hello-interval} \\
\textbf{Syntax} \texttt{hello-interval seconds} \\
\texttt{no hello-interval} \\
\textbf{Context} \texttt{config}\textgreater service\textgreater vpls \textless instance\textgreater b-vpls\textgreater sap\textgreater spb\textgreater level \\
\texttt{config}\textgreater service\textgreater vpls \textless instance\textgreater b-vpls\textgreater spoke-sdp\textgreater spb\textgreater level \\
\textbf{Description} This command configures the interval in seconds between hello messages issued on this interface at this level. This command is valid only for interfaces on control B-VPLS. \\
The no form of the command reverts to the default value. \\
\textbf{Default} \begin{itemize} \\
\item 3 — Hello interval default for the designated intersystem. \\
\item 9 — Hello interval default for non-designated intersystems. \\
\end{itemize} \\
\textbf{Parameters} \begin{itemize} \\
\item \texttt{seconds} — The hello interval in seconds expressed as a decimal integer. \\
\end{itemize} \\
\textbf{Values} \begin{itemize} \\
\item 1 — 20000 \\
\end{itemize} \\

\textbf{hello-multiplier} \\
\textbf{Syntax} \texttt{hello-multiplier multiplier} \\
\texttt{no hello-multiplier} \\
\textbf{Context} \texttt{config}\textgreater service\textgreater vpls \textless instance\textgreater b-vpls\textgreater sap\textgreater spb\textgreater level \\
\texttt{config}\textgreater service\textgreater vpls \textless instance\textgreater b-vpls\textgreater spoke-sdp\textgreater spb\textgreater level \\
\textbf{Description} This command configures the number of missing hello PDUs from a neighbor SPB declares the adjacency down. This command is valid only for interfaces on control B-VPLS. \\
The no form of the command reverts to the default value. \\
\textbf{Default} \begin{itemize} \\
\item 3 — SPB can miss up to 3 hello messages before declaring the adjacency down. \\
\end{itemize} \\
\textbf{Parameters} \begin{itemize} \\
\item \texttt{multiplier} — The multiplier for the hello interval expressed as a decimal integer. \\
\end{itemize} \\
\textbf{Values} \begin{itemize} \\
\item 2 — 100 \\
\end{itemize}
**mrp**

**Syntax**

```
mrp
```

**Context**

```
config>service>vpls
config>service>vpls>mesh-sdp
config>service>vpls>sap
config>service>vpls>spoke-sdp
```

**Description**

This command configures Multiple Registration Protocol (MRP) parameters. MRP is valid only under B-VPLS.

---

**attribute-table-size**

**Syntax**

```
[no] attribute-table-size value
```

**Context**

```
config>service>vpls>mrp
```

**Description**

This command controls the number of attributes accepted on a per B-VPLS basis. When the limit is reached, no new attributes will be registered.

If a new lower limit (smaller than the current number of attributes) from a local or dynamic I-VPLS is being provisioned, a CLI warning will be issued stating that the system is currently beyond the new limit. The value will be accepted, but any creation of new attributes will be blocked under the attribute count drops below the new limit; the software will then start enforcing the new limit.

**Default**

maximum number of attributes

**Parameters**

- `value` — [1-2048] for ESS-6/7/12 or SR-7/SR-12
  - [1-1023] for ESS1/SR1/7710

---

**attribute-table-high-wmark**

**Syntax**

```
[no] attribute-table-high-wmark high-water-mark
```

**Context**

```
config>service>vpls>mrp
```

**Description**

This command specifies the percentage filling level of the MMRP attribute table where logs and traps are sent.

**Default**

95%

**Parameters**

- `high-water-mark` — 1%-100%

---

**attribute-table-low-wmark**

**Syntax**

```
[no] attribute-table-low-wmark low-water-mark
```

---

7950 SR OS Services Guide Page 1041
VPLS Service Commands

**Context**  
config>service>vpls>mrp

**Description**  
This command specifies the MMRP attribute table low watermark as a percentage. When the percentage filling level of the MMRP attribute table drops below the configured value, the corresponding trap is cleared and/or a log entry is added.

**Default**  
90%

**Parameters**  
*low-water-mark — 1%-100%*

---

**flood-time**

**Syntax**  
*flood-time* flood-time  
no flood-time

**Context**  
config>service>vpls>mrp

**Description**  
This command configures the amount of time, in seconds, after a status change in the VPLS service during which traffic is flooded. Once that time expires, traffic will be delivered according to the MMRP registrations that exist in the VPLS. When “no flood-time” is executed, flooding behavior is disabled.

**Default**  
no flood-time

**Parameters**  
*flood-time — Specifies the MRP flood time, in seconds.  
*Values*  
3 — 600

---

**join-time**

**Syntax**  
[no] join-time *value*

**Context**  
config>service>vpls>sap>mrp  
config>service>vpls>spoke-sdp>mrp  
config>service>vpls>mesh-sdp>mrp

**Description**  
This command controls the interval between transmission opportunities that are applied to the Applicant state machine. An instance of this Join Period Timer is required on a per-Port, per-MRP Participant basis. For additional information, refer to IEEE 802.1ak-2007 section 10.7.4.1.

**Default**  
2

**Parameters**  
*value — [1-10] tenths of a second*

---

**leave-time**

**Syntax**  
[no] leave-time *value*

**Context**  
config>service>vpls>sap>mrp  
config>service>vpls>spoke-sdp>mrp
Description
This command controls the period of time that the Registrar state machine will wait in the leave state before transitioning to the MT state when it is removed. An instance of the timer is required for each state machine that is in the leave state. The Leave Period Timer is set to the value leave-time when it is started.

A registration is normally in “in” state where there is an MFIB entry and traffic is being forwarded. When a “leave all” is performed (periodically around every 10-15 seconds per SAP/SDP binding - see leave-all-time-below), a node sends a message to its peer indicating a leave all is occurring and puts all of its registrations in leave state.

The peer refreshes its registrations based on the leave all PDU it receives and sends a PDU back to the originating node with the state of all its declarations.

Refer to IEEE 802.1ak-2007 section 10.7.4.2.

Default
30

Parameters
value — [30-60] tenths of a second
VPLS Service Commands

**periodic-timer**

**Syntax**  
[no] periodic-timer

**Context**  
config>service>vpls>sap>mrp  
config>service>vpls>spoke-sdp>mrp  
config>service>vpls>mesh-sdp>mrp

**Description**  
This command enables or disables the Periodic Transmission Timer.

**Default**  
disabled

**send-flush-on-failure**

**Syntax**  
[no] send-flush-on-failure

**Context**  
config>service>vpls

**Description**  
This command enables sending out “flush-all-from-ME” messages to all LDP peers included in affected VPLS, in the event of physical port failures or “oper-down” events of individual SAPs. This feature provides an LDP-based mechanism for recovering a physical link failure in a dual-homed connection to a VPLS service. This method provides an alternative to RSTP solutions where dual homing redundancy and recovery, in the case of link failure, is resolved by RSTP running between a PE router and CE devices. If the endpoint is configured within the VPLS and send-flush-on-failure is enabled, flush-all-from-me messages will be sent out only when all spoke SDPs associated with the endpoint go down.

This feature cannot be enabled on management VPLS.

**Default**  
no send-flush-on-failure

**pbb**

**Syntax**  
pbb

**Context**  
config>service  
config>service>vpl  
config>service>epipe

**Description**  
This command configures global PBB parameters.

**mac-name**

**Syntax**  
mac-name name ieee-address  
no mac-name name

**Context**  
config>service>pbb
### Description
This command configures the MAC name for the MAC address. It associates an ASCII name with an IEEE MAC to improve the PBB Epipe configuration. It can also change the dest-BMAC in one place instead of 1000s of Epipe.

### Parameters
- **name** — Specifies the MAC name up to 32 characters in length.
- **ieee-address** — The MAC address assigned to the MAC name. The value should be input in either a `xx:xx:xx:xx:xx:xx` or `xx-xx-xx-xx-xx-xx` format.

### source-bmac

**Syntax**
```
source-bmac ieee-address
no source-bmac
```

**Context**
```
config>service>pbb
```

**Description**
This command configures the source B-VPLS MAC address to use with PBB and provisions a chassis level source BMAC.

**Parameters**
- **ieee-address** — The MAC address assigned to the BMAC. The value should be input in either a `xx:xx:xx:xx:xx:xx` or `xx-xx-xx-xx-xx-xx` format.

### force-qtag-forwarding

**Syntax**
```
[no] force-qtag-forwarding
```

**Context**
```
config>service>vpls ivpls>pbb
```

**Description**
This command forces the addition of a IEEE 802.1q tag after the Customer MAC (CMAC) address when the PBB header is built as it egresses a related BVPLS. It is used to preserve the dot1q and DE bits from the customer domain when the service delimiting qtags are stripped as the packet is ingressing a PBB Epipe or an IVPLS. The VLAN value of the service delimiting QTAG, if one exists, is used for the corresponding inserted dot1q field. If a service delimiting QTAG does not exist, then the value of zero is used for all the inserted QTAG bits. The no form of this command sets default behavior.

The no form of this command disables the command.

### source-bmac

**Syntax**
```
source-bmac ieee-address
```

**Context**
```
config>service>vpls bvpls>pbb
```

**Description**
This command configures the base source BMAC for the B-VPLS. The first 32 bits must be the same with what is configured in the MC-LAG peer. If not configured here, it will inherit the chassis level BMAC configured under the new PBB object added in the previous section. If the use-sap-bmac command is on, the value of the last 16 bits (lsb) of the source BMAC must be part of the reserved-
source-bmac-lsb configured at chassis level, under service PBB component. If that is not the case, the command will fail.

use-sap-bmac

Syntax  [no] use-sap-bmac
Context  config>service>vpls bvpls>pbb
Description  This command enables on a per BVPLS basis the use of source BMACs allocated to multi-homed SAPs (assigned to an MC-LAG) in the related IVPLS or Epipe service. The command will fail if the value of the source-bmac assigned to the BVPLS is the hardware (chassis) BMAC. In other words, the source-bmac must be a configured one.
Default  no use-sap-bmac

mac-notification

Syntax  mac-notification
Context  config>service>vpls bvpls
Description  This command controls the settings for the MAC notification message.

The mac-notification message must be generated under the following events:

1. When enabled in the BVPLS using no shutdown, a MAC notification will be sent for every active MC-LAG link. The following 3 cases assume no shutdown in the BVPLS.
2. Whenever a related MC-LAG link becomes active (related MC-LAG link = has at least 1 SAP associated with the BVPLS) if the MC-LAG peering is initialized and the PE peers are synchronized.
3. 1st SAP on an active MC-LAG is associated (via IVPLS/Epipe) with the BVPLS
4. The link between IVPLS/Epipe and BVPLS is configured and there are I-SAPs configured on an active MC-LAG link.

The MAC notification is not sent for the following events:

1. Change of source-bmac or source-bmac-lsb
2. On changes of use-sap-bmac parameter
3. If MC-LAG peering is not (initialized and in sync).

interval

Syntax  [no] interval value
Context  config>service>vpls>pbb>mac-notification
Description  This command controls the frequency of subsequent MAC notification messages.
**VPLS Service Commands**

**Default**
Inherits the chassis level configuration from config>service>mac-notification

**Parameters**

- **value** — Specifies the frequency of subsequent MAC notification messages.

  **Values**
  - 100 ms – 10 sec, in increments of 100 ms up to 1 sec and then in increments of 1 second up to 10 sec.

---

**renotify**

**Syntax**
renotify value
no renotify

**Context**
config>service>vpls>pbb>mac-notification

**Description**
This command controls the periodic interval at which sets of MAC notification messages are sent. At each expiration of the renotify timer, a new burst of notification messages is sent, specifically <count> frames at <interval> deci-seconds.

**Default**
no renotify

**Parameters**

- **value** — Specifies the time interval between re-notification in seconds.

  **Values**
  - 240—840 seconds

---

**count**

**Syntax**
[no] count value

**Context**
config>service>vpls>pbb>mac-notification

**Description**
This command configures how often MAC notification messages are sent.

**Parameters**

- **value** — Specifies, in seconds, how often MAC notification messages are sent.

  **Values**
  - 1—10

  **Default**
  Inherits the chassis level configuration from config>service>mac-notification

---

**shutdown**

**Syntax**
[no] shutdown

**Context**
config>service>vpls bvpls

**Description**
This command disables the sending of the notification message in the BVPLS domain.

**Default**
shutdown

---

**backbone-vpls**
Backbone-VPLS

Syntax: `backbone-vpls service-id [isid isid]
no backbone-vpls`

Context: `config>service>vpls>pbb`

Description: This command configures B-VPLS service associated with the I-VPLS.

Parameters:
- `service-id` — Specifies the service ID.
  - Values: 1..2147483648
- `isid` — Specifies the ISID.
  - Values: 0..16777215

IGMP snooping

Syntax: `igmp-snooping`

Context:
- `config>service>vpls>pbb>backbone-vpls`
- `config>service>vpls>pbb>backbone-vpls>sap`
- `config>service>vpls>pbb>backbone-vpls>sdp`

Description: This command configures IGMP snooping attributes for I-VPLS.

MRouter-dest

Syntax: `[no] mrouter-dest mac-name`

Context: `config>service>vpls>pbb>backbone-vpls`

Description: This command configures the destination BMAC address name to be used in the related backbone VPLS to reach a specific IGMP snooping MRouter. The name is associated at system level with the MAC address using the command “config>service>pbb>mac-name name ieee-address”.

Parameters:
- `mac-name` — Specifies the MAC name.
  - Values: 32 chars max

SAP

Syntax: `[no] sap sap-id`

Context: `config>service>vpls>pbb>backbone-vpls`

Description: This command configures attributes of a SAP on the B-VPLS service.

MRouter-port
Syntax  [no] mrouter-port

Context  config>service>vpls>pbb>backbone-vpls>sap>igmp-snooping
 config>service>vpls>pbb>backbone-vpls>sdp>igmp-snooping

Description  This command specifies whether a multicast router is attached behind this SAP.

Configuring a SAP as an mrouter-port will have a double effect. Firstly, all multicast traffic received on another SAP will be copied to this SAP. Secondly, IGMP reports generated by the system as a result of someone joining or leaving a multicast group, will be sent to this SAP or SDP.

If two multicast routers exist in the network, one of them will become the active querier. While the other multicast router (non-querier) stops sending IGMP queries, it should still receive reports to keep its multicast trees up to date. To support this, the mrouter-port should be enabled on all SAPs connecting to a multicast router.

Note that the IGMP version to be used for the reports (v1, v2 or v3) can only be determined after an initial query has been received. Until such time no reports are sent on the SAP, even if mrouter-port is enabled.

If the send-queries command is enabled on this SAP, the mrouter-port parameter cannot be set.

Default  no mrouter-port

sdp

Syntax  [no] sdp sdپ:vc-id

Context  config>service>vpls>pbb>backbone-vpls

Description  This command configures attributes of a SDP binding on the B-VPLS service.

Parameters  sdp-id — Specifies the SDP ID.

Values  1..17407

vc-id — Specifies the VC ID.

Values  1..4294967295

stp

Syntax  [no] stp

Context  config>service>Vpls>pbb>backbone-vpls

Description  This command enables or disable STP through B-VPLS service.

force-qtag-forwarding

Syntax  [no] force-qtag-forwarding
VPLS Service Commands

**Context**

config>service>vpls ivpls>pbb
config>service>epipe>pbb

**Description**

This command forces the addition of a IEEE 802.1q tag after the Customer MAC (CMAC) addresses when the PBB header is built, as it egresses a related BVPLS.

It is used to preserve the dot1q and DE bits from the customer domain when the service delimiting qtags are stripped when the packet is ingressing a PBB Epipe or an IVPLS. The VLAN value of the service delimiting QTAG if one exists is used for the corresponding inserted dot1q field. If a service delimiting QTAG does not exist, then the value of zero is used for all the inserted QTAG bits.

The **no** form of this command sets default behavior.

**Default**
disabled

**mrp-policy**

**Syntax**

[no] mrp-policy

**Context**

config>service>vpls>sap>mrp
config>service>vpls>spoke-sdp>mrp
config>service>vpls>mesh-sdp>mrp

**Description**

This command instructs MMRP to use the mrp-policy defined in the command to control which group BMAC attributes will be declares and registered on the egress SAP/Mesh-SDP/Spoke-SDP. The Group BMACs will be derived from the ISIDs using the procedure used in the PBB solution. The Group MAC = standard OUI with the last 24 bits being the ISID value. If the policy-name refers to a non-existing mrp-policy the command should return error. Changes to a mrp-policy are allowed and applied to the SAP/SDPs under which the policy is referenced.

**Default**
no mrp-policy

**send-bvpls-flush**

**Syntax**

[no] send-bvpls-flush {[all-from-me] | [all-but-mine]}

**Context**

config>service>vpls

**Description**

This command configures the BVPLS flush. If B-SDPs are used and MAC notification mechanism is turned on in the related BVPLS (MPLS use case), it makes sense to turn off the T-LDP MAC Flush.

**mac-notification**

**Syntax**

mac-notification

**Context**

config>service>pbb

**Description**

This command controls the settings for the MAC notification messages.
interval

Syntax  
\[\text{[no]} \text{ interval } \text{value}\]

Context  
config>service>pbb>mac-notification

Description  
This command controls the frequency of subsequent MAC notification messages.

Default  
100 ms

Parameters  
value — Specifies the frequency of subsequent MAC notification messages.

Values  
100 ms – 10 sec, in increments of 100 ms up to 1 sec and then in increments of 1 second up to 10 sec.

count

Syntax  
\[\text{[no]} \text{ count } \text{value}\]

Context  
config>service>pbb>mac-notification

Description  
This command configures how often MAC notification messages are sent.

Parameters  
value — Specifies, in seconds, how often MAC notification messages are sent.

Values  
1-10

Default  
3

epipe

Syntax  
epipe service-id customer customer-id [vpn vpn-id] [vc-switching] [create]
epipe service-id
no epipe service-id

Context  
config>service

Description  
This command configures an Epipe service instance. This command is used to configure a point-to-point epipe service. An Epipe connects two endpoints defined as Service Access Points (SAPs). Both SAPs may be defined in one

No MAC learning or filtering is provided on an Epipe.

When a service is created, the customer keyword and customer-id must be specified and associates the service with a customer. The customer-id must already exist having been created using the customer command in the service context. Once a service has been created with a customer association, it is not possible to edit the customer association. The service must be deleted and recreated with a new customer association.

Once a service is created, the use of the customer customer-id is optional for navigating into the service configuration context. Attempting to edit a service with the incorrect customer-id specified will result in an error.
By default, no epipe services exist until they are explicitly created with this command. The `no` form of this command deletes the epipe service instance with the specified `service-id`. The service cannot be deleted until the service has been shutdown.

`service-id` — The unique service identification number identifying the service in the service domain. This ID must be unique to this service and may not be used for any other service of any type. The `service-id` must be the same number used for every service on which this service is defined.

**Values**

1 — 2147483648

`customer customer-id` — Specifies the customer ID number to be associated with the service. This parameter is required on service creation and optional for service editing or deleting.

**Values**

1 — 2147483647

`create` — Keyword used to create the service instance. The `create` keyword requirement can be enabled/disabled in the `environment>create` context.
Internet Enhanced Service

In This Chapter

This chapter provides information about Internet Enhanced Service (IES), process overview, and implementation notes.

Topics in this chapter include:

- IES Service Overview on page 1054
- IES Features on page 1055
  - IP Interfaces on page 1055
    - QoS Policy Propagation Using BGP (QPPB) on page 1056
  - Object Grouping and State Monitoring on page 1067
  - Filter Policies on page 1079
- Configuring an IES Service with CLI on page 1081
- Basic Configuration on page 1082
- Common Configuration Tasks on page 1083
- Service Management Tasks on page 1088
IES Service Overview

Internet Enhanced Service (IES) is a routed connectivity service where the subscriber communicates with an IP router interface to send and receive Internet traffic. An IES has one or more logical IP routing interfaces each with a SAP which acts as the access point to the subscriber’s network. IES allows customer-facing IP interfaces to participate in the same routing instance used for service network core routing connectivity. IES services require that the IP addressing scheme used by the subscriber be unique between other provider addressing schemes and potentially the entire Internet.

While IES is part of the routing domain, the usable IP address space may be limited. This allows a portion of the service provider address space to be reserved for service IP provisioning, and be administered by a separate but subordinate address authority.

IP interfaces defined within the context of an IES service must have a SAP associated as the uplink access point to the subscriber network. Multiple IES services are created to segregate subscriber-owned IP interfaces.

Figure 140: Internet Enhanced Service
IES Features

This section describes various of the general service features and any special capabilities or considerations as they relate to IES services.

IP Interfaces

IES customer IP interfaces can be configured with most of the same options found on the core IP interfaces. The advanced configuration options supported are:

- QoS Policy Propagation Using BGP (QPPB) on page 1056
- ICMP Options

Configuration options found on core IP interfaces not supported on IES IP interfaces are:

- MPLS forwarding
- NTP broadcast receipt
QoS Policy Propagation Using BGP (QPPB)

This section discusses QPPB as it applies to VPRN, IES, and router interfaces. Refer to the Internet Enhanced Service section on page 1053 and the IP Router Configuration section in the 7x50 OS Router Configuration Guide.

QoS policy propagation using BGP (QPPB) is a feature that allows a route to be installed in the routing table with a forwarding-class and priority so that packets matching the route can receive the associated QoS. The forwarding-class and priority associated with a BGP route are set using BGP import route policies. In the industry this feature is called QPPB, and even though the feature name refers to BGP specifically. On SR routers, QPPB is supported for BGP (IPv4, IPv6, VPN-IPv4, VPN-IPv6), RIP and static routes.

While SAP ingress and network QoS policies can achieve the same end result as QPPB, assigning a packet arriving on a particular IP interface to a specific forwarding-class and priority/profile based on the source IP address or destination IP address of the packet—the effort involved in creating the QoS policies, keeping them up-to-date, and applying them across many nodes is much greater than with QPPB. In a typical application of QPPB, a BGP route is advertised with a BGP community attribute that conveys a particular QoS. Routers that receive the advertisement accept the route into their routing table and set the forwarding-class and priority of the route from the community attribute.

QPPB Applications

There are two typical applications of QPPB:

1. Coordination of QoS policies between different administrative domains.
2. Traffic differentiation within a single domain, based on route characteristics.

Inter-AS Coordination of QoS Policies

The operator of an administrative domain A can use QPPB to signal to a peer administrative domain B that traffic sent to certain prefixes advertised by domain A should receive a particular QoS treatment in domain B. More specifically, an ASBR of domain A can advertise a prefix XYZ to domain B and include a BGP community attribute with the route. The community value implies a particular QoS treatment, as agreed by the two domains (in their peering agreement or service level agreement, for example). When the ASBR and other routers in domain B accept and install the route for XYZ into their routing table, they apply a QoS policy on selected interfaces that classifies traffic towards network XYZ into the QoS class implied by the BGP community value.

QPPB may also be used to request that traffic sourced from certain networks receive appropriate QoS handling in downstream nodes that may span different administrative domains. This can be
achieved by advertising the source prefix with a BGP community, as discussed above. However, in this case other approaches are equally valid, such as marking the DSCP or other CoS fields based on source IP address so that downstream domains can take action based on a common understanding of the QoS treatment implied by different DSCP values.

In the above examples, coordination of QoS policies using QPPB could be between a business customer and its IP VPN service provider, or between one service provider and another.

**Traffic Differentiation Based on Route Characteristics**

There may be times when a network operator wants to provide differentiated service to certain traffic flows within its network, and these traffic flows can be identified with known routes. For example, the operator of an ISP network may want to give priority to traffic originating in a particular ASN (the ASN of a content provider offering over-the-top services to the ISP’s customers), following a certain AS_PATH, or destined for a particular next-hop (remaining on-net vs. off-net).

Figure 141 shows an example of an ISP that has an agreement with the content provider managing AS300 to provide traffic sourced and terminating within AS300 with differentiated service appropriate to the content being transported. In this example we presume that ASBR1 and ASBR2 mark the DSCP of packets terminating and sourced, respectively, in AS300 so that other nodes within the ISP’s network do not need to rely on QPPB to determine the correct forwarding-class to use for the traffic. Note however, that the DSCP or other COS markings could be left unchanged in the ISP’s network and QPPB used on every node.
Figure 141: Use of QPPB to Differentiate Traffic in an ISP Network
QPPB

There are two main aspects of the QPPB feature:

- The ability to associate a forwarding-class and priority with certain routes in the routing table.
- The ability to classify an IP packet arriving on a particular IP interface to the forwarding-class and priority associated with the route that best matches the packet.

Associating an FC and Priority with a Route

This feature uses a command in the route-policy hierarchy to set the forwarding class and optionally the priority associated with routes accepted by a route-policy entry. The command has the following structure:

```
fc fc-name [priority {low | high}]
```

The use of this command is illustrated by the following example:

```
config>router>policy-options
begin
  community gold members 300:100
  policy-statement qppb_policy
  entry 10
  from
  protocol bgp
  community gold
  exit
  action accept
  fc h1 priority high
  exit
  exit
exit
commit
```

The `fc` command is supported with all existing from and to match conditions in a route policy entry and with any action other than reject, it is supported with next-entry, next-policy and accept actions. If a next-entry or next-policy action results in multiple matching entries then the last entry with a QPPB action determines the forwarding class and priority.

A route policy that includes the `fc` command in one or more entries can be used in any import or export policy but the `fc` command has no effect except in the following types of policies:

- VRF import policies:
  → `config>service>vprn>vrf-import`
IES Features

- **BGP import policies:**
  - `config>router>bgp>import`
  - `config>router>bgp>group>import`
  - `config>router>bgp>group>neighbor>import`
  - `config>service>vprn>bgp>import`
  - `config>service>vprn>bgp>group>import`
  - `config>service>vprn>bgp>group>neighbor>import`

- **RIP import policies:**
  - `config>router>rip>import`
  - `config>router>rip>group>import`
  - `config>router>rip>group>neighbor>import`
  - `config>service>vprn>rip>import`
  - `config>service>vprn>rip>group>import`
  - `config>service>vprn>rip>group>neighbor>import`

As evident from above, QPPB route policies support routes learned from RIP and BGP neighbors of a VPRN as well as for routes learned from RIP and BGP neighbors of the base/global routing instance.

QPPB is supported for BGP routes belonging to any of the address families listed below:

- IPv4 (AFI=1, SAFI=1)
- IPv6 (AFI=2, SAFI=1)
- VPN-IPv4 (AFI=1, SAFI=128)
- VPN-IPv6 (AFI=2, SAFI=128)

Note that a VPN-IP route may match both a VRF import policy entry and a BGP import policy entry (if vpn-apply-import is configured in the base router BGP instance). In this case the VRF import policy is applied first and then the BGP import policy, so the QPPB QoS is based on the BGP import policy entry.

This feature also introduces the ability to associate a forwarding-class and optionally priority with IPv4 and IPv6 static routes. This is achieved using the following modified versions of the static-route commands:

- `static-route {ip-prefix/prefix-length|ip-prefix netmask} [fc fc-name [priority {low | high}]]` next-hop `ip-int-name|ip-address`
- `static-route {ip-prefix/prefix-length|ip-prefix netmask} [fc fc-name [priority {low | high}]]` indirect `ip-address`
Priority is optional when specifying the forwarding class of a static route, but once configured it can only be deleted and returned to unspecified by deleting the entire static route.

---

**Displaying QoS Information Associated with Routes**

The following commands are enhanced to show the forwarding-class and priority associated with the displayed routes:

- `show router route-table`
- `show router fib`
- `show router bgp routes`
- `show router rip database`
- `show router static-route`

This feature uses a `qos` keyword to the `show router route-table` command. When this option is specified the output includes an additional line per route entry that displays the forwarding class and priority of the route. If a route has no fc and priority information then the third line is blank. The following CLI shows an example:

```
show router route-table [family] [ip-prefix[/prefix-length]] [longer | exact] [protocol protocol-name] qos
```

An example output of this command is shown below:

```
A:Dut-A# show router route-table 10.1.5.0/24 qos
===============================================================================
Route Table (Router: Base)
===============================================================================
Dest Prefix                                   Type    Proto    Age         Pref   Next Hop[Interface Name]         Metric   QoS
-------------------------------------------------------------------------------
10.1.5.0/24                                   Remote  BGP      15h32m52s   0     PE1_to_PE2                                                   0     h1, high
-------------------------------------------------------------------------------
No. of Routes: 1
===============================================================================
A:Dut-A#
```
Enabling QPPB on an IP Interface

To enable QoS classification of ingress IP packets on an interface based on the QoS information associated with the routes that best match the packets the `qos-route-lookup` command is necessary in the configuration of the IP interface. The `qos-route-lookup` command has parameters to indicate whether the QoS result is based on lookup of the source or destination IP address in every packet. There are separate `qos-route-lookup` commands for the IPv4 and IPv6 packets on an interface, which allows QPPB to enabled for IPv4 only, IPv6 only, or both IPv4 and IPv6. Note however, current QPPB based on a source IP address is not supported for IPv6 packets nor is it supported for ingress subscriber management traffic on a group interface.

The `qos-route-lookup` command is supported on the following types of IP interfaces:

- base router network interfaces (config>router>interface)
- VPRN SAP and spoke SDP interfaces (config>service>vprn>interface)
- IES SAP and spoke SDP interfaces (config>service>ies>interface)

When the `qos-route-lookup` command with the destination parameter is applied to an IP interface and the destination address of an incoming IP packet matches a route with QoS information the packet is classified to the fc and priority associated with that route, overriding the fc and priority/profile determined from the sap-ingress or network qos policy associated with the IP interface (see section 5.7 for further details). If the destination address of the incoming packet matches a route with no QoS information the fc and priority of the packet remain as determined by the sap-ingress or network qos policy.

Similarly, when the `qos-route-lookup` command with the source parameter is applied to an IP interface and the source address of an incoming IP packet matches a route with QoS information the packet is classified to the fc and priority associated with that route, overriding the fc and priority/profile determined from the sap-ingress or network qos policy associated with the IP interface. If the source address of the incoming packet matches a route with no QoS information the fc and priority of the packet remain as determined by the sap-ingress or network qos policy.

Currently, QPPB is not supported for ingress MPLS traffic on network interfaces or on CsC PE’-CE’ interfaces (config>service>vprn>nw-if).
QPPB When Next-Hops are Resolved by QPPB Routes

In some circumstances (IP VPN inter-AS model C, Carrier Supporting Carrier, indirect static routes, etc.) an IPv4 or IPv6 packet may arrive on a QPPB-enabled interface and match a route A1 whose next-hop N1 is resolved by a route A2 with next-hop N2 and perhaps N2 is resolved by a route A3 with next-hop N3, etc. In release 9.0 the QPPB result is based only on the forwarding-class and priority of route A1. If A1 does not have a forwarding-class and priority association then the QoS classification is not based on QPPB, even if routes A2, A3, etc. have forwarding-class and priority associations.

QPPB and Multiple Paths to a Destination

When ECMP is enabled some routes may have multiple equal-cost next-hops in the forwarding table. When an IP packet matches such a route the next-hop selection is typically based on a hash algorithm that tries to load balance traffic across all the next-hops while keeping all packets of a given flow on the same path. The QPPB configuration model described in Associating an FC and Priority with a Route on page 1059 allows different QoS information to be associated with the different ECMP next-hops of a route. The forwarding-class and priority of a packet matching an ECMP route is based on the particular next-hop used to forward the packet.

When BGP fast reroute [1] is enabled some BGP routes may have a backup next-hop in the forwarding table in addition to the one or more primary next-hops representing the equal-cost best paths allowed by the ECMP/multipath configuration. When an IP packet matches such a route a reachable primary next-hop is selected (based on the hash result) but if all the primary next-hops are unreachable then the backup next-hop is used. The QPPB configuration model described in Associating an FC and Priority with a Route on page 1059 allows the forwarding-class and priority associated with the backup path to be different from the QoS characteristics of the equal-cost best paths. The forwarding class and priority of a packet forwarded on the backup path is based on the fc and priority of the backup route.

QPPB and Policy-Based Routing

When an IPv4 or IPv6 packet with destination address X arrives on an interface with both QPPB and policy-based-routing enabled:

- There is no QPPB classification if the IP filter action redirects the packet to a directly connected interface, even if X is matched by a route with a forwarding-class and priority
- QPPB classification is based on the forwarding-class and priority of the route matching IP address Y if the IP filter action redirects the packet to the indirect next-hop IP address Y, even if X is matched by a route with a forwarding-class and priority
QPPB and GRT Lookup

Source-address based QPPB is not supported on any SAP or spoke SDP interface of a VPRN configured with the `grt-lookup` command.

QPPB Interaction with SAP Ingress QoS Policy

When QPPB is enabled on a SAP IP interface the forwarding class of a packet may change from `fc1`, the original `fc` determined by the SAP ingress QoS policy to `fc2`, the new `fc` determined by QPPB. In the ingress datapath SAP ingress QoS policies are applied in the first P chip and route lookup/QPPB occurs in the second P chip. This has the implications listed below:

- Ingress remarking (based on profile state) is always based on the original `fc` (`fc1`) and subclass (if defined).
- The profile state of a SAP ingress packet that matches a QPPB route depends on the configuration of `fc2` only. If the de-1-out-profile flag is enabled in `fc2` and `fc2` is not mapped to a priority mode queue then the packet will be marked out of profile if its DE bit = 1. If the profile state of `fc2` is explicitly configured (in or out) and `fc2` is not mapped to a priority mode queue then the packet is assigned this profile state. In both cases there is no consideration of whether or not `fc1` was mapped to a priority mode queue.
- The priority of a SAP ingress packet that matches a QPPB route depends on several factors. If the de-1-out-profile flag is enabled in `fc2` and the DE bit is set in the packet then priority will be low regardless of the QPPB priority or `fc2` mapping to profile mode queue, priority mode queue or policer. If `fc2` is associated with a profile mode queue then the packet priority will be based on the explicitly configured profile state of `fc2` (in profile = high, out profile = low, undefined = high), regardless of the QPPB priority or `fc1` configuration. If `fc2` is associated with a priority mode queue or policer then the packet priority will be based on QPPB (unless DE=1), but if no priority information is associated with the route then the packet priority will be based on the configuration of `fc1` (if `fc1` mapped to a priority mode queue then it is based on DSCP/IP prec/802.1p and if `fc1` mapped to a profile mode queue then it is based on the profile state of `fc1`).

Table 16 summarizes these interactions.
<table>
<thead>
<tr>
<th>Original FC object mapping</th>
<th>New FC object mapping</th>
<th>Profile</th>
<th>Priority (drop preference)</th>
<th>DE=1 override</th>
<th>In/out of profile marking</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile mode queue</td>
<td>Profile mode queue</td>
<td>From new base FC unless overridden by DE=1</td>
<td>From QPPB, unless packet is marked in or out of profile in which case follows profile. Default is high priority</td>
<td>From new base FC</td>
<td>From original FC and sub-class</td>
</tr>
<tr>
<td>Priority mode queue</td>
<td>Priority mode queue</td>
<td>Ignored</td>
<td>If DE=1 override then low otherwise from QPPB. If no DEI or QPPB overrides then from original dot1p/exp/DSCP mapping or policy default.</td>
<td>From new base FC</td>
<td>From original FC and sub-class</td>
</tr>
<tr>
<td>Policer</td>
<td>Policer</td>
<td>From new base FC unless overridden by DE=1</td>
<td>If DE=1 override then low otherwise from QPPB. If no DEI or QPPB overrides then from original dot1p/exp/DSCP mapping or policy default.</td>
<td>From new base FC</td>
<td>From original FC and sub-class</td>
</tr>
<tr>
<td>Priority mode queue</td>
<td>Policer</td>
<td>From new base FC unless overridden by DE=1</td>
<td>If DE=1 override then low otherwise from QPPB. If no DEI or QPPB overrides then from original dot1p/exp/DSCP mapping or policy default.</td>
<td>From new base FC</td>
<td>From original FC and sub-class</td>
</tr>
<tr>
<td>Policer</td>
<td>Priority mode queue</td>
<td>Ignored</td>
<td>If DE=1 override then low otherwise from QPPB. If no DEI or QPPB overrides then from original dot1p/exp/DSCP mapping or policy default.</td>
<td>From new base FC</td>
<td>From original FC and sub-class</td>
</tr>
<tr>
<td>Original FC object mapping</td>
<td>New FC object mapping</td>
<td>Profile</td>
<td>Priority (drop preference)</td>
<td>DE=1 override</td>
<td>In/out of profile marking</td>
</tr>
<tr>
<td>---------------------------</td>
<td>----------------------</td>
<td>--------------------------</td>
<td>-------------------------------------------------------------------------------------------</td>
<td>-------------------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>Profile mode queue</td>
<td>Priority mode queue</td>
<td>Ignored</td>
<td>If DE=1 override then low otherwise from QPPB. If no DEI or QPPB overrides then follows original FC’s profile mode rules.</td>
<td>From new base FC</td>
<td>From original FC and sub-class</td>
</tr>
<tr>
<td>Priority mode queue</td>
<td>Priority mode queue</td>
<td>From new base FC unless overridden by DE=1</td>
<td>From QPPB, unless packet is marked in or out of profile in which case follows profile. Default is high priority</td>
<td>From new base FC</td>
<td>From original FC and sub-class</td>
</tr>
<tr>
<td>Profile mode queue</td>
<td>Policer</td>
<td>From new base FC unless overridden by DE=1</td>
<td>If DE=1 override then low otherwise from QPPB. If no DEI or QPPB overrides then follows original FC’s profile mode rules.</td>
<td>From new base FC</td>
<td>From original FC and sub-class</td>
</tr>
<tr>
<td>Policer</td>
<td>Profile mode queue</td>
<td>From new base FC unless overridden by DE=1</td>
<td>From QPPB, unless packet is marked in or out of profile in which case follows profile. Default is high priority</td>
<td>From new base FC</td>
<td>From original FC and sub-class</td>
</tr>
</tbody>
</table>
Object Grouping and State Monitoring

This feature introduces a generic operational group object which associates different service endpoints (pseudowires and SAPs) located in the same or in different service instances. The operational group status is derived from the status of the individual components using certain rules specific to the application using the concept. A number of other service entities, the monitoring objects, can be configured to monitor the operational group status and to perform certain actions as a result of status transitions. For example, if the operational group goes down, the monitoring objects will be brought down.

IES IP Interface Applicability

This concept is used by an IPv4 IES interface to affect the operational state of the IP interface monitoring the operational group. Individual SAP and spoke SDPs are supported as monitoring objects.

The following rules apply:

- An object can only belong to one group at a time.
- An object that is part of a group cannot monitor the status of a group.
- An object that monitors the status of a group cannot be part of a group.
- An operational group may contain any combination of member types: SAP or Spoke-SDPs.
- An operational group may contain members from different VPLS service instances.
- Objects from different services may monitor the oper-group.

There are two steps involved in enabling the functionality:

1. Identify a set of objects whose forwarding state should be considered as a whole group then group them under an operational group using the `oper-group` command.
4. Associate the IP interface to the oper-group using the `monitor-group` command.

The status of the operational group (oper-group) is dictated by the status of one or more members according to the following rules:

- The oper-group goes down if all the objects in the oper-group go down. The oper-group comes up if at least one component is up.
• An object in the group is considered down if it is not forwarding traffic in at least one direction. That could be because the operational state is down or the direction is blocked through some validation mechanism.

• If a group is configured but no members are specified yet then its status is considered up.

• As soon as the first object is configured the status of the operational group is dictated by the status of the provisioned member(s).

The following configuration shows the oper-group g1, the VPLS SAP that is mapped to it and the IP interfaces in IES service 2001 monitoring the oper-group g1. This is example uses an R-VPLS context. The VPLS instance includes the **allow-ip-int-binding** and the **service-name v1**. The IES interface links to the VPLS using the **vpls v1** option. All commands are under the configuration service hierarchy.

To further explain the configuration. Oper-group g1 has a single SAP (1/1/1:2001) mapped to it and the IP interfaces in the IES service 2001 will derive its state from the state of oper-group g1.

```plaintext
oper-group g1 create
vpls 1 customer 1 create
  allow-ip-int-binding
  stp
  shutdown
  exit
  service-name "v1"
  sap 1/1/1:2001 create
  oper-group g1
  eth-cfm
    mep domain 1 association 1 direction down
    ccm-enable
    no shutdown
    exit
    exit
  sap 1/1/2:2001 create
  exit
  sap 1/1/3:2001 create
  exit
  no shutdown

ies 2001 customer 1 create
  interface "i2001" create
    address 21.1.1.1/24
    monitor-oper-group "g1"
    vpls "v1"
  exit
  no shutdown
  exit
```
SAPs

Encapsulations

The following SAP encapsulations are supported on the 7950 IES services:

- Ethernet null
- Ethernet dot1q
Pseudowire SAPs

This feature allows customers of an IES or VPRN service and connected to an Ethernet SAP on an Access PE to be backhauled through an Ethernet aggregation network using MPLS pseudowires terminating directly on a Layer 3 PE hosting the IES or VPRN service. This service is different from VLL Spoke-SDP termination on an IES or VPRN because, in this case, access QoS policies can be applied directly at a centralized PE hosting the IES or VPRN instance. This feature uses the same concepts of pseudowire ports and pseudowire SAPs that are used for ESM over MPLS pseudowires, described in the SR OS Triple Play Service Delivery Architecture user guide.

The MPLS pseudowire originates from the first hop aggregation PE (referred to as access PE) upstream of the Access-Node (or directly from a multi-service AN), and terminates on the Layer 3 PE. Multiple customers from a given access-port on the Access-PE can be backhauled over a single MPLS pseudowire towards the Layer 3 PE. This capability allows the network to scale and does not require an MPLS pseudowire per customer between the Access-PE and the Layer 3 PE. The access-port on the Access-PE can be dot1q, q-in-q or NULL encapsulated. The Layer 3 PE terminates the MPLS pseudowire, decapsulates the received frames, and provides access QoS functions including HQoS, without requiring an internal or external loopback. Each MPLS pseudowire is represented on the BNG as a “PW-port” for which SAPs are created. These SAPs are termed “PW SAPs”, and must be statically configured on IES or VPRN interfaces (unlike the ESM case where a capture SAP can be configured). The underlying Ethernet port must be in hybrid mode. Pseudowire SAPs are supported on Ethernet MDAs and on the HSMDAv2.

Figure 142 illustrates the architecture of an aggregation network that uses pseudowire SAPs.
Encapsulation

The packet is encapsulated on an Ethernet pseudowire, which is associated with a pseudowire port on the Layer 3 PE, and a spoke-sdp on the access PE. The optional control word is not supported. The SDP could use an LDP, RSVP LSP, or LDP over RSVP tunnel. Hash labels are not supported. The SDP is bound to a port or a LAG, although note that shaping vports for pseudowire ports on LAGs in distributed mode is not supported. If an SDP is rerouted, then the corresponding pseudowire ports are brought operationally down. Pseudowire ports are associated with an SDP by configuration.
Pseudowire SAP Configuration

The following steps are required at the access PE:

1. Configure an Epipe VLL service
2. Configure a NULL, 1q or q-in-q SAP on the Epipe service.

The following steps are used to configure a pseudowire SAP on the IES or VPRN service at the Layer 3 PE:

1. Define a pseudowire port
   ```
   pw-port 1 create
   exit
   pw-port 2 create
   exit
   ```

2. Bind a physical port or LAG, in hybrid mode, with the pseudowire port.
   ```
   service
   customer 1 create
   multi-service-site "abc" create
   assignment port pw-1
   egress
   policer-control-policy "abc"
   exit
   exit
   description "Default customer"
   exit
   sdp 1 mpls create
   far-end 10.1.1.2
   ldp
   path-mtu 1514
   keep-alive
   shutdown
   exit
   binding
   port lag-1
   pw-port 1 vc-id 1 create
   no shutdown
   exit
   pw-port 2 vc-id 2 create
   no shutdown
   exit
   exit
   no shutdown
   exit
   ```

3. Configure a SAP on the IES or VPRN interface, with a SAP ID that uses the form \texttt{pw-id}.
   ```
   ies 1 customer 1 create
   interface "ies if" create
   address 30.1.1.1/24
   mac 00:00:00:00:ff
   ```
QoS for Pseudowire Ports and Pseudowire SAPs

Pseudowire SAPs support the QoS models allowed for regular IES or VPRN SAPs. These include:

- **Per-service HQoS.**
  This allows shaping of the total traffic per access node (and total traffic per class per AN), assuming one pseudowire per AN from the A-PE.

- **SAP QoS support as available on the IOM3-XP, including**
  H-QoS (service scheduler child to port scheduler parent)
  → SAP queues attached to H-QoS scheduler by ‘parent’ statement
  → Scheduler attached to Port Scheduler by ‘port-parent’ statement
  Direct service queue to port scheduler mapping
  → Aggregate-rate-limit
  Support for the redirection of SAP egress queues to an access queue group instance. It is possible to redirect SAP queues of a pseudowire SAP using the SAP based redirection for the IOM3 with Ethernet MDA or HSMDAv2, and policy based redirection for the IOM3 with Ethernet MDA, as applicable.

- **Policing and H-POL**
Shaping and Bandwidth Control

Pseudowire SAPs can be shaped on egress by a vport on a physical port. The pseudowire SAP egress cannot explicitly declare which vport to use, but they will inherit the vport used by the pw-port egress shaping.

Note that the vport is represented by a secondary shaper on an HSMDAv2. The intermediate destination identifier, used for ESM on MPLS pseudowires, is not applicable to IES and VPRN pseudowire SAPs.

If a pseudowire port is configured on a LAG, then vport shaping is only supported if the LAG is in link mode.

Per-access node shaping is configured as follows:

1. Configure a vport(s) per AN under the port (or LAG) to which the SDP corresponding to the pseudowire SAP is bound. The vport would be configured with aggregate rate-limit (\texttt{configure>port>ethernet>access>egress>vport vport-name create}).

2. Explicitly assign (via static configuration) a pseudowire port to a vport. For limiting the total traffic to an AN, all pseudowire ports for an AN-port would refer to the same vport.

As in the ESM on pseudowire case, vport scheduling on the HSMDAv2 is implemented using an exp-secondary-shaper. This is referred to as a pw-sap-secondary-shaper in the new CLI below. If an 'hsmda-queue-override secondary-shape' is defined for the pw-sap, then the system will use the override, else:

- If a named pw-sap-secondary-shaper is defined for the pw-port, then that is used,
- Else, the default exp-secondary-shaper for the port is used.

For bandwidth control per pseudowire, the following configuration steps are used:

1. Create multiple vports under the port to which SDP is bound. Each vport can be configured with \texttt{agg-rate rate}, a scheduler or port-scheduler.

2. Assign each pseudowire to an AN to a unique vport shaper (regular IOM/MDA) or secondary shaper (on HSMDAv2).

To make use of the \texttt{agg-rate rate} or \texttt{port-scheduler} under a VPORT, PW SAP queues and schedulers must be configured with the \texttt{port-parent} command. To make use of a scheduler under a VPORT, PW SAP schedulers must be configured with a \texttt{parent} command and the \texttt{parent-location vport} under the tier 1 of the scheduler policy. The egress hierarchical parenting relationship options are shown in Figure 143. See the SR OS Quality of Service guide for more details.
Last Mile Packet Size Adjustment

In the application where pseudowire SAPs are used to apply access QoS for services aggregated from an Ethernet access network, MPLS labels may not be present on the last-mile and link from an access node. In these cases, policers, queues and H-QoS schedulers should account for packets without MPLS overhead, modeled as “encaps-offset”. Vport and port schedulers behave as per the table below. In the data-path, the actual pseudowire encap overhead (taking into account the MPLS labels) added to the packet is tracked, and may be applied to the scheduler calculations via the configured packet-byte-offset.

Note that the exp-secondary-shaper used on the HSMDAv2 always assumes MPLS overhead and does not account for the packet-byte-offset. In all other cases, the rate limit configured for the pseudowire SAP accounts for subscriber or service frame wire rate: without MPLS overhead and including the last mile overhead (unless a packet-byte-offset is configured).

Table 17 summarizes the default packet sizes used at each of the schedulers on the IOM/Ethernet MDA and HSMDAv2, assuming a 1000byte customer packet.
Redundancy with Pseudowire SAPs

Within a chassis, IOM and port based redundancy is based on active/backup LAG. The topology for the base MPLS LSP used by the SDP could be constrained such that it could get re-routed in the aggregation network, but would always appear on the LAG ports on the Layer 3 PE. In the case that the tunnel is re-routed to a different port, the MPLS pseudowire SAPs would be brought down.

In order to provide Layer 3 PE redundancy, dual homing of the access PE into separate Layer 3 PEs using active/standby pseudowire status is supported. This is shown in Figure 144.

<table>
<thead>
<tr>
<th>Type</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>exp-secondary-shaper</td>
<td>20B preamble + 26 MPLS + 1000B pkt</td>
</tr>
<tr>
<td>queue/policer rate on hsmdav2</td>
<td>1000B customer pkt</td>
</tr>
<tr>
<td>port-scheduler rate</td>
<td>20B preamble + 1000B pkt</td>
</tr>
<tr>
<td>regular queue/policer rate</td>
<td>1000B pkt</td>
</tr>
<tr>
<td>vport agg-limit-rate</td>
<td>20B preamble + 1000B pkt</td>
</tr>
<tr>
<td>vport port-scheduler rate</td>
<td>20B preamble + 1000B pkt</td>
</tr>
<tr>
<td>vport scheduler rate</td>
<td>1000B pkt</td>
</tr>
<tr>
<td>vport scheduler to port-scheduler rates</td>
<td>20B preamble + 1000B pkt</td>
</tr>
</tbody>
</table>

Figure 144: Dual Homing into Multiple Layer 3 PEs
Dual homing operates in a similar manner to spoke-sdp termination on IES/VPRN. Figure 144 displays the access PE is dual-homed to the Layer 3 PEs using two spoke-SDPs. The endpoint in the access PE is configured to be the master from a pseudowire redundancy perspective using the standby-signaling-master command. The access PE picks one of the spoke-SDPs to make active, and one to make standby, based on the local configuration of primary or spoke SDP precedence.

The pseudowire port at the Layer 3 PE behaves as a slave from the perspective of pseudowire status signaling. That is, if its peer signals "PW FWD standby (0x20)" status bit for the given spoke-sdp and the local configuration does not allow this bit to be ignored, the PE will take the pseudowire port to a local operationally down state. This is consistent with the spoke-sdp behavior for the case of spoke-sdp termination on IES/VPRN.

As a consequence, all of the pseudowire SAPs bound to the pseudowire port are taken down, which causes the corresponding IES or VPRN interface to go to a local operationally down state and thus will stop forwarding packets towards this pseudowire port.

Conversely, the formerly standby pseudowire is made active and then the corresponding pseudowire port on the second Layer 3 PE is taken locally operationally up. Therefore, all of the pseudowire SAPs bound to the pseudowire port are brought up, which causes the corresponding IES or VPRN interface to go to a local operationally up state allowing forwarding of packets towards this pseudowire port.
Routing Protocols

The IES IP interfaces are restricted as to the routing protocols that can be defined on the interface based on the fact that the customer has a different routing domain for this service. The IES IP interfaces support the following routing protocols:

- RIP
- OSPF
- IS-IS
- BGP
- IGMP
- PIM

Note that the SAP for the IES IP interface is created at the IES service level, but the routing protocols for the IES IP interface are configured at the routing protocol level for the main router instance.

CPE Connectivity Check

Static routes are used within many IES services. Unlike dynamic routing protocols, there is no way to change the state of routes based on availability information for the associated CPE. CPE connectivity check adds flexibility so that unavailable destinations will be removed from the service provider’s routing tables dynamically and minimize wasted bandwidth.

The availability of the far-end static route is monitored through periodic polling. The polling period is configured. If the poll fails a specified number of sequential polls, the static route is marked as inactive.

An ICPM ping mechanism is used to test the connectivity.

If the connectivity check fails and the static route is de-activated, the router will continue to send polls and re-activate any routes that are restored.
QoS Policies

When applied to SR-OS IES services, service ingress QoS policies only create the unicast queues defined in the policy. The multipoint queues are not created on the service. With IES services, service egress QoS policies function as with other services where the class-based queues are created as defined in the policy. Note that both Layer 2 or Layer 3 criteria can be used in the QoS policies for traffic classification in an IES.

Filter Policies

Only IP filter policies can be applied to IES services.
Configuring an IES Service with CLI

This section provides information to configure IES services using the command line interface. Topics in this section include:

- **Basic Configuration on page 1082**
- **Common Configuration Tasks on page 1083**
  - Configuring IES Components on page 1084
    - Configuring an IES Service on page 1084
    - Configuring IES Interface Parameters on page 1085
  - Configuring SAP Parameters on page 1086
- **Service Management Tasks on page 1088**
  - Modifying IES Service Parameters on page 1088
  - Deleting an IES Service on page 1089
  - Disabling an IES Service on page 1090
  - Re-Enabling an IES Service on page 1090
Basic Configuration

The most basic IES service configuration has the following entities:

- Customer ID (refer to Configuring Customers on page 84)
- An interface to create and maintain IP routing interfaces within IES service ID.
- A SAP on the interface specifying the access port and encapsulation values.

The following example displays a sample configuration of an IES service on ALA-48.

```
*A:ALA-48>config>service# info
----------------------------------------------
  ies 1000 customer 50 vpn 1000 create
description "to internet"
  interface "to-web" create
       address 10.1.1.1/24
       sap 1/1/5:0.1 create
       exit
exit
no shutdown
----------------------------------------------
*A:ALA-48>config>service#
```
Common Configuration Tasks

This section provides a brief overview of the tasks that must be performed to configure IES services and provides the CLI commands.

1. Associate an IES service with a customer ID.
2. Associate customer ID with the service.
3. Assign an IP address.
4. Create an interface.
5. Define SAP parameters on the interface
   → Select node(s) and port(s).
   → Optional — select filter policies (configured in the config>filter context).
6. Enable service.
Configuring IES Components

Use the CLI syntax to configure the following entities:

- Configuring an IES Service on page 1084
- Configuring IES Interface Parameters on page 1085
  → Configuring SAP Parameters on page 1086

Configuring an IES Service

Use the following CLI syntax to create an IES service:

The following example displays a basic IES service configuration.

```
A:ALA-48>config>service#
----------------------------------------------
...  
  ies 1001 customer 1730 create
description "to-internet"
  no shutdown
  exit
----------------------------------------------
A:ALA-48>config>service#
```
Configuring IES Interface Parameters

The following example displays an IES configuration with interface parameters:

```
A:ALA-48>config>service>ies>if# info
----------------------------------------------
 address 10.1.1.1/24
 sap 1/1/10:0.* create
 exit
----------------------------------------------
A:ALA-48>config>service>ies>if#
```
Configuring SAP Parameters

A SAP is a combination of a port and encapsulation parameters which identifies the service access point on the interface and within the router. Each SAP must be unique within a router.

Filter policies are configured in the `config>filter` context and must be explicitly applied to a SAP. There are no default filter policies.

This example displays an IES SAP configuration.

```
*A:ALA-A>config>service>ies>if# info
--------------------------------------------
  address 10.10.36.2/24
  exit
--------------------------------------------
*A:ALA-A>config>service>ies>if#
```
IGMP Host Tracking

The following output displays an IES service with IGMP host tracking parameters configured.

*A:ALA-49>config>service# info
---------------------------------------------------------------
...  
es 25 customer 1 create
    interface "ip_if_4" create
        loopback
delayed-enable 1200
address 64.64.64.64/24
    sap lag-64:64 create
        no shutdown
        exit
        allow-directed-broadcasts
        host-connectivity-verify
        ip-mtu 9000
        local-dhcp-server "server 1"
        local-proxy-arp
        proxy-arp-policy treetrace-1
        remote-proxy-arp
        secondary 2.3.4.5 255.255.255.0
        secondary 2.3.4.5/24
        tos-marking-state trusted
        tos-marking-state untrusted
        urpf-check
    exit
...  
es 25 customer 1 create
    interface "ip_if_4" create
        loopback
delayed-enable 1200
address 64.64.64.64/24
    sap lag-64:64 create
        no shutdown
        exit
        allow-directed-broadcasts
        host-connectivity-verify
        ip-mtu 9000
        local-dhcp-server "server 1"
        local-proxy-arp
        proxy-arp-policy treetrace-1
        remote-proxy-arp
        secondary 2.3.4.5 255.255.255.0
        secondary 2.3.4.5/24
        tos-marking-state trusted
        tos-marking-state untrusted
        urpf-check
    exit
...  

*A:ALA-49>config>service#*
Service Management Tasks

This section discusses the following service management tasks:

- Modifying IES Service Parameters on page 1088
- Deleting an IES Service on page 1089

Modifying IES Service Parameters

Existing IES service parameters in the CLI or NMS can be modified, added, removed, enabled or disabled. The changes are applied immediately to all services when the charges are applied.

To display a list of customer IDs, use the `show service customer` command.

Enter the parameter(s) (such as description, SAP information and SDP information) and then enter the new information.

The following displays the modified service:

```
*A:ALA-A>config>service>ies# info
----------------------------------------------
  ies 1000 customer 50 vpn 1000 create
    description "This is a new description"
    interface "to-web" create
    address 10.1.1.1/24
    mac 00:dc:98:1d:00:00
    allow-directed-broadcast
    exit
  exit
  no shutdown
  exit
----------------------------------------------
*A:ALA-A>config>service#
```
Deleting an IES Service

An IES service cannot be deleted until SAPs and interfaces are shut down and deleted and the service is shutdown on the service level.

Use the following CLI syntax to delete an IES service:

**CLI Syntax:**
```
config>service#
    [no] ies service-id
    shutdown
    [no] interface ip-int-name
    shutdown
    [no] sap sap-id
    shutdown
```
Disabling an IES Service

An IES service can be shut down without deleting the service parameters.

**CLI Syntax:**

```
config>service> ies service-id
    shutdown
```

Re-Enabling an IES Service

To re-enable an IES service that was shut down.

**CLI Syntax:**

```
config>service> ies service-id
    [no] shutdown
```

**Example:**

```
config>service# ies 2000
config>service>ies# no shutdown
config>service>ies# exit
```
IES Services Command Reference

Command Hierarchies

- IES Service Configuration Commands on page 1091
- Global Commands on page 1091
- Interface Commands on page 1091
- Interface SAP Commands on page 1094
- VRRP Commands on page 1097
- Spoke SDP Commands on page 1099
- Show Commands on page 1101

IES Service Configuration Commands

Global Commands

```
config
    service
        ies service-id [customer customer-id] [vpn vpn-id] [create]
        no ies service-id
            description description-string
            no description
            igmp-host-tracking
                expiry-time expiry-time
                [no] shutdown
            service-name service-name
            no service-name
            [no] shutdown
```

Interface Commands

```
config
    service
        ies service-id [customer customer-id] [vpn vpn-id]
        interface ip-int-name [create] [tunnel]
        no interface ip-int-name
            address {ip-address/mask | ip-address netmask} [broadcast [all-ones | host-ones]]
            no address [ip-address/mask | ip-address netmask]
            [no] allow-directed-broadcasts
            [no] arp-populate
            arp-timeout seconds
            no arp-timeout
```
— bfd transmit-interval [receive receive-interval] [multiplier multiplier] [echo-receive echo-interval] [type cpm-np]

— no bfd

— cflowd [acl | interface] [direction]
— no cflowd

— cpu-protection policy-id
— no cpu-protection
— description description-string
— no description

— dynamic-tunnel-redundant-next-hop ip-address
— no dynamic-tunnel-redundant-next-hop

— [no] egr-ip-load-balancing
— [no] enable-ingress-stats
— [no] enable-mac-accounting
— [no] flowspec

— host-connectivity-verify [source {vrrp | interface}] [interval interval] [action {remove | alarm}]

— icmp

— [no] mask-reply
— redirects [number seconds]
— no redirects
— ttl-expired [number seconds]
— no ttl-expired
— unreachable {number seconds]
— no unreachable}

— if-attribute

— [no] admin-group group-name [group-name...(up to 5 max)]
— no admin-group
— [no] srlg-group group-name [group-name...(up to 5 max)]
— no srlg-group

— ip-mtu octets
— no ip-mtu

— ip

— [no] ip-address [secondary ip-address]
— ip secondary ip-address
— no ip-address [secondary ip-address]
— peer-ip-address ip-address
— no peer-ip-address

— [no] ipv6

— address ipv6-address/prefix-length [eui-64]
— no address ipv6-address/prefix-length
— bfd transmit-interval [receive receive-interval] [multiplier multiplier] [echo-receive echo-interval] [type cpm-np]
— no bfd

— icmp6

— [no] local-proxy-nd
— neighbor ipv6-address mac-address
— no neighbor ipv6-address
— proxy-nd-policy policy-name [policy-name...(up to 5 max)]
— no proxy-nd-policy
— [no] qos-route-lookup
— tcp-mss mss-value
— no tcp-mss
— [no] urpf-check
  — mode [strict | loose | strict-no-ecmp]
  — no mode

— [no] local-proxy-arp
— [no] loopback
— [no] mac ieee-address
— monitor-oper-group name
— no monitor-oper-group
— [no] proxy-arp-policy policy-name [policy-name...(up to 5 max)]
— [no] ptp-hw-assist
— qos-route-lookup [source | destination]
— no qos-route-lookup
— [no] remote-proxy-arp
— secondary [ip-address/mask | ip-address netmask] [broadcast all-ones | host-ones] [igp-inhibit]
— no secondary ip-address
— [no] shutdown
— static-arp ieee-mac-addr unnumbered
— no static-arp unnumbered
— static-tunnel-redundant-next-hop ip-address
— no static-tunnel-redundant-next-hop
— tcp-mss mss-value
— no tcp-mss
— [no] teid-load-balancing
— tos-marking-state [trusted | untrusted]
— no tos-marking-state
— unnumbered [ip-int-name | ip-address]
— no unnumbered
— [no] urpf-check
  — mode [strict | loose | strict-no-ecmp]
  — no mode
Interface SAP Commands

```plaintext
config
  — service
    — ies service-id [customer customer-id] [vpn vpn-id]
    — [no] interface ip-int-name
    — [no] sap sap-id
      — aarp aarpid type type
      — no aarp
      — accounting-policy acct-policy-id
      — no accounting-policy [acct-policy-id]
      — anti-spoof {ip | ip-mac}
      — no anti-spoof
      — app-profile app-profile-name
      — no app-profile
      — calling-station-id calling-station-id
      — no calling-station-id
      — description description-string
      — no description
  — egress
    — agg-rate-limit agg-rate [queue-frame-based-accounting]
    — no agg-rate-limit
    — [no] agg-rate
      — rate {max | rate}
      — no rate
      — [no] limit-unused-bandwidth
      — [no] queue-frame-based-accounting
      — [no] qinq-mark-top-only
    — filter [ip ip-filter-id]
    — filter [ipv6 ipv6-filter-id]
    — no filter [ip ip-filter-id] [ipv6 ipv6-filter-id]
    — [no] qinq-mark-top-only
    — qos policy-id [port-redirect-group queue-group-name instance instance-id]
    — no qos
    — [no] queue-override
      — [no] queue queue-id
        — adaptation-rule [pir {max | min | closest}] [cir {max | min | closest}]
        — no adaptation-rule
        — avg-frame-overhead percentage
        — no avg-frame-overhead
        — cbs size-in-kbytes
        — no cbs
        — high-prio-only percent
        — no high-prio-only
        — mbs size-in-kbytes
        — no mbs
        — rate pir-rate [cir cir-rate]
        — no rate
      — [no] scheduler-override
        — [no] scheduler scheduler-name
        — rate pir-rate [cir cir-rate]
        — no rate
    — scheduler-policy scheduler-policy-name
```
— no scheduler-policy

— eth-cfm

— mep mep-id domain md-index association ma-index
  [direction {up | down}]

— no mep mep-id domain md-index association ma-index
  [direction {up | down}]

  — [no] ais-enable
  — [no] interface-support-enable

  — [no] ccm-enable

  — ccm-ltm-priority priority

  — no ccm-ltm-priority

  — [no] ccm-padding-size ccm-padding

  — [no] description

  — [no] eth-test-enable
    — [no] test-pattern {all-zeros | all-ones}
    — [no] crc-enable

  — fault-propagation-enable {use-if-tlv | suspend-ecm}

  — no fault-propagation-enable

  — low-priority-defect {allDef | macRemErrXcon | remErrXcon | xcon | noXcon}

  — one-way-delay-threshold seconds

  — [no] shutdown

  — [no] squelch-ingress-levels [md-level [md-level...]]

  — tunnel-fault [accept | ignore]

— host-lockout-policy policy-name

— no host-lockout-policy

— [no] host-shutdown

— ingress

  — filter [ip ip-filter-id]
  — filter [ipv6 ipv6-filter-id]

  — no filter [ip ip-filter-id] [ipv6 ipv6-filter-id]

  — [no] flowspec

  — flowspec-ipv6

  — [no] flowspec-ipv6

  — match-qinq-dot1p {top | bottom}

  — no match-qinq-dot1p

  — qos policy-id [shared-queueing | multipoint-shared][fp-redirect-group queue-group-name
    instance instance-id]

  — no qos policy-id

  — [no] queue-override

  — [no] queue queue-id

    — adaptation-rule [pir {max | min | closest}] [cir {max | min | closest}]

    — no adaptation-rule

    — avg-frame-overhead percentage

    — no avg-frame-overhead

    — cbs size-in-kbytes

    — no cbs

    — high-prio-only percent

    — no high-prio-only
— mbs size-in-kbytes
— no mbs
— rate pir-rate [cir cir-rate]
— no rate
— [no] scheduler-override
— [no] scheduler scheduler-name
— rate pir-rate [cir cir-rate]
— no rate
— scheduler-policy scheduler-policy-name
— no scheduler-policy
— lag-link-map-profile lag-ink-map-profile-id
— no lag-link-map-profile
— multi-service-site customer-site-name
— no multi-service-site
— static-host ip ip/did-address [mac ieee-address] [create]
— static-host mac ieee-address [create]
— no static-host [ip ip-address] mac ieee-address
— no static-host all [force]
— no static-host ip ip-address
— ancp-string ancp-string
— no ancp-string
— app-profile app-profile-name
— no app-profile
— inter-dest-id intermediate-destination-id
— no inter-dest-id
— [no] shutdown
— sla-profile sla-profile-name
— no sla-profile
— sub-profile sub-profile-name
— no sub-profile
— subscriber sub-ident
— no subscriber
— [no] subscriber-sap-id
— tod-suite tod-suite-name
— no tod-suite
— transit-policy ip-aasub-policy-id
— no transit-policy
— [no] shutdown
VRRP Commands

```plaintext
config
  service
    ies service-id [customer customer-id] [vpn vpn-id]
    [no] interface ip-int-name
    [no] ipv6
      vrrp virtual-router-id [owner]
      no vrrp virtual-router-id
        [no] backup ip-address
        [no] bfd-enable service-id interface interface-name dst-ip ip-address
        [no] bfd-enable interface interface-name dst-ip ip-address
        init-delay seconds
        no init-delay
        mac mac-address
        no mac
        [no] master-int-inherit
        message-interval ([seconds] [milliseconds milliseconds])
        no message-interval
        [no] ping-reply
        policy vrrp-policy-id
        no policy
        [no] preempt
        priority base-priority
        no priority
        [no] shutdown
        [no] standby-forwarding
        [no] telnet-reply
        [no] traceroute-reply
  vrrp virtual-router-id [owner]
  no vrrp virtual-router-id
    authentication-key {authentication-key | hash-key} [hash | hash2]
    no authentication-key
    authentication-type {password | message-digest}
    no authentication-type
    [no] backup ip-address
    [no] bfd-enable [service-id] interface interface-name dst-ip ip-address
    init-delay seconds
    no init-delay
    mac ieee-address
    no mac
    [no] master-int-inherit
    message-interval ([seconds] [milliseconds milliseconds])
    no message-interval
    [no] ping-reply
    policy vrrp-policy-id
```
— no policy
— [no] preempt
— priority priority
— no priority
— [no] shutdown
— [no] ssh-reply
— [no] standby-forwarding
— [no] telnet-reply
— [no] traceroute-reply
Spoke SDP Commands

```
config
  -- service
    -- ies service-id [customer customer-id] [vpn vpn-id]
    -- [no] interface ip-int-name
    -- [no] spoke-sdp sdp-id:vc-id [vc-type {ether | ipipe}] [create]
      -- aarp aarpId type
      -- no aarp
      -- accounting-policy acct-policy-id
      -- no accounting-policy
      -- app-profile app-profile-name
      -- no app-profile
      -- [no] collect-stats
    -- eth-cfm
      -- mep mep-id domain md-index association ma-index
        [direction {up | down}]
      -- no mep mep-id domain md-index association ma-index
        -- [no] ais-enable
        -- [no] interface-support-enable
        -- [no] ccm-enable
        -- ccm-ltm-priority priority
        -- no ccm-ltm-priority
        -- [no] description
        -- [no] eth-test-enable
          -- [no] test-pattern {all-zeros | all-ones}
          -- [crc-enable]
        -- fault-propagation-enable {use-if-tlv | suspend-cm}
        -- no fault-propagation-enable
        -- low-priority-defect {allDef | macRemErrXcon | remErrXcon | errXcon | noXcon}
        -- low-priority-defect seconds
        -- [no] shutdown
    -- egress
      -- filter [ip ip-filter-id]
      -- filter [ipv6 ipv6-filter-id]
      -- no filter [ip ip-filter-id] [ipv6 ipv6-filter-id]
      -- qos network-policy-id port-redirect-group queue-group-name [instance instance-id]
        -- no qos
        -- vc-label egress-vc-label
        -- no vc-label [egress-vc-label]
      -- flowspec
      -- [no] flowspec
      -- flowspec-ipv6
      -- [no] flowspec-ipv6
      -- [no] hash-label
      -- ingress
        -- filter [ip ip-filter-id]
        -- filter [ipv6 ipv6-filter-id]
```
— no filter
— [no] flowspec
— qos network-policy-id fp-redirect-group queue-group-name instance instance-id
— no qos
— vc-label ingress-vc-label
— no vc-label [ingress-vc-label]
— [no] shutdown
— transit-policy ip-aasub-policy-id
— no transit-policy
— [no] proxy-arp-policy policy-name [policy-name...(up to 5 max)]
— [no] remote-proxy-arp
— [no] unreachable
Show Commands

```plaintext
tshow
  -- service
    -- customer [customer-id] [site customer-site-name]
    -- sap-using [sap sap-id]
    -- sap-using interface [ip-address | ip-int-name]
    -- sap-using [ingress | egress] atm-td-profile id-profile-id
    -- sap-using [ingress | egress] filter filter-id
    -- sap-using [ingress | egress] qos-policy qos-policy-id
    -- sap-using authentication-policy policy-name
    -- service-using [ies] [customer customer-id]
    -- id service-id
      -- all
        -- arp [ip-address][mac ieee-address][sap sap-id][interface ip-int-name] [sdp sd-p-id:vc-id]
        -- base
        -- gsmp
          -- neighbors group [name] [ip-address]
            -- sessions [group name] neighbor ip-address [port port-number] [association] [statistics]
            -- host
            -- host-connectivity-verify statistics [sap sap-id]
        -- interface [ip-address | ip-int-name] [interface-type] [detail] [family]
        -- interface
        -- retailers
        -- sap sap-id [detail]
        -- sdp [sdp-id | far-end ip-address] [detail]
    -- router
    -- vrrp
        -- instance
        -- instance interface interface-name [vrid virtual-router-id]
        -- instance interface interface-name vrid virtual-router-id ipv6
        -- statistics
```

Clear Commands

```plaintext
tclear
  -- router
    -- interface [ip-int-name | ip-address] [icmp]
    -- vrrp
    -- interface interface-name [vrid virtual-router-id]
    -- interface interface-name vrid virtual-router-id ipv6
    -- statistics
    -- statistics interface interface-name [vrid virtual-router-id]
    -- statistics interface interface-name vrid virtual-router-id ipv6
  -- service
    -- id service-id
      -- arp-host
      -- arp-host { mac ieee-address | sap sap-id | ip-address ip-address[mask] }
```
— **arp-host** [port port-id] [inter-dest-id intermediate-destination-id | no-inter-dest-id]
— **arp-host statistics** [sap sap-id | interface interface-name]
— **fdb** [all | mac ieee-address | sap sap-id | mesh-sdp sdp-id:vc-id] | **spoke-sdp** sdp-id:vc-id ingress-vc-label
— **site** service-id
— **spoke-sdp** sdp-id:vc-id ingress-vc-label
— **stp**
Debug Commands

debug
  — service
    — id service-id
    — [no] arp-host
      — [no] host-connectivity-verify
        — [no] ip ip-address
        — [no] mac ieee-address
        — [no] sap sap-id
    — router
      — vrrp
        — [no] events
        — events interface-name [vrid virtual-router-id]
        — events interface-name vrid virtual-router-id ipv6
        — [no] packets
        — packets interface-name [vrid virtual-router-id]
        — packets interface-name vrid virtual-router-id ipv6

Monitor Commands

monitor
  — router
    — vrrp
      — instance interface interface-name vr-id virtual-router-id [ipv6] [interval seconds]
      [repeat repeat] [absolute|rate]
IES Service Configuration Commands

Generic Commands

shutdown

Syntax  [no] shutdown

Context  config>service>ies
         config>service>ies>igmp-snooping
         config>service>ies/if.sap>eth-cfm
         config>service>ies/if
         config>service>ies/if>vrp

Description  This command administratively disables an entity. When disabled, an entity does not change, reset, or remove any configuration settings or statistics. The operational state of the entity is disabled as well as the operational state of any entities contained within. Many objects must be shut down before they may be deleted.

Services are created in the administratively down (shutdown) state. When a no shutdown command is entered, the service becomes administratively up and then tries to enter the operationally up state. Default administrative states for services and service entities is described below in Special Cases.

The no form of this command places the entity into an administratively enabled state.

Special Cases  IES — The default administrative status of an IES service is down. While the service is down, all its associated virtual router interfaces will be operationally down. The administrative state of the service is not reflected in the administrative state of the virtual router interface.

For example if:  1) An IES service is operational and an associated interface is shut down.
   2) The IES service is administratively shutdown and brought back up.
   3) The interface shutdown will remain in administrative shutdown state.

A service is regarded as operational provided that one IP Interface is operational.

IES IP Interfaces — When the IP interface is shutdown, it enters the administratively and operationally down states. For a SAP bound to the IP interface, no packets are transmitted out the SAP and all packets received on the SAP will be dropped while incrementing the packet discard counter.

description

Syntax  description description-string
no description

Context  config>service>ies
         config>service>ies/if>dhcp

Description  This command creates a text description stored in the configuration file for a configuration context.
The **description** command associates a text string with a configuration context to help identify the content in the configuration file.

The **no** form of this command removes the string from the configuration.

**Default**

No description associated with the configuration context.

**Parameters**

`string` — The description character string. Allowed values are any string up to 80 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.
IES Global Commands

ies

Syntax

ies service-id customer customer-id [vpn vpn-id] [create]
no ies service-id

Context

config>service

Description

This command creates or edits an IES service instance.

The ies command is used to create or maintain an Internet Enhanced Service (IES). If the service-id does not exist, a context for the service is created. If the service-id exists, the context for editing the service is entered.

IES services allow the creation of customer facing IP interfaces in the same routing instance used for service network core routing connectivity. IES services require that the IP addressing scheme used by the subscriber must be unique between it and other addressing schemes used by the provider and potentially the entire Internet.

While IES is part of the routing domain, the usable IP address space may be limited. This allows a portion of the service provider address space to be set aside for service IP provisioning, becoming administered by a separate but subordinate address authority. This feature is defined using the config router service-prefix command.

IP interfaces defined within the context of an IES service ID must have a SAP created as the access point to the subscriber network. This allows a combination of bridging and IP routing for redundancy purposes.

When a service is created, the customer keyword and customer-id must be specified and associates the service with a customer. The customer-id must already exist having been created using the customer command in the service context. Once a service has been created with a customer association, it is not possible to edit the customer association. The service must be deleted and recreated with a new customer association.

Once a service is created, the use of the customer customer-id is optional for navigating into the service configuration context. Attempting to edit a service with the incorrect customer-id specified will result in an error.

Multiple IES services are created to separate customer owned IP interfaces. More than one IES service may be created for a single customer ID. More than one IP interface may be created within a single IES service ID. All IP interfaces created within an IES service ID belongs to the same customer.

By default, no IES service instances exist until they are explicitly created.

The no form of this command deletes the IES service instance with the specified service-id. The service cannot be deleted until all the IP interfaces defined within the service ID have been shutdown and deleted.

Parameters

service-id — The unique service identification number or string identifying the service in the service domain. This ID must be unique to this service and may not be used for any other service of any type. The service-id must be the same number used for every SR OS router on which this service is defined.

Values

service-id: 1 — 2147483648
svc-name: 64 characters maximum
customer customer-id — Specifies the customer ID number to be associated with the service. This parameter is required on service creation and optional for service editing or deleting.

Values 1 — 2147483647

vpn vpn-id — Specifies the VPN ID number which allows you to identify virtual private networks (VPNs) by a VPN identification number.

Values 1 — 2147483647

Default null (0)

service-name

Syntax service-name service-name
no service-name

Context config>service>ies

Description This command configures an optional service name, up to 64 characters in length, which adds a name identifier to a given service to then use that service name in configuration references as well as display and use service names in show commands throughout the system. This helps the service provider/administrator to identify and manage services within the SR OS platforms.

All services are required to assign a service ID to initially create a service. However, either the service ID or the service name can be used to identify and reference a given service once it is initially created.

Parameters service-name — Specifies a unique service name to identify the service. Service names may not begin with an integer (0-9).
IES Interface Commands

**interface**

**Syntax**  
```
interface ip-int-name [create] [tunnel]
no interface ip-int-name
```

**Context**  
```
config>service>ies
```

**Description**  
This command creates a logical IP routing interface for an Internet Enhanced Service (IES). Once created, attributes like an IP address and service access point (SAP) can be associated with the IP interface.

The `interface` command, under the context of services, is used to create and maintain IP routing interfaces within IES service IDs. The `interface` command can be executed in the context of an IES service ID. The IP interface created is associated with the service core network routing instance and default routing table. The typical use for IP interfaces created in this manner is for subscriber internet access. An IP address cannot be assigned to an IES interface. Multiple SAPs can be assigned to a single group interface.

Interface names are case sensitive and must be unique within the group of defined IP interfaces defined for `config router interface` and `config service ies interface` (that is, the network core router instance). Interface names must not be in the dotted decimal notation of an IP address. For example, the name “1.1.1.1” is not allowed, but “int-1.1.1.1” is allowed. Show commands for router interfaces use either interface names or the IP addresses. Use unique IP address values and IP address names to maintain clarity. It could be unclear to the user if the same IP address and IP address name values are used. Although not recommended, duplicate interface names can exist in different router instances.

The available IP address space for local subnets and routes is controlled with the `config router service-prefix` command. The `service-prefix` command administers the allowed subnets that can be defined on IES IP interfaces. It also controls the prefixes that may be learned or statically defined with the IES IP interface as the egress interface. This allows segmenting the IP address space into `config router` and `config service` domains.

When a new name is entered, a new logical router interface is created. When an existing interface name is entered, the user enters the router interface context for editing and configuration.

By default, there are no default IP interface names defined within the system. All IES IP interfaces must be explicitly defined. Interfaces are created in an enabled state.

The `no` form of this command removes IP the interface and all the associated configuration. The interface must be administratively shutdown before issuing the `no interface` command.

For IES services, the IP interface must be shutdown before the SAP on that interface may be removed. IES services do not have the `shutdown` command in the SAP CLI context. IES service SAPs rely on the interface status to enable and disable them.

**Parameters**  
`ip-int-name` — Specifies the name of the IP interface. Interface names must be unique within the group of defined IP interfaces for `config router interface` and `config service ies interface` commands. An interface name cannot be in the form of an IP address. Interface names can be from 1 to 32 alphanumeric characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.
IES Interface Commands

If ip-int-name already exists within the service ID, the context will be changed to maintain that IP interface. If ip-int-name already exists within another service ID or is an IP interface defined within the config router commands, an error will occur and context will not be changed to that IP interface. If ip-int-name does not exist, the interface is created and context is changed to that interface for further command processing.

address

Syntax

address {ip-address/mask | ip-address netmask} [broadcast [all-ones | host-ones]]
no address [ip-address/mask | ip-address netmask]

Context

config>service>ies>if

Description

This command assigns an IP address, IP subnet, and broadcast address format to an IES IP router interface. Only one IP address can be associated with an IP interface. An IP address must be assigned to each IES IP interface. An IP address and a mask are used together to create a local IP prefix. The defined IP prefix must be unique within the context of the routing instance. It cannot overlap with other existing IP prefixes defined as local subnets on other IP interfaces in the same routing context within the router.

The local subnet that the address command defines must be part of the services address space within the routing context using the config router service-prefix command. The default is to disallow the complete address space to services. Once a portion of the address space is allocated as a service prefix, that portion can be made unavailable for IP interfaces defined within the config router interface CLI context for network core connectivity with the exclude option in the config router service-prefix command.

The IP address for the interface can be entered in either CIDR (Classless Inter-Domain Routing) or traditional dotted decimal notation. The show commands display CIDR notation and is stored in configuration files.

By default, no IP address or subnet association exists on an IP interface until it is explicitly created. Use the no form of this command to remove the IP address assignment from the IP interface.

The no form of this command will cause ptp-hw-assist to be disabled.

<table>
<thead>
<tr>
<th>Address</th>
<th>Admin state</th>
<th>Oper state</th>
</tr>
</thead>
<tbody>
<tr>
<td>No address</td>
<td>up</td>
<td>down</td>
</tr>
<tr>
<td>No address</td>
<td>down</td>
<td>down</td>
</tr>
<tr>
<td>1.1.1.1</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>1.1.1.1</td>
<td>down</td>
<td>down</td>
</tr>
</tbody>
</table>

The operational state is a read-only variable and the only controlling variables are the address and admin states. The address and admin states are independent and can be set independently. If an interface is in an administratively up state and an address is assigned, it becomes operationally up and the protocol interfaces and the MPLS LSPs associated with that IP interface will be reinitialized.

ip-address — The IP address of the IP interface. The ip-address portion of the address command specifies the IP host address that will be used by the IP interface within the subnet. This address must be unique within the subnet and specified in dotted decimal notation. Allowed values are IP addresses in the range 1.0.0.0 – 223.255.255.255 (with support of /31 subnets).
The forward slash is a parameter delimiter and separates the \textit{ip-address} portion of the IP address from the mask that defines the scope of the local subnet. No spaces are allowed between the \textit{ip-address}, the \textit{/} and the \textit{mask-length} parameter. If a forward slash is not immediately following the \textit{ip-address}, a dotted decimal mask must follow the prefix.

\texttt{mask-length} — The subnet mask length when the IP prefix is specified in CIDR notation. When the IP prefix is specified in CIDR notation, a forward slash (\textit{/}) separates the \textit{ip-address} from the \textit{mask-length} parameter. The mask length parameter indicates the number of bits used for the network portion of the IP address; the remainder of the IP address is used to determine the host portion of the IP address. Allowed values are integers in the range 0 – 30. Note that a mask length of 32 is reserved for system IP addresses.

\texttt{mask} — The subnet mask in dotted decimal notation. When the IP prefix is not specified in CIDR notation, a space separates the \textit{ip-address} from a traditional dotted decimal mask. The \textit{mask} parameter indicates the complete mask that will be used in a logical ‘AND’ function to derive the local subnet of the IP address. Allowed values are dotted decimal addresses in the range 128.0.0.0 – 255.255.255.252. Note that a mask of 255.255.255.255 is reserved for system IP addresses.

\texttt{netmask} — Specifies a string of 0s and 1s that mask or screen out the network part of an IP address so that only the host computer part of the address remains.

\texttt{broadcast} — The optional \texttt{broadcast} parameter overrides the default broadcast address used by the IP interface when sourcing IP broadcasts on the IP interface. If no broadcast format is specified for the IP address, the default value is \texttt{host-ones} which indicates a subnet broadcast address. Use this parameter to change the broadcast address to \texttt{all-ones} or revert back to a broadcast address of \texttt{host-ones}.

This parameter does not affect the type of broadcasts that can be received by the IP interface. A host sending either the local broadcast (\texttt{all-ones}) or the valid subnet broadcast address (\texttt{host-ones}) will be received by the IP interface. (Default: \texttt{host-ones})

\texttt{all-ones} — The \texttt{all-ones} keyword following the \texttt{broadcast} parameter specifies the broadcast address used by the IP interface for this IP address will be 255.255.255.255, also known as the local broadcast.

\texttt{host-ones} — The \texttt{host-ones} keyword following the \texttt{broadcast} parameter specifies that the broadcast address used by the IP interface for this IP address will be the subnet broadcast address. This is an IP address that corresponds to the local subnet described by the \textit{ip-address} and the \textit{mask-length} or \textit{mask} with all the host bits set to binary one. This is the default broadcast address used by an IP interface.

The \texttt{broadcast} parameter within the \texttt{address} command does not have a negate feature, which is usually used to revert a parameter to the default value. To change the \texttt{broadcast} type to \texttt{host-ones} after being changed to \texttt{all-ones}, the \texttt{address} command must be executed with the \texttt{broadcast} parameter defined.

**allow-directed-broadcasts**

**Syntax**
[no] allow-directed-broadcasts

**Context**
config>service>ies>if

**Description**
This command enables the forwarding of directed broadcasts out of the IP interface.

A directed broadcast is a packet received on a local router interface destined for the subnet broadcast address on another IP interface. The \texttt{allow-directed-broadcasts} command on an IP interface enables or disables the transmission of packets destined to the subnet broadcast address of the egress IP interface.
IES Interface Commands

When enabled, a frame destined to the local subnet on this IP interface will be sent as a subnet broadcast out this interface. Care should be exercised when allowing directed broadcasts as it is a well-known mechanism used for denial-of-service attacks.

When disabled, directed broadcast packets discarded at this egress IP interface will be counted in the normal discard counters for the egress SAP.

By default, directed broadcasts are not allowed and will be discarded at this egress IP interface.

The no form of this command disables the forwarding of directed broadcasts out of the IP interface.

Default no allow-directed-broadcasts — Directed broadcasts are dropped.

anti-spoof

Syntax anti-spoof {ip | mac | ip-mac}

no anti-spoof

Context config>service>ies>if>sap

Description This command enables anti-spoof filtering and optionally changes the anti-spoof matching type for the SAP. The type of anti-spoof filtering defines what information in the incoming packet is used to generate the criteria to lookup an entry in the anti-spoof filter table. The type parameter (ip, ip-mac, nh-mac) defines the anti-spoof filter type enforced by the SAP when anti-spoof filtering is enabled.

The no form of the command disables anti-spoof filtering on the SAP.

Default no anti-spoof

Parameters ip — Configures SAP anti-spoof filtering to use only the source IP address in its lookup. If a static host exists on the SAP without an IP address specified, the anti-spoof type ip command will fail.

mac — Configures SAP anti-spoof filtering to use only the source MAC address in its lookup. Setting the anti-spoof filter type to mac is not allowed on non-Ethernet encapsulated SAPs. If a static host exists on the SAP without a specified MAC address, the anti-spoof type mac command will fail. The anti-spoof type mac command will also fail if the SAP does not support Ethernet encapsulation.

ip-mac — Configures SAP anti-spoof filtering to use both the source IP address and the source MAC address in its lookup. If a static host exists on the SAP without both the IP address and MAC address specified, the anti-spoof type ip-mac command will fail. This is also true if the default anti-spoof filter type of the SAP is ip-mac and the default is not overridden. The anti-spoof type ip-mac command will also fail if the SAP does not support Ethernet encapsulation.

app-profile

Syntax app-profile app-profile-name

no app-profile

Context config>service>ies>if>sap

Description This command configures the application profile name.
Parameters  

app-profile-name — Specifies an existing application profile name configured in the config>app-assure>group>policy context.

arp-timeout

Syntax  

arp-timeout seconds  
no arp-timeout

Context  

config>service>ies>if

Description  

This command configures the minimum time in seconds an ARP entry learned on the IP interface will be stored in the ARP table. ARP entries are automatically refreshed when an ARP request or gratuitous ARP is seen from an IP host, otherwise, the ARP entry is aged from the ARP table. If arp-timeout is set to a value of zero seconds, ARP aging is disabled.

The no form of this command restores arp-timeout to the default value.

Default  

14400 seconds

Parameters  

seconds — The minimum number of seconds a learned ARP entry will be stored in the ARP table, expressed as a decimal integer. A value of zero specifies that the timer is inoperative and learned ARP entries will not be aged.

Values  

0 — 65535

bfd

Syntax  

bfd transmit-interval [receive receive-interval] [multiplier multiplier] [echo-receive echo-interval]

no bfd

Context  

config>service>ies>if  
config>service>ies>if>ipv6

This command specifies the BFD parameters for the associated IP interface. If no parameters are defined the default value are used.

The multiplier specifies the number of consecutive BFD messages that must be missed from the peer before the BFD session state is changed to down and the upper level protocols (OSPF, IS-IS, BGP or PIM) is notified of the fault.

The no form of the command removes BFD from the interface.

Default  

no bfd

Parameters  

transmit-interval — Sets the transmit interval for the BFD session.

Values  

100 — 100000

Default  

100

receive receive-interval — Sets the receive interval for the BFD session.
Values 100 — 100000

Default 100

dmultiplier multiplier — Set the multiplier for the BFD session.
Values 3— 20
Default 3

callin-rvieve echo-interval — Sets the minimum echo receive interval, in milliseconds, for the BFD session.
Values 100 — 100000
Default 100

cflowd

Syntax cflowd {acl | interface} [direction]
no cflowd

Context config>service>ies>if

Description This command enables cflowd to collect traffic flow samples through a router for analysis.
cflowd is used for network planning and traffic engineering, capacity planning, security, application and user profiling, performance monitoring, usage-based billing, and SLA measurement. When cflowd is enabled at the interface level, all packets forwarded by the interface are subjected to analysis according to the cflowd configuration.

If cflowd is enabled without either egress-only or both specified or with the ingress-only keyword specified, then only ingress sampling will be enabled on the associated IP interface.

Default no cflowd

Parameters acl — cflowd configuration associated with a filter.
interface — cflowd configuration associated with an IP interface.
direction — Specifies the direction to collect traffic flow samples.

Values ingress-only — Enables ingress sampling only on the associated interface.
egress-only — Enables egress sampling only on the associated interface.
both — Enables both ingress and egress cflowd sampling.

cpu-protection

Syntax cpu-protection policy-id
no cpu-protection

Context config>service>ies>if
Description
This command assigns an existing CPU protection policy to the associated service interface. For these interface types, the per-source rate limit is not applicable. The CPU protection policies are configured in the config>sys>security>cpu-protection>policy cpu-protection-policy-id context.

If no cpu-protection policy is assigned to a service interface, then the default policy is used to limit the overall-rate. The default policy is policy number 254 for access interfaces and 255 for network interfaces.

The no form of the command removes the association of the CPU protection policy from the associated interface and reverts to the default policy values.

cpu-protection 254 (for access interfaces)
cpu-protection 255 (for network interfaces)
none (for video-interfaces, shown as no cpu-protection in CLI)

The configuration of no cpu-protection returns the interface/SAP to the default policies as shown above.

Parameters

- policy-id — Specifies an existing CPU protection policy.
  - Values 1 — 255

local-proxy-arp

Syntax  

[no] local-proxy-arp

Context  config>service>ies>if

Description  This command enables local proxy ARP. When local proxy ARP is enabled on an IP interface, the system responds to all ARP requests for IP addresses belonging to the subnet with its own MAC address, and thus will become the forwarding point for all traffic between hosts in that subnet. When local-proxy-arp is enabled, ICMP redirects on the ports associated with the service are automatically blocked.

Default  ies>if: no local-proxy-arp

ip-mtu

Syntax  ip-mtu octets
        no ip-mtu

Context  config>service>ies>if

Description  This command configures the IP maximum transmit unit (packet) for this interface.

Note that because this connects a Layer 2 to a Layer 3 service, this parameter can be adjusted under the IES interface.

The MTU that is advertised from the IES size is:

\[ \text{MINIMUM}((\text{SdpOperPathMtu} - \text{EtherHeaderSize}), (\text{Configured ip-mtu})) \]

By default (for ethernet network interface) if no ip-mtu is configured it is \((1568 - 14) = 1554\).

The no form of the command returns the default value.

Default  no ip-mtu
IES Interface Commands

**loopback**

**Syntax**  
[no] loopback

**Context**  
config>service>ies>if

**Description**  
This command specifies that the associated interface is a loopback interface that has no associated physical interface. As a result, the associated IES interface cannot be bound to a SAP.

Note that you can configure an IES interface as a loopback interface by issuing the `loopback` command instead of the `sap` command. The loopback flag cannot be set on an interface where a SAP is already defined and a SAP cannot be defined on a loopback interface.

**Default**  
none

**mac**

**Syntax**  
mac ieee-address  
no mac

**Context**  
config>service>ies>if

**Description**  
This command assigns a specific MAC address to an IES IP interface.

For Routed Central Office (CO), a group interface has no IP address explicitly configured but inherits an address from the parent subscriber interface when needed. For example, a MAC will respond to an ARP request when an ARP is requested for one of the IPs associated with the subscriber interface through the group interface.

The `no` form of the command returns the MAC address of the IP interface to the default value.

**Default**  
The physical MAC address associated with the Ethernet interface that the SAP is configured on (the default MAC address assigned to the interface, assigned by the system).

**Parameters**  
`ieee-address` — Specifies the 48-bit MAC address for the static ARP in the form aa:bb:cc:dd:ee:ff or aa-bb-cc-dd-ee-ff where aa, bb, cc, dd, ee, and ff are hexadecimal numbers. Allowed values are any non-broadcast, non-multicast MAC and non-IEEE reserved MAC addresses.

**monitor-oper-group**

**Syntax**  
monitor-oper-group name  
no monitor-oper-group

**Context**  
config>service>ies>if

**Description**  
This command specifies the operational group to be monitored by the object under which it is configured.

The oper-group name must be already configured under the config>service context before its name is referenced in this command.

The `no` form of the command removes the association from the configuration.

**Default**  
no monitor-oper-group
Parameters

name — Specifies a character string of maximum 32 ASCII characters identifying the group instance.

secondary

Syntax

secondary {ip-address/mask | ip-address netmask} [broadcast all-ones | host-ones] [igp-inhibit]
no secondary ip-address

Context

config>service>ies>if

Description

This command assigns a secondary IP address/IP subnet/broadcast address format to the interface.

Default

none

Parameters

ip-address — The IP address of the IP interface. The ip-address portion of the address command specifies the IP host address that will be used by the IP interface within the subnet. This address must be unique within the subnet and specified in dotted decimal notation. Allowed values are IP addresses in the range 1.0.0.0 – 223.255.255.255 (with support of /31 subnets).

mask — The subnet mask in dotted decimal notation. When the IP prefix is not specified in CIDR notation, a space separates the ip-address from a traditional dotted decimal mask. The mask parameter indicates the complete mask that will be used in a logical ‘AND’ function to derive the local subnet of the IP address. Allowed values are dotted decimal addresses in the range 128.0.0.0 – 255.255.255.252. Note that a mask of 255.255.255.255 is reserved for system IP addresses.

netmask — Specifies a string of 0s and 1s that mask or screen out the network part of an IP address so that only the host computer part of the address remains.

broadcast — The optional broadcast parameter overrides the default broadcast address used by the IP interface when sourcing IP broadcasts on the IP interface. If no broadcast format is specified for the IP address, the default value is host-ones which indicates a subnet broadcast address. Use this parameter to change the broadcast address to all-ones or revert back to a broadcast address of host-ones.

The broadcast format on an IP interface can be specified when the IP address is assigned or changed. This parameter does not affect the type of broadcasts that can be received by the IP interface. A host sending either the local broadcast (all-ones) or the valid subnet broadcast address (host-ones) will be received by the IP interface. (Default: host-ones)

all-ones — The all-ones keyword following the broadcast parameter specifies the broadcast address used by the IP interface for this IP address will be 255.255.255.255, also known as the local broadcast.

host-ones — The host-ones keyword following the broadcast parameter specifies that the broadcast address used by the IP interface for this IP address will be the subnet broadcast address. This is an IP address that corresponds to the local subnet described by the ip-address and the mask-length or mask with all the host bits set to binary one. This is the default broadcast address used by an IP interface.

The broadcast parameter within the address command does not have a negate feature, which is usually used to revert a parameter to the default value. To change the broadcast type to host-ones after being changed to all-ones, the address command must be executed with the broadcast parameter defined.

igp-inhibit — The optional igp-inhibit parameter signals that the given secondary IP interface should not be recognized as a local interface by the running IGP. For OSPF and IS-IS, this means that the specified secondary IP interfaces will not be injected and used as passive interfaces and will not be advertised as
IES Interface Commands

internal IP interfaces into the IGP’s link state database. For RIP, this means that these secondary IP interfaces will not source RIP updates.

static-arp

Syntax  

static-arp ieee-mac-address unnumbered  
no static-arp unnumbered

Context  

config>service>ies>if

Description  

This command configures a static address resolution protocol (ARP) entry associating a subscriber IP address with a MAC address for the core router instance. This static ARP appears in the core routing ARP table. A static ARP can only be configured if it exists on the network attached to the IP interface.

If an entry for a particular IP address already exists and a new MAC address is configured for the IP address, the existing MAC address will be replaced with the new MAC address.

The no form of the command removes a static ARP entry.

Default  

None

Parameters  

ip-address — Specifies the IP address for the static ARP in IP address dotted decimal notation.

ieee-mac-address — Specifies the 48-bit MAC address for the static ARP in the form aa:bb:cc:dd:ee:ff or aa-bb-cc-dd-ee-ff where aa, bb, cc, dd, ee and ff are hexadecimal numbers. Allowed values are any non-broadcast, non-multicast MAC and non-IEEE reserved MAC addresses.

unnumbered — Specifies the static ARP MAC for an unnumbered interface. Unnumbered interfaces support dynamic ARP. Once this command is configured, it overrides any dynamic ARP.

static-tunnel-redundant-next-hop

Syntax  

static-tunnel-redundant-next-hop ip-address  
no static-tunnel-redundant-next-hop

Context  

config>service>ies>if

Description  

This command specifies redundant next-hop address on public or private IPsec interface (with public or private tunnel-sap) for static IPsec tunnel. The specified next-hop address will be used by standby node to shunt traffic to master in case of it receives them.

The next-hop address will be resolved in routing table of corresponding service.

The no form of the command removes the address from the interface configuration.

Default  

none

Parameters  

ip-address — Specifies the static ISA tunnel redundant next-hop address.

teid-load-balancing

Syntax  

[no] teid-load-balancing
Context
config>service>vprn>sub-inf
config>service>vprn>nw-if

Description
This command enables inclusion of TEID in hashing for GTP-U/C encapsulates traffic for GTPv1/GTPv2. The no form of this command ignores TEID in hashing.

Default
disabled

tos-marking-state

Syntax
tos-marking-state \{trusted | untrusted\}
no tos-marking-state

Context
config>service>ies>if

Description
This command is used to change the default trusted state to a non-trusted state. When unset or reverted to the trusted default, the ToS field will not be remarked by egress network IP interfaces unless the egress network IP interface has the remark-trusted state set, in which case the egress network interface treats all IES and network IP interface as untrusted.

When the ingress interface is set to untrusted, all egress network IP interfaces will remark IP packets received on the network interface according to the egress marking definitions on each network interface. The egress network remarking rules also apply to the ToS field of IP packets routed using IGP shortcuts (tunneled to a remote next-hop). However, the tunnel QoS markings are always derived from the egress network QoS definitions.

Egress marking and remarking is based on the internal forwarding class and profile state of the packet once it reaches the egress interface. The forwarding class is derived from ingress classification functions. The profile of a packet is either derived from ingress classification or ingress policing.

The default marking state for network IP interfaces is trusted. This is equivalent to declaring no tos-marking-state on the network IP interface. When undefined or set to tos-marking-state trusted, the trusted state of the interface will not be displayed when using show config or show info unless the detail parameter is given. The save config command will not store the default tos-marking-state trusted state for network IP interfaces unless the detail parameter is also specified.

The no tos-marking-state command is used to restore the trusted state to a network IP interface. This is equivalent to executing the tos-marking-state trusted command.

Default
untrusted for config>service>ies context

Parameters
trusted — The default prevents the ToS field to not be remarked by egress network IP interfaces unless the egress network IP interface has the remark-trusted state set

untrusted — Specifies that all egress network IP interfaces will remark IP packets received on the network interface according to the egress marking definitions on each network interface.
IES Interface Commands

unnumbered

Syntax unnumbered [ip-int-name | ip-address]

no unnumbered

Context config>service>ies>if

Description This command configures the interface as an unnumbered interface. Unnumbered IP interfaces are supported on a SONET/SDH access port with the PPP, ATM, Frame Relay, cisco-HDLC encapsulation. It is not supported on access ports that do not carry IP traffic, but are used for native TDM circuit emulation.

Parameters ip-int-name — Specifies the name of an IP interface. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

ip-address — Specifies an IP address.

urpf-check

Syntax [no] urpf-check

Context config>service>ies>if
config>service>ies>if>ipv6

Description This command enables unicast RPF (uRPF) Check on this interface.
The no form of the command disables unicast RPF (uRPF) Check on this interface.

Default disabled

mode

Syntax mode {strict | loose | strict-no-ecmp}

no mode

Context config>service>ies>if>urfp-check

Description This command specifies the mode of unicast RPF check.
The no form of the command reverts to the default (strict) mode.

Default strict

Parameters strict — When specified, uRPF checks whether incoming packet has a source address that matches a prefix in the routing table, and whether the interface expects to receive a packet with this source address prefix.

loose — In loose mode, uRPF checks whether incoming packet has source address with a corresponding prefix in the routing table. However, the loose mode does not check whether the interface expects to receive a packet with a specific source address prefix. This object is valid only when urpf-check is enabled.

strict-no-ecmp — When a packet is received on an interface in this mode and the SA matches an ECMP route the packet is dropped by uRPF.
proxy-arp-policy

**Syntax**

```
[no] proxy-arp policy-name [policy-name...(up to 5 max)]
```

**Context**

```
config>service>ies>if
```

**Description**

This command configures a proxy ARP policy for the interface.

The no form of this command disables the proxy ARP capability.

**Parameters**

- `policy-name` — The export route policy name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes. The specified name(s) must already be defined.

ptp-hw-assist

**Syntax**

```
[no] ptp-hw-assist
```

**Context**

```
config>service>ies>if
```

**Description**

This command configures the 1588 port based timestamping assist function for the interface. This capability is supported on a specific set of hardware. The command may be blocked if not all hardware has the required level of support.

Only one interface per physical port can have ptp-hw-assist enabled.

```
no ptp-hw-assist
```

qos-route-lookup

**Syntax**

```
qos-route-lookup [source | destination]
```

```
no qos-route-lookup
```

**Context**

```
config>service>ies>if
config>service>ies>if>ipv6
```

**Description**

This command enables QoS classification of the ingress IP packets on an interface based on the QoS information associated with routes in the forwarding table.

If the optional `destination` parameter is specified and the destination address of an incoming IP packet matches a route with QoS information the packet is classified to the fc and priority associated with that route, overriding the fc and priority/profile determined from the sap-ingress or network qos policy associated with the IP interface. If the destination address of the incoming packet matches a route with no QoS information the fc and priority of the packet remain as determined by the sap-ingress or network qos policy.
If the optional **source** parameter is specified and the source address of an incoming IP packet matches a route with QoS information the packet is classified to the fc and priority associated with that route, overriding the fc and priority/profile determined from the sap-ingress or network qos policy associated with the IP interface. If the source address of the incoming packet matches a route with no QoS information the fc and priority of the packet remain as determined by the sap-ingress or network qos policy.

If neither the optional **source** or **destination** parameter is present, then the default is **destination** address matching.

The functionality enabled by the `qos-route-lookup` command can be applied to IPv4 packets or IPv6 packets on an interface, depending on whether it is present at the interface context (applies to IPv4) or the `interface>ipv6` context (applies to IPv6). The ability to specify source address based QoS lookup is not supported for IPv6. Subscriber management group interfaces also do not support the source QPPB option.

The **no** form of the command reverts to the default.

**Default**

destination

**Parameters**

**source** — Enables QoS classification of incoming IP packets based on the source address matching a route with QoS information.

**destination** — Enables QoS classification of incoming IP packets based on the destination address matching a route with QoS information.

tcp-mss

**Syntax**

tcp-mss mss-value

**no tcp-mss**

**Context**

config>service>ies>if
config>service>ies>if>ipv6

**Description**

This command allows the TCP MSS value used for TCP connections associated with the IPv4 or IPv6 interface to be set to a static value instead of being determined by the IP MTU value. The configured TCP MSS value will only be used for future TCP connections associated with the IPv4 or IPv6 interface, existing TCP connections are not affected by the static value.

The **no** form of the command removed the static MSS configuration and all future TCP connection will use a calculated MSS value based on the IP interface MTU.

**Default**

**no tcp-mss**

**Parameters**

**mss-value** — The TCP MSS value that should be used in the TCP SYN packet during the three-way handshake negotiation of a TCP connection.

**Values**

- 384 - 9158 (IPv4)
- 1220 - 9138 (IPv6)
remote-proxy-arp

Context  config>service>ies>if

Description  This command enables remote proxy ARP on the interface.
Remote proxy ARP is similar to proxy ARP. It allows the router to answer an ARP request on an interface for a subnet that is not provisioned on that interface. This allows the router to forward to the other subnet on behalf of the requester. To distinguish remote proxy ARP from local proxy ARP, local proxy ARP performs a similar function but only when the requested IP is on the receiving interface.

Default  no remote-proxy-arp

Values

host-lockout-policy

Syntax  host-lockout-policy policy-name
   no host-lockout-policy

Context  config>service>ies>if>sap

Description  This command configures a host lockout policy.
The no form of the command removes the policy name from the configuration.

host-shutdown

Syntax  [no] host-shutdown

Context  config>service>ies>if>sap

Description  This command administratively enables host creation on this SAP.

ip-tunnel

Syntax  ip-tunnel name [create]
   no ip-tunnel name

Context  config>service>ies>if>sap

Description  This command is used to configure an IP-GRE or IP-IP tunnel and associate it with a private tunnel SAP within an IES or VPRN service.
The no form of the command deletes the specified IP/GRE or IP-IP tunnel from the configuration. The tunnel must be administratively shutdown before issuing the no ip-tunnel command.

Default  No IP tunnels are defined.
IES Interface Commands

Parameters  

**ip-tunnel-name** — Specifies the name of the IP tunnel. Tunnel names can be from 1 to 32 alphanumeric characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

flowspec

**Syntax**  

[no] flowspec

**Context**  

config>service>ies>if>sap>ingress

**Description**  

This command enables flowspec filtering on an IP interface of the base router. Filtering is based on all of the flowspec routes that have been received and accepted by the base router. Ingress traffic on an IP interface can be filtered by both a user-defined ip filter and flowspec. In this case, the user-defined ip filter entries are evaluated before the flowspec routes and the default action of the user-defined ip filter applies as the very last rule.

The no form of the command removes flowspec filtering from an IP interface.

**Default**  

No interfaces have flowspec enabled.
IES Interface ICMP Commands

icmp

Syntax     icmp
Context    config>service>ies>if
Description This command enables the context to configure Internet Control Message Protocol (ICMP) parameters on an IES service

mask-reply

Syntax     [no] mask-reply
Context    config>service>ies>if>icmp
Description This command enables responses to Internet Control Message Protocol (ICMP) mask requests on the router interface.

If a local node sends an ICMP mask request to the router interface, the mask-reply command configures the router interface to reply to the request.

By default, the router instance will reply to mask requests.

The no form of this command disables replies to ICMP mask requests on the router interface.

Default    mask-reply — Reply to ICMP mask requests.

redirects

Syntax     redirects [number seconds]
no redirects

Context    config>service>ies>if>icmp
Description This command configures the rate for Internet Control Message Protocol (ICMP) redirect messages issued on the router interface.

When routes are not optimal on this router and another router on the same subnetwork has a better route, the router can issue an ICMP redirect to alert the sending node that a better route is available.

The redirects command enables the generation of ICMP redirects on the router interface. The rate at which ICMP redirects is issued can be controlled with the optional number and seconds parameters by indicating the maximum number of redirect messages that can be issued on the interface for a given time interval.

By default, generation of ICMP redirect messages is enabled at a maximum rate of 100 per 10 second time interval. (Default: redirects 100 10)

The no form of this command disables the generation of icmp redirects on the router interface.
IES Interface Commands

Default redirects **100 10** — Maximum of 100 redirect messages in 10 seconds

Parameters

- **number** — The maximum number of ICMP redirect messages to send. This parameter must be specified with the **seconds** parameter.
  - **Values**: 10 — 1000

- **seconds** — The time frame in seconds used to limit the **number** of ICMP redirect messages that can be issued.
  - **Values**: 1 — 60

### ttl-expired

**Syntax**

ttl-expired **number** **seconds**

no ttl-expired

**Context**

config>service>ies>if>icmp

**Description**

This command configures the rate Internet Control Message Protocol (ICMP) TTL expired messages are issued by the IP interface.

By default, generation of ICMP TTL expired messages is enabled at a maximum rate of 100 per 10 second time interval.

The no form of this command disables the limiting the rate of TTL expired messages on the router interface.

**Default**

ttl-expired 100 10

**Parameters**

- **number** — The maximum number of ICMP TTL expired messages to send, expressed as a decimal integer. This parameter must be specified with the **seconds** parameter.
  - **Values**: 10 — 1000

- **seconds** — The time frame in seconds used to limit the **number** of ICMP TTL expired messages that can be issued, expressed as a decimal integer.
  - **Values**: 1 — 60

### unreachables

**Syntax**

unreachables **[number seconds]**

no unreachables

**Context**

config>service>ies>if>icmp

**Description**

This command configures the rate for ICMP host and network destination unreachable messages issued on the router interface.

The **unreachables** command enables the generation of ICMP destination unreachables on the router interface. The rate at which ICMP unreachables is issued can be controlled with the optional **number** and **time** parameters by indicating the maximum number of destination unreachable messages which can be issued on the interface for a given time interval.

By default, generation of ICMP destination unreachable messages is enabled at a maximum rate of 10 per 60
second time interval.

The no form of this command disables the generation of icmp destination unreachable messages on the router interface.

**Default**

unreachables 100 10

**Parameters**

*number* — The maximum number of ICMP unreachable messages to send. This parameter must be specified with the *seconds* parameter.

**Values**

10 — 1000

*seconds* — The time frame in seconds used to limit the *number* of ICMP unreachable messages that can be issued.

**Values**

1 — 60

### if-attribute

**Syntax**

if-attribute

**Context**

config>router
config>router>interface
config>service>ies>interface
config>service>vprn>interface

**Description**

This command creates the context to configure or apply IP interface attributes such as administrative group (admin-group) or Shared Risk Loss Group (SRLG).

### admin-group

**Syntax**

admin-group group-name [group-name...up to 5 max]

no admin-group group-name [group-name...up to 5 max]

**Context**

config>router>interface>if-attribute
config>service>ies>interface>if-attribute
config>service>vprn>interface>if-attribute
config>router>mpls>interface

**Description**

This command configures the admin group membership of an interface. The user can apply admin groups to an IES, VPRN, network IP, or MPLS interface.

Each single operation of the admin-group command allows a maximum of five (5) groups to be specified at a time. However, a maximum of 32 groups can be added to a given interface through multiple operations. Once an admin group is bound to one or more interface, its value cannot be changed until all bindings are removed.

The configured admin-group membership will be applied in all levels/areas the interface is participating in. The same interface cannot have different memberships in different levels/areas.
It should be noted that only the admin groups bound to an MPLS interface are advertised in TE link TLVs and sub-TLVs when the **traffic-engineering** option is enabled in IS-IS or OSPF. IES and VPRN interfaces do not have their attributes advertised in TE TLVs.

The **no** form of this command deletes one or more of the admin-group memberships of an interface. The user can also delete all memberships of an interface by not specifying a group name.

**Parameters**

*group-name* — Specifies the name of the group with up to 32 characters. The association of group name and value should be unique within an IP/MPLS domain.

### srlg-group

**Syntax**

```mermaid
srlg-group group-name [group-name...(up to 5 max)]
no srlg-group group-name [group-name...(up to 5 max)]
no srlg-group
```

**Context**

```
config>router>interface>if-attribute
config>service>ies>interface>if-attribute
config>service>vprn>interface>if-attribute
config>router>mpls>interface
```

**Description**

This command configures the SRLG membership of an interface. The user can apply SRLGs to an IES, VPRN, network IP, or MPLS interface.

An interface can belong to up to 64 SRLG groups. However, each single operation of the **srlg-group** command allows a maximum of five (5) groups to be specified at a time. Once an SRLG group is bound to one or more interface, its value cannot be changed until all bindings are removed.

The configured SRLG membership will be applied in all levels/areas the interface is participating in. The same interface cannot have different memberships in different levels/areas.

It should be noted that only the SRLGs bound to an MPLS interface are advertised in TE link TLVs and sub-TLVs when the **traffic-engineering** option is enabled in IS-IS or OSPF. IES and VPRN interfaces do not have their attributes advertised in TE TLVs.

The **no** form of this command deletes one or more of the SRLG memberships of an interface. The user can also delete all memberships of an interface by not specifying a group name.

**Parameters**

*group-name* — Specifies the name of the group, up to 32 characters. The association of group name and value should be unique within an IP/MPLS domain.
IES Interface IPv6 Commands

ipv6

Syntax

    [no] ipv6

Context

    config>service>ies>if

Description

    This command enables the context to configure IPv6 for an IES interface.

default address

Syntax

    address ipv6-address/prefix-length [eui-64]
    no address ipv6-address/prefix-length

Context

    config>service>ies>if>ipv6

Description

    This command assigns an IPv6 address to the IES interface.

Parameters

    ipv6-address/prefix-length — Specify the IPv6 address on the interface.

Values

    ipv6-address/prefix: ipv6-address  x:x:x:x:x:x:x:x:x (eight 16-bit pieces)
    x:x:x:x:x:x:d.d.d
    x [0 — FFFF]H
    d [0 — 255]D
    prefix-length 1 — 128

eui-64 — When the eui-64 keyword is specified, a complete IPv6 address from the supplied
prefix and 64-bit interface identifier is formed. The 64-bit interface identifier is derived from
MAC address on Ethernet interfaces. For interfaces without a MAC address, for example ATM
interfaces, the Base MAC address of the chassis is used.

icmp6

Syntax

    icmp6

Context

    config>service>ies>if>ipv6

Description

    This command configures ICMPv6 parameters for the IES interface.

classic packet-too-big

Syntax

    packet-too-big [number seconds]
    no packet-too-big

Context

    config>service>ies>if>ipv6>icmp6
IES Interface Commands

### Description
This command specifies whether “packet-too-big” ICMPv6 messages should be sent. When enabled, ICMPv6 “packet-too-big” messages are generated by this interface.

The **no** form of the command disables the sending of ICMPv6 “packet-too-big” messages.

**Default** 100 10

### Parameters

- **number** — Specifies the number of “packet-too-big” ICMPv6 messages to send in the time frame specified by the **seconds** parameter.
  - **Values** 10 — 1000
  - **Default** 100

- **seconds** — Specifies the time frame in seconds that is used to limit the number of “packet-too-big” ICMPv6 messages issued.
  - **Values** 1 — 60
  - **Default** 10

---

### param-problem

**Syntax** `param-problem [number seconds]`

- **no packet-too-big**

**Context** `config>service>ies>if>ipv6>icmp6`

**Description**
This command specifies whether “parameter-problem” ICMPv6 messages should be sent. When enabled, “parameter-problem” ICMPv6 messages are generated by this interface.

The **no** form of the command disables the sending of “parameter-problem” ICMPv6 messages.

**Default** 100 10

- **number** — Specifies the number of “parameter-problem” ICMPv6 messages to send in the time frame specified by the **seconds** parameter.
  - **Values** 10 — 1000
  - **Default** 100

- **seconds** — Specifies the time frame in seconds that is used to limit the number of “parameter-problem” ICMPv6 messages issued.
  - **Values** 1 — 60
  - **Default** 10

---

### redirects

**Syntax** `redirects [number seconds]`

- **no redirects**

**Context** `config>service>ies>if>ipv6>icmp6`

---

Page 1130 7950 SR OS Services Guide
This command configures ICMPv6 redirect messages. When enabled, ICMPv6 redirects are generated when routes are not optimal on this router and another router on the same subnetwork has a better route in order to alert that node that a better route is available.

When disabled, ICMPv6 redirects are not generated.

**Default**

100 10

- **number** — Specifies the number of version 6 redirects are to be issued in the time frame specified by the **seconds** parameter.
  - **Values** 10 — 1000
  - **Default** 100

- **seconds** — Specifies the time frame in seconds that is used to limit the number of version 6 redirects issued.
  - **Values** 1 — 60
  - **Default** 10

---

This command specifies whether “time-exceeded” ICMPv6 messages should be sent. When enabled, ICMPv6 “time-exceeded” messages are generated by this interface.

When disabled, ICMPv6 “time-exceeded” messages are not sent.

**Default**

100 10

- **number** — Specifies the number of “time-exceeded” ICMPv6 messages are to be issued in the time frame specified by the **seconds** parameter.
  - **Values** 10 — 1000
  - **Default** 100

- **seconds** — Specifies the time frame in seconds that is used to limit the number of “time-exceeded” ICMPv6 message to be issued.
  - **Values** 1 — 60
  - **Default** 10

---

This command configures ICMPv6 unreachable messages. When enabled, ICMPv6 unreachable messages are generated when a destination node is not reachable.

When disabled, ICMPv6 unreachable messages are not generated.

**Default**

100 10

- **number** — Specifies the number of ICMPv6 unreachable messages are to be issued in the time frame specified by the **seconds** parameter.
  - **Values** 10 — 1000
  - **Default** 100

- **seconds** — Specifies the time frame in seconds that is used to limit the number of ICMPv6 unreachable message to be issued.
  - **Values** 1 — 60
  - **Default** 10
IES Interface Commands

**Description**  
This command specifies that ICMPv6 host and network unreachable messages are generated by this interface.

When disabled, ICMPv6 host and network unreachable messages are not sent.

**Default**  
100 10

- **number** — Specifies the number of destination unreachable ICMPv6 messages are issued in the time frame specified by the `seconds` parameter.
  - **Values** 10 — 1000
  - **Default** 100

- **seconds** — Specifies the time frame in seconds that is used to limit the number of destination unreachable ICMPv6 messages to be issued.
  - **Values** 1 — 60
  - **Default** 10

---

**local-proxy-nd**

**Syntax**  
[no] local-proxy-nd

**Context**  
config>service>ies>if>ipv6

**Description**  
This command enables local proxy neighbor discovery on the interface.

The `no` form of the command disables local proxy neighbor discovery.

---

**proxy-nd-policy**

**Syntax**  
proxy-nd-policy policy-name [policy-name...(up to 5 max)]

- **no proxy-nd-policy**

**Context**  
config>service>ies>if>ipv6

**Description**  
This command applies a proxy neighbor discovery policy for the interface.

**Parameters**  
- **policy-name** — Specifies an existing neighbor discovery policy name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes. The specified policy name(s) must already be defined.

---

**neighbor**

**Syntax**  
neighbor ipv6-address mac-address

- **no neighbor ipv6-address**

**Context**  
config>service>ies>if>ipv6
**backup**

**Syntax**

```
[no] backup ip-address
```

**Context**

`config>service>ies>if>ipv6>vrrp`

**Description**

This command configures virtual router IP addresses for the interface.

**init-delay**

**Syntax**

```
init-delay seconds
no init-delay
```

**Context**

`config>service>ies>if>ipv6>vrrp`

**Description**

This command configures a VRRP initialization delay timer.

**Default**

`no init-delay`

**Parameters**

- `seconds` — Specifies the initialization delay timer for VRRP, in seconds.

**Values**

`1 — 65535`

**mac**

**Syntax**

```
mac mac-address
no mac
```

**Context**

`config>service>ies>if>ipv6>vrrp`

**Description**

This command assigns a specific MAC address to an IES IP interface.

The `no` form of the command returns the MAC address of the IP interface to the default value.

**Default**

The physical MAC address associated with the Ethernet interface that the SAP is configured on (the default
MAC address assigned to the interface, assigned by the system).

**Parameters**

- **mac-address** — Specifies the 48-bit MAC address for the static ARP in the form aa:bb:cc:dd:ee:ff or aa-bb-cc-dd-ee-ff where aa, bb, cc, dd, ee, and ff are hexadecimal numbers. Allowed values are any non-broadcast, non-multicast MAC and non-IEEE reserved MAC addresses.

**master-int-inherit**

**Syntax**

```
[no] master-int-inherit
```

**Context**

`config>service>ies>if>ipv6>vrrp`

**Description**

This command allows the master instance to dictate the master down timer (non-owner context only).

**Default**

`no master-int-inherit`

**message-interval**

**Syntax**

```
message-interval {[seconds] [milliseconds milliseconds]}
```

**no message-interval**

**Context**

`config>service>ies>if>ipv6>vrrp`

**Description**

This command sets the advertisement timer and indirectly sets the master down timer on the virtual router instance. The message-interval setting must be the same for all virtual routers participating as a virtual router. Any VRRP advertisement message received with an Advertisement Interval field different than the virtual router instance configured message-interval value will be silently discarded.

The message-interval command is available in both non-owner and owner `vrrp virtual-router-id nodal` contexts. If the message-interval command is not executed, the default message interval of 1 second will be used.

The **no** form of this command restores the default message interval value of 1 second to the virtual router instance.

**Parameters**

- **seconds** — The number of seconds that will transpire before the advertisement timer expires.
  - **Values**
    - `1 — 255`
  - **Default**
    - `1`

- **milliseconds milliseconds** — Specifies the time interval, in milliseconds, between sending advertisement messages.
  - **Values**
    - `100 — 900`

**ping-reply**

**Syntax**

```
[no] ping-reply
```

**Context**

`config>service>ies>if>ipv6>vrrp`
**Description**
This command enables the non-owner master to reply to ICMP echo requests directed at the virtual router instances IP addresses. The ping request can be received on any routed interface.

Ping must not have been disabled at the management security level (either on the parental Ip interface or based on the ping source host address). When ping-reply is not enabled, icmp Echo Requests to non-owner master virtual IP addresses are silently discarded.

Non-owner backup virtual routers never respond to ICMP echo requests regardless of the setting of ping-reply configuration.

The ping-reply command is only available in non-owner **vrrp** virtual-router-id nodal context. If the ping-reply command is not executed, ICMP echo requests to the virtual router instance IP addresses will be silently discarded.

The **no** form of this command restores the default operation of discarding all ICMP echo request messages destined to the non-owner virtual router instance IP addresses.

**Default**
no ping-reply

---

**policy**

**Syntax**
```
policy vrrp-policy-id
no policy
```

**Context**
config>service>ies>if>ipv6>vrrp

**Description**
This command creates VRRP control policies. The VRRP policy ID must be created by the policy command prior to association with the virtual router instance.

The policy command provides the ability to associate a VRRP priority control policy to a virtual router instance. The policy may be associated with more than one virtual router instance. The priority events within the policy either override or diminish the base-priority dynamically affecting the in-use priority. As priority events clear in the policy, the in-use priority may eventually be restored to the base-priority value.

The policy command is only available in the non-owner **vrrp** virtual-router-id nodal context. The priority of owner virtual router instances is permanently set to 255 and cannot be changed by VRRP priority control policies. For non-owner virtual router instances, if the policy command is not executed, the base-priority will be used as the in-use priority.

The **no** form of this command removes any existing VRRP priority control policy association from the virtual router instance. All such associations must be removed prior to the policy being deleted from the system.

**Default**
None

**Parameters**
```
vrrp-policy-id — The vrrp-policy-id parameter associated the corresponding VRRP priority control policy-id with the virtual router instance. The vrrp-policy-id must already exist in the system for the policy command to be successful.
```

**Values**
1 to 9999
IES Interface Commands

preempt

Syntax  [no] preempt

Context  config>service>ies>if>ipv6>vrrp

Description  The preempt command provides the ability of overriding an existing non-owner master to the virtual router instance. Enabling preempt mode is almost required for proper operation of the base-priority and vrrp-policy-id definitions on the virtual router instance. If the virtual router cannot preempt an existing non-owner master, the affect of the dynamic changing of the in-use priority is greatly diminished.

The preempt command is only available in the non-owner vrrp virtual-router-id nodal context. The owner may not be preempted due to the fact that the priority of non-owners can never be higher than the owner. The owner will always preempt all other virtual routers when it is available.

Non-owner virtual router instances will only preempt when preempt is set and the current master has an in-use message priority value less than the virtual router instances in-use priority.

A master non-owner virtual router will only allow itself to be preempted when the incoming VRRP Advertisement message Priority field value is one of the following:

- Greater than the virtual router in-use priority value
- Equal to the in-use priority value and the source IP address (primary IP address) is greater than the virtual router instance primary IP address

The no form of this command prevents a non-owner virtual router instance from preempting another, less desirable virtual router. Use the preempt command to restore the default mode.

Default  preempt

priority

Syntax  priority base-priority

no priority

Context  config>service>ies>if>ipv6>vrrp

Description  The priority command provides the ability to configure a specific priority value to the virtual router instance. In conjunction with an optional policy command, the base-priority is used to derive the in-use priority of the virtual router instance.

The priority command is only available in the non-owner vrrp virtual-router-id nodal context. The priority of owner virtual router instances is permanently set to 255 and cannot be changed. For non-owner virtual router instances, if the priority command is not executed, the base-priority will be set to 100.

The no form of this command restores the default value of 100 to base-priority.

Parameters  base-priority — The base-priority parameter configures the base priority used by the virtual router instance. If a VRRP Priority Control policy is not also defined, the base-priority will be the in-use priority for the virtual router instance.

Values  1 — 254

Default  100
standby-forwarding

Syntax  
[no] standby-forwarding

Context  
config>service>ies>if>ipv6>vrrp

Description  
This command allows the forwarding of packets by a standby router.

The no form of the command specifies that a standby router should not forward traffic sent to virtual router's MAC address. However, the standby router should forward traffic sent to the standby router’s real MAC address.

Default  
no standby-forwarding

telnet-reply

Syntax  
[no] telnet-reply

Context  
config>service>ies>if>ipv6>vrrp

Description  
This command enables the non-owner master to reply to TCP port 23 Telnet requests directed at the virtual router instances IP addresses. The Telnet request can be received on any routed interface. Telnet must not have been disabled at the management security level (either on the parental IP interface or based on the Telnet source host address). Proper login and CLI command authentication is still enforced.

When telnet-reply is not enabled, TCP port 23 Telnet packets to non-owner master virtual IP addresses are silently discarded.

Non-owner backup virtual routers never respond to Telnet requests regardless of the telnet-reply configuration.

The telnet-reply command is only available in non-owner VRRP nodal context. If the telnet-reply command is not executed, Telnet packets to the virtual router instance IP addresses will be silently discarded.

The no form of this command restores the default operation of discarding all Telnet packets destined to the non-owner virtual router instance IP addresses.

Default  
no telnet-reply

traceroute-reply

Syntax  
[no] traceroute-reply

Context  
config>service>ies>if>ipv6>vrrp

Description  
This command is valid only if the VRRP virtual router instance associated with this entry is a non-owner.

When this command is enabled, a non-owner master can reply to traceroute requests directed to the virtual router instance IP addresses.

A non-owner backup virtual router never responds to such traceroute requests regardless of the trace-route-reply status.
IES Interface Commands

**Default**
no traceroute-reply
IES Spoke SDP Commands

spoke-sdp

Syntax
[no] spoke-sdp sdp-id[:vc-id] [vc-type {ether | ipipe}] [create]

Context
config>service>ies>if

Description
This command binds a service to an existing Service Distribution Point (SDP).

A spoke SDP is treated like the equivalent of a traditional bridge “port” where flooded traffic received on the spoke SDP is replicated on all other “ports” (other spoke and mesh SDPs or SAPs) and not transmitted on the port it was received.

The SDP has an operational state which determines the operational state of the SDP within the service. For example, if the SDP is administratively or operationally down, the SDP for the service will be down.

The SDP must already be defined in the config>service>sdp context in order to associate an SDP with an IES service. If the sdp sdp-id is not already configured, an error message is generated. If the sdp-id does exist, a binding between that sdp-id and the service is created.

SDPs must be explicitly associated and bound to a service. If an SDP is not bound to a service, no far-end devices can participate in the service.

The no form of this command removes the SDP binding from the service. The SDP configuration is not affected; only the binding of the SDP to a service. Once removed, no packets are forwarded to the far-end router. The spoke SDP must be shut down first before it can be deleted from the configuration.

Default
No sdp-id is bound to a service.

SpecCases
IES — At most, only one sdp-id can be bound to an IES service.

Parameters
sdp-id — The SDP identifier. Allowed values are integers in the range of 1 and 17407 for existing SDPs.

vc-id — The virtual circuit identifier.

Values
1 — 4294967295

vc-type — The encapsulation and pseudowire type for the spoke-sdp.

Values
ether : Specifies Ethernet pseudowire as the type of virtual circuit (VC) associated with the SDP binding.

ipipe : Specifies Ipipe pseudowire as the type of virtual circuit (VC) associated with the SDP binding.

Default
ether

egress

Syntax
egress

Context
config>service>ies>>if>spoke-sdp

Description
This command configures the egress SDP context.
IES Interface Commands

**QoS**

**Syntax**
```
qos network-policy-id port-redirect-group queue-group-name [instance instance-id]
no qos [network-policy-id]
```

**Context**
```
configure>service>apipe>spoke-sdp>egress
configure>service>cpipe>spoke-sdp>egress
configure>service>epipe>spoke-sdp>egress
configure>service>fpipe>spoke-sdp>egress
configure>service>ipipe>spoke-sdp>egress
configure>service>vpls>spoke-sdp>egress
configure>service>vpls>mesh-sdp>egress
configure>service>pw-template>egress
configure>service>vprn>interface>spoke-sdp>egress
configure>service>ies>interface>spoke-sdp>egress
```

**Description**
This command is used to redirect pseudowire packets to an egress port queue-group for the purpose of shaping.

The egress pseudowire shaping provisioning model allows the mapping of one or more pseudowires to the same instance of queues, or policers and queues, which are defined in the queue-group template.

Operationally, the provisioning model consists of the following steps:

1. Create an egress queue-group template and configure queues only or policers and queues for each FC that needs to be redirected.
2. Apply the queue-group template to the network egress context of all ports where there exists a network IP interface on which the pseudowire packets can be forwarded. This creates one instance of the template on the egress of the port. One or more instances of the same template can be created.
3. Configure FC-to-policer or FC-to-queue mappings together with the redirect to a queue-group in the egress context of a network QoS policy. No queue-group name is specified in this step, which means the same network QoS policy can redirect different pseudowires to different queue-group templates.
4. Apply this network QoS policy to the egress context of a spoke-SPD inside a service or to the egress context of a pseudowire template and specify the redirect queue-group name.

One or more spoke-SPDs can have their FCs redirected to use queues only or queues and policers in the same queue-group instance.

The following are the constraints and rules of this provisioning model:

1. When a pseudowire FC is redirected to use a queue or a policer and a queue in a queue-group and the queue-group name does not exist, the association is failed at the time the user associates the egress context of a spoke-SPD to the named queue-group. In such a case, the pseudowire packet will be fed directly to the corresponding egress queue for that FC used by the IP network interface on which the pseudowire packet is forwarded. This queue can be a queue-group queue, or the egress shared queue for that FC defined in the network-queue policy applied to the egress of this port. This is the existing implementation and default behavior for a pseudowire packet.
2. When a pseudowire FC is redirected to use a queue or a policer, and a queue in a queue-group and the queue-group name exists, but the policer-id and/or the queue-id is not defined in the queue-group template, the association is failed at the time the user associates the egress context of a
spoke-SPD to the named queue-group. In such a case, the pseudowire packet will be fed directly to the corresponding egress queue for that FC used by the IP network interface the pseudowire packet is forwarded on.

3. When a pseudowire FC is redirected to use a queue, or a policer and a queue in a queue-group, and the queue-group name exists and the policer-id or policer-id plus queue-id exist, it is not required to check that an instance of that queue-group exists in all egress network ports which have network IP interfaces. The handling of this is dealt with in the data path as follows:
   a. When a pseudowire packet for that FC is forwarded and an instance of the referenced queue-group name exists on that egress port, the packet is processed by the queue-group policer and will then be fed to the queue-group queue.
   b. When a pseudowire packet for that FC is forwarded and an instance of the referenced queue-group name does not exist on that egress port, the pseudowire packet will be fed directly to the corresponding egress shared queue for that FC defined in the network-queue policy applied to the egress of this port.

4. If a network QoS policy is applied to the egress context of a pseudowire, any pseudowire FC, which is not explicitly redirected in the network QoS policy, will have the corresponding packets feed directly the corresponding the egress shared queue for that FC defined in the network-queue policy applied to the egress of this port.

When the queue-group name the pseudowire is redirected to exists and the redirection succeeds, the marking of the packet DEI/dot1.p/DSCP and the tunnel DEI/dot1.p/DSCP/EXP is performed; according to the relevant mappings of the (FC, profile) in the egress context of the network QoS policy applied to the pseudowire. This is true regardless, whether an instance of the queue-group exists or not on the egress port to which the pseudowire packet is forwarded. If the packet profile value changed due to egress child policer CIR profiling, the new profile value is used to mark the packet DEI/dot1.p and the tunnel DEI/dot1.p/EXP, but the DSCP is not modified by the policer operation.

When the queue-group name the pseudowire is redirected does not exist, the redirection command is failed. In this case, the marking of the packet DEI/dot1.p/DSCP and the tunnel DEI/dot1.p/DSCP/EXP fields is performed according to the relevant commands in the egress context of the network QoS policy applied to the network IP interface to which the pseudowire packet is forwarded.

The no version of this command removes the redirection of the pseudowire to the queue-group.

**Parameters**

*network-policy-id* — Specifies the network policy identification. The value uniquely identifies the policy on the system.

**Values**  
1 — 65535

*queue-redirect-group queue-group-name* — This optional parameter specifies that the queue-group-name will be used for all egress forwarding class redirections within the network QoS policy ID. The specified queue-group-name must exist as a port egress queue group on the port associated with the IP interface.

*egress-instance instance-id* — Specifies the identification of a specific instance of the queue-group.

**Values**  
1 — 16384
IES Interface Commands

vc-label

**Syntax**

```plaintext
[no] vc-label egress-vc-label
```

**Context**

```
config>service>ies>if>spoke-sdp>egress
```

**Description**

This command configures the static MPLS VC label used by this device to send packets to the far-end device in this service via this SDP.

**Parameters**

- `egress-vc-label` — A VC egress value that indicates a specific connection.

  **Values**

<table>
<thead>
<tr>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>16</td>
</tr>
<tr>
<td>1048575</td>
</tr>
</tbody>
</table>

hash-label

**Syntax**

```plaintext
hash-label [signal-capability]
```

**Context**

```
config>service>ies>if>spoke-sdp
```

**Description**

This command enables the use of the hash label on a VLL, VPLS, or VPRN service bound to LDP or RSVP SDP as well as to a VPRN service using the autobind mode with the with the ldp, rsvp-te, or mpls options. This feature is not supported on a service bound to a GRE SDP or for a VPRN service using the autobind mode with the gre option.

When this feature is enabled, the ingress data path is modified such that the result of the hash on the packet header is communicated to the egress data path for use as the value of the label field of the hash label. The egress data path appends the hash label at the bottom of the stack (BoS) and sets the S-bit to 1 to indicate that.

In order to allow for applications whereby the egress LER infers the presence of the hash label implicitly from the value of the label, the Most Significant Bit (MSB) of the result of the hash is set before copying into the hash label. This means that the value of the hash label will always be in the range [524,288 — 1,048,575] and will not overlap with the signaled/static LSP and signaled/static service label ranges. This also guarantees that the hash label will not match a value in the reserved label range.

The (unmodified) result of the hash continues to be used for the purpose of ECMP and LAG spraying of packets locally on the ingress LER. Note however that for VLL services, the result of the hash is overwritten and the ECMP and LAG spraying will be based on service-id when ingress SAP shared queuing is not enabled. However, the hash label will still reflect the result of the hash such that an LSR can use it to perform fine grained load balancing of VLL pseudowire packets.

Packets that are generated in CPM and forwarded labeled within the context of a service (for example, OAM packets) must also include a hash label at the BoS and set the S-bit accordingly.

The TTL of the hash label is set to a value of 0.

The user enables the signaling of the hash-label capability under a VLL spoke-sdp, a VPLS spoke-sdp or mesh-sdp, or an IES/VPRN spoke interface by adding the `signal-capability` option. In this case, the decision whether to insert the hash label on the user and control plane packets by the local PE is solely determined by the outcome of the signaling process and can override the local PE configuration. The following are the procedures:

- The local PE will insert the flow label interface parameters sub-TLV with F=1 in the PW ID FEC element in the label mapping message for that spoke-sdp or mesh-sdp.
• If the remote PE includes this sub-TLV with F=1 or F=0, then local PE must insert the hash label in the user and control plane packets.

• If remote PE does not include this sub-TLV (for example, it does not support it, or it is supported but the user did not enable the hash-label option or the signal-capability option), then the local PE establishes the PW but must not insert the hash label in the user and control packets over that spoke-sdp or mesh-sdp. If the remote PE does not support the signal-capability option, then there are a couple of possible outcomes:
  – If the hash-label option was enabled on the local configuration of the spoke-sdp or mesh-sdp at the remote PE, the PW packets received by the local PE will have the hash label included. These packets must be dropped. The only way to solve this is to disable the signaling capability option on the local node which will result in the insertion of the hash label by both PE nodes.
  – If the hash-label option is not supported or was not enabled on the local configuration of the spoke-sdp or mesh-sdp at the remote PE, the PW received by the local PE will not have the hash label included.

• The user can enable or disable the signal-capability option in CLI as needed. When doing so, the must withdraw the label it sent to its peer and send a new label mapping message with the new value of the F bit in the flow label interface parameters sub-TLV of the PW ID FEC element.

The no form of this command disables the use of the hash label.

**Default**
no hash-label

**Parameters**

**signal-capability** — Enables the signaling and negotiation of the use of the hash label between the local and remote PE nodes. The signal-capability option is not supported on a VPRN spoke-sdp.

**ingress**

**Syntax**
ingress

**Context**
config>service>ies>if>spoke-sdp

**Description**
This command configures the ingress SDP context.

**flowspec**

**Syntax**
flowspec
no flowspec

**Context**
config>service>ies>if>spoke-sdp>ingress

**Description**
This command enables flowspec filtering on an IP interface of the base router. Filtering is based on all of the flowspec routes that have been received and accepted by the base router. Ingress traffic on an IP interface can be filtered by both a user-defined ip filter and flowspec. In this case, the user-defined ip filter entries are evaluated before the flowspec routes and the default action of the user-defined ip filter applies as the very last rule.

The no form of the command removes flowspec filtering from an IP interface.

**Default**
No interfaces have flowspec enabled.
IES Interface Commands

**qos**

**Syntax**
```
qos network-policy-id fp-redirect-group queue-group-name instance instance-id]
no qos
```

**Context**
```
configure>service>apipe>spoke-sdp>ingress
configure>service>cpipe>spoke-sdp>ingress
configure>service>epipe>spoke-sdp>ingress
configure>service>fpipe>spoke-sdp>ingress
configure>service>ipipe>spoke-sdp>ingress
config>service>vpls>spoke-sdp>ingress
config>service>vpls>mesh-sdp>ingress
config>service>pw-template>ingress
config>service>vprn>interface>spoke-sdp>ingress
config>service>ies>interface>spoke-sdp>ingress
```

**Description**
This command is used to redirect pseudowire packets to an ingress forwarding plane queue-group for the purpose of rate-limiting.

The ingress pseudowire rate-limiting feature uses a policer in queue-group provisioning model. This model allows the mapping of one or more pseudowires to the same instance of policers, which are defined in a queue-group template.

Operationally, the provisioning model in the case of the ingress pseudowire shaping feature consists of the following steps:

1. Create an ingress queue-group template and configure policers for each FC that needs to be redirected and optionally, for each traffic type (unicast or multicast).
2. Apply the queue-group template to the network ingress forwarding plane where there exists a network IP interface to which the pseudowire packets can be received. This creates one instance of the template on the ingress of the FP. One or more instances of the same template can be created.
3. Configure FC-to-policer mappings together with the policer redirect to a queue-group in the ingress context of a network QoS policy. No queue-group name is specified in this step, which means the same network QoS policy can redirect different pseudowires to different queue-group templates.
4. Apply this network QoS policy to the ingress context of a spoke-SDP inside a service, or to the ingress context of a pseudowire template, and specify the redirect queue-group name.
5. One or more spoke-SDPs can have their FCs redirected to use policers in the same policer queue-group instance.

The following are the constraints and rules of this provisioning model when used in the ingress pseudowire rate-limiting feature:

1. When a pseudowire FC is redirected to use a policer in a named policer queue-group and the queue-group name does not exist, the association is failed at the time the user associates the ingress context of a spoke-SDP to the named queue-group. In such a case, the pseudowire packet will feed directly the ingress network shared queue for that FC defined in the network-queue policy applied to the ingress of the MDA/FP.
2. When a pseudowire FC is redirected to use a policer in a named policer queue-group and the queue-group name exists but the policer-id is not defined in the queue-group template, the association is failed at the time the user associates the ingress context of a spoke-SPD to the named queue-group. In such a case, the pseudowire packet will feed directly the ingress network shared queue for that FC defined in the network-queue policy applied to the ingress of the MDA/FP.
3. When a pseudowire FC is redirected to use a policer in a named policer queue-group and the queue-group name exists and the policer-id is defined in the queue-group template, it is not required to check that an instance of that queue-group exists in all ingress FPs which have network IP interfaces. The handling of this is dealt with in the data path as follows:

   a. When a pseudowire packet for that FC is received and an instance of the referenced queue-group name exists on that FP, the packet is processed by the policer and will then feed the per-FP ingress shared queues referred to as `policer-output-queues`.
   
   b. When a pseudowire packet for that FC is received and an instance of the referenced queue-group name does not exist on that FP, the pseudowire packets will be fed directly into the corresponding ingress network shared queue for that FC defined in the network-queue policy applied to the ingress of the MDA/FP.

4. If a network QoS policy is applied to the ingress context of a pseudowire, any pseudowire FC which is not explicitly redirected in the network QoS policy will have the corresponding packets feed directly the ingress network shared queue for that FC defined in the network-queue policy applied to the ingress of the MDA/FP.

5. If no network QoS policy is applied to the ingress context of the pseudowire, then all packets of the pseudowire will feed:

   a. the ingress network shared queue for the packet FC defined in the network-queue policy applied to the ingress of the MDA/FP. This is the default behavior.
   
   b. a queue-group policer followed by the per-FP ingress shared queues referred to as `policer-output-queues` if the ingress context of the network IP interface from which the packet is received is redirected to a queue-group (csc-policing). The only exceptions to this behavior are for packets received from a IES/VPRN spoke interface and from an R-VPLS spoke-SPD, which is forwarded to the R-VPLS IP interface. In these two cases, the ingress network shared queue for the packet FC defined in the network-queue policy applied to the ingress of the MDA/FP is used.

When a pseudowire is redirected to use a policer queue-group, the classification of the packet for the purpose of FC and profile determination is performed according to default classification rule or the QoS filters defined in the ingress context of the network QoS policy applied to the pseudowire. This is true regardless of whether an instance of the named policer queue-group exists on the ingress FP on which the pseudowire packet is received. The user can apply a QoS filter matching the dot1.p in the VLAN tag corresponding to the Ethernet port encapsulation, the EXP in the outer label when the tunnel is an LSP, the DSCP in the IP header if the tunnel encapsulation is GRE, and the DSCP in the payload IP header if the user enabled the `ler-use-dscp` option and the pseudowire terminates in IES or VPRN service (spoke-interface).

When the policer queue-group name the pseudowire is redirected does not exist, the redirection command is failed. In this case, the packet classification is performed according to default classification rule or the QoS filters defined in the ingress context of the network QoS policy applied to the network IP interface on which the pseudowire packet is received.

The `no` version of this command removes the redirection of the pseudowire to the queue-group.

**Parameters**

- `network-policy-id` — Specifies the network policy identification. The value uniquely identifies the policy on the system.

  **Values**

  1 — 65535

- `fp-redirect-group queue-group-name` — Specifies the name of the queue group template up to 32 characters in length.
**ingress-instance instance-id** — Specifies the identification of a specific instance of the queue-group.

**Values**  
1 — 16384

---

**vc-label**

**Syntax**  
[no] vc-label ingress-vc-label

**Context**  
config>service>ies>if>spoke-sdp>ingress

**Description**  
This command configures the static MPLS VC label used by the far-end device to send packets to this device in this service via this SDP.

**Parameters**  
*ingress-vc-label* — A VC ingress value that indicates a specific connection.

**Values**  
2048 — 18431

---

**accounting-policy**

**Syntax**  
accounting-policy acct-policy-id

**Context**  
config>service>ies>if>spoke-sdp

**Description**  
This command configures an accounting-policy.

**Parameters**  
*acct-policy-id* — Specifies an accounting policy ID.

**Values**  
1 — 99

---

**app-profile**

**Syntax**  
app-profile app-profile-name

**Context**  
config>service>ies>if>spoke-sdp

**Description**  
This command configures the application profile name.

**Parameters**  
*app-profile-name* — Specifies the application profile name.

---

**collect-stats**

**Syntax**  
[no] collect-stats

**Context**  
config>service>ies>if>spoke-sdp

**Description**  
This command enables or disables statistics collection.
IES SAP Commands

sap

**Syntax**

```bash
sap sap-id [create]
no sap sap-id
```

**Context**

`config>service>ies>if`

**Description**

This command creates a Service Access Point (SAP) within a service. A SAP is a combination of port and encapsulation parameters which identifies the service access point on the interface and within the router. Each SAP must be unique.

All SAPs must be explicitly created. If no SAPs are created within a service or on an IP interface, a SAP will not exist on that object.

Enter an existing SAP without the `create` keyword to edit SAP parameters. The SAP is owned by the service in which it was created.

A SAP can only be associated with a single service. A SAP can only be defined on a port that has been configured as an access port using the command.

If a port is shutdown, all SAPs on that port become operationally down. When a service is shutdown, SAPs for the service are not displayed as operationally down although all traffic traversing the service will be discarded. The operational state of a SAP is relative to the operational state of the port on which the SAP is defined.

Note that you can configure an IES interface as a loopback interface by issuing the `loopback` command instead of the `sap sap-id` command. The loopback flag cannot be set on an interface where a SAP is already defined and a SAP cannot be defined on a loopback interface.

The `no` form of this command deletes the SAP with the specified port. When a SAP is deleted, all configuration parameters for the SAP will also be deleted. For Internet Enhanced Service (IES), the IP interface must be shutdown before the SAP on that interface may be removed. The `no` form of this command causes the ptp-hw-assist to be disabled.

**Default**

No SAPs are defined.

**Special Cases**

**IES** — A SAP is defined within the context of an IP routed interface. Each IP interface is limited to a single SAP definition. Attempts to create a second SAP on an IP interface will fail and generate an error; the original SAP will not be affected.

**Parameters**

- `sap-id` — Specifies the physical port identifier portion of the SAP definition. See Common CLI Command Descriptions on page 1783 for command syntax.

  * `port-id` — Specifies the physical port ID in the `slot/mda/port` format.

  If the card in the slot has Media Dependent Adapters (MDAs) installed, the `port-id` must be in the `slot_number/MDA_number/port_number` format. For example, `1/1/1` specifies port 1 on MDA 1 in slot 1.
The port-id must reference a valid port type. When the port-id parameter represents SONET/SDH, the port ID must include the channel ID. A period “.” separates the physical port from the channel-id. The port must be configured as an access port.

If the SONET/SDH port is configured as clear-channel then only the port is specified.

create — Keyword used to create a SAP instance. The create keyword requirement can be enabled/disabled in the environment>create context.

aarp

Syntax  
```
aarp aarpId type type
no aarp
```

Context  
```
config>service>ies>if>sap
config>service>ies>if>spoke-sdp
```

Description  
This command associates an aarp instance to a multi-homed SAP or spoke-sdp. This instance is paired with the same aarp-id in the same node or in a peer node as part of a configuration to provide flow and packet asymmetry removal for traffic for a multi-homed SAP or spoke-sdp.

The type specifies the role of this service point in the AARP: primary (dual-homed), secondary (dual-homed-secondary). The AA service attributes (app-profile, transit-policy) of the primary are inherited by the secondary endpoints. All endpoints within an aarp must be of the same type (sap or spoke), and all endpoints with an aarp must be within the same service.

The no form of the command removes the association.

Default  
```
no aarp
```

Parameters  
```
aarpId — Specifies the AARP instance associated with this SAP. If not configured, no AARP instance is associated with this SAP.
```

Values  
```
1 —
```

```
type — Specifies the role of the SAP referenced by the AARP instance identified by AARP ID.
```

Values  
```
dual-homed — the primary dual homed aa-subscriber side service point of an aarp instance, only supported for IES and VPRN SAP and spoke-sdp
dual-homed-secondary — One of the secondary dual homed aa-subscriber side service points of an aarp instance, only supported for IES and VPRN SAP and spoke-sdp.
```

ip-tunnel

Syntax  
```
ip-tunnel name [create]
o no ip-tunnel name
```

Context  
```
config>service>ies>if>sap
```

Description  
This command is used to configure an IP-GRE or IP-IP tunnel and associate it with a private tunnel SAP within an IES or VPRN service.

The no form of the command deletes the specified IP/GRE or IP-IP tunnel from the configuration. The tunnel must be administratively shutdown before issuing the no ip-tunnel command.
**Default**  No IP tunnels are defined.

**Parameters**  
*ip-tunnel name* — Specifies the name of the IP tunnel. Tunnel names can be from 1 to 32 alphanumeric characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

---

### lag-link-map-profile

**Syntax**  
`lag-link-map-profile lag-link-map-profile-id`  
`no lag-link-map-profile`

**Context**  
`config>service>ies>if>sap`

**Description**  
This command assigns a pre-configured lag link map profile to a SAP/network interface configured on a LAG or a PW port that exists on a LAG. Once assigned/de-assigned, the SAP/network interface egress traffic will be re-hashed over LAG as required by the new configuration.

The *no* form of this command reverts the SAP/network interface to use per-flow, service or link hash as configured for the service/LAG.

**Default**  
*no lag-link-map-profile*

**Parameters**  
*lag-link-map-profile-id* — An integer from 1 to 64 that defines a unique lag link map profile on which the LAG the SAP/network interface exist.

---

### multi-service-site

**Syntax**  
`multi-service-site customer-site-name`  
`no multi-service-site customer-site-name`

**Context**  
`config>service>ies>if>sap`

**Description**  
This command creates a new customer site or edits an existing customer site with the *customer-site-name* parameter. A customer site is an anchor point to create an ingress and egress virtual scheduler hierarchy. When scheduler policies are defined for ingress and egress, the scheduler names contained in each policy are created according to the parameters defined in the policy. Multi-service customer sites exist for the sole purpose of creating a virtual scheduler hierarchy and making it available to queues on multiple Service Access Points (SAPs).

The scheduler policy association with the customer site normally prevents the scheduler policy from being deleted until after the scheduler policy is removed from the customer site. The multi-service-site object will generate a log message indicating that the association was deleted due to scheduler policy removal.

When the multi-service customer site is created, an ingress and egress scheduler policy association does not exist. This does not prevent the site from being assigned to a chassis slot or prevent service SAP assignment. After the site has been created, the ingress and egress scheduler policy associations can be assigned or removed at any time.

**Default**  
None — Each customer site must be explicitly created.

**Parameters**  
*customer-site-name* — Each customer site must have a unique name within the context of the customer. If *customer-site-name* already exists for the customer ID, the CLI context changes to that site name for the
purpose of editing the site scheduler policies or assignment. Any modifications made to an existing site will affect all SAPs associated with the site. Changing a scheduler policy association may cause new schedulers to be created and existing queues on the SAPs to no longer be orphaned. Existing schedulers on the site may cease to exist, causing queues relying on that scheduler to be orphaned.

If the \textit{customer-site-name} does not exist, it is assumed that an attempt is being made to create a site of that name in the customer ID context. The success of the command execution depends on the following:

- The maximum number of customer sites defined for the chassis has not been met.
- The \textit{customer-site-name} is valid.
- The \textit{create} keyword is included in the command line syntax (if the system requires it).

When the maximum number of customer sites has been exceeded a configuration error occurs; the command will not execute and the CLI context will not change.

If the \textit{customer-site-name} is invalid, a syntax error occurs; the command will not execute and the CLI context will not change.

\textbf{Values} \hspace{1em} Valid names consist of any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

\textbf{ancp-string}

\begin{itemize}
  \item Syntax \hspace{1em} \texttt{ancp-string ancp-string}
  \item Syntax \hspace{1em} \texttt{no ancp-string}
  \item Context \hspace{1em} \texttt{config>service>ies>if>sap>static-host}
  \item Description \hspace{1em} This command specifies the ANCP string associated to this SAP host.
  \item Parameters \hspace{1em} \texttt{ancp-string} — Specifies the ANCP string up to 63 characters in length.
\end{itemize}

\textbf{app-profile}

\begin{itemize}
  \item Syntax \hspace{1em} \texttt{app-profile app-profile-name}
  \item Syntax \hspace{1em} \texttt{no app-profile}
  \item Context \hspace{1em} \texttt{config>service>ies>if>sap>static-host}
  \item Description \hspace{1em} This command specifies an application profile name.
  \item Parameters \hspace{1em} \texttt{app-profile-name} — Specifies the application profile name up to 32 characters in length.
\end{itemize}

\textbf{inter-dest-id}

\begin{itemize}
  \item Syntax \hspace{1em} \texttt{inter-dest-id intermediate-destination-id}
  \item Syntax \hspace{1em} \texttt{no inter-dest-id}
  \item Context \hspace{1em} \texttt{config>service>ies>if>sap>static-host}
\end{itemize}
**Description**
Specifies to which intermediate destination (for example, a DSLAM) this host belongs.

**Parameters**
- `intermediate-destination-id` — Specifies the intermediate destination identifier, up to 32 characters in length.

### tod-suite

**Syntax**
tod-suite **tod-suite-name**  
no tod-suite

**Context**
config>service>ies>if>sap

**Description**
This command applies a time-based policy (filter or QoS policy) to the service SAP. The suite name must already exist in the `config>cron` context.

**Default**
no tod-suite

**Parameters**
- `tod-suite-name` — Specifies collection of policies (ACLs, QoS) including time-ranges that define the full or partial behavior of a SAP. The suite can be applied to more than one SAP.

### dynamic-tunnel-redundant-next-hop

**Syntax**
dynamic-tunnel-redundant-next-hop **ip-address**  
no dynamic-tunnel-redundant-next-hop

**Context**
config>service>ies>if

**Description**
This command specifies redundant next-hop address on public or private IPsec interface (with public or private tunnel-sap) for dynamic IPsec tunnel. The specified next-hop address will be used by standby node to shunt traffic to master in case of it receives them.

The next-hop address will be resolved in routing table of corresponding service.

**Default**
none

**Parameters**
- `ip-address` — Specifies the dynamic ISA tunnel redundant next-hop address.

### egr-ip-load-balancing

**Syntax**
eggr-ip-load-balancing {**src-ip** | **dst-ip**}  
no egr-ip-load-balancing

**Context**
config>service>ies>if

**Description**
This command specifies whether to include source address or destination address or both in LAG/ECMP hash on IP interfaces. Additionally, when l4-load-balancing is enabled the command applies also to inclusion of source/destination port in the hash inputs.

The **no** form of this command includes both source and destination parameters.

**Default**
no egr-ip-load-balancing
IES Interface Commands

Parameters

src-ip — Specifies using source address and (if l4-load balancing is enabled) source port in the hash, ignore destination address/port.

dst-ip — Specifies using destination address and (if l4-load balancing is enabled) destination port in the hash, ignore source address/port.

enable-mac-accounting

Syntax

[no] enable-mac-accounting

Context

config>service>ies>if

Description

This command enables MAC accounting functionality on this interface. The no form of the command disables MAC accounting functionality on this interface.

flowspec

Syntax

[no] flowspec

Context

config>service>vprn>interface>sap>ingress
cfg@service>vprn>interface>spoke-sdp>ingress
cfg@service>ies>interface>sap>ingress
cfg@service>ies>interface>spoke-sdp>ingress

Description

This command enables IPv4 flowspec filtering on an access IP interface associated with a VPRN or IES service. Filtering is based on all of the IPv4 flowspec routes that have been received and accepted by the corresponding BGP instance. Ingress IPv4 traffic on an interface can be filtered by both a user-defined IPv4 filter and flowspec. Evaluation proceeds in this order:

1. user-defined IPv4 filter entries
2. flowspec-derived filter entries
3. user-defined IPv4 filter default-action

The no form of the command removes IPv4 flowspec filtering from an IP interface.

Default

No access interfaces have IPv4 flowspec enabled.

flowspec-ipv6

Syntax

flowspec-ipv6

no flowspec-ipv6

Context

config>service>vprn>interface>sap>ingress
cfg@service>vprn>interface>spoke-sdp>ingress
cfg@service>ies>interface>sap>ingress
cfg@service>ies>interface>spoke-sdp>ingress
Description  This command enables IPv6 flowspec filtering on an access IP interface associated with a VPRN or IES service. Filtering is based on all of the IPv6 flowspec routes that have been received and accepted by the corresponding BGP instance. Ingress IPv6 traffic on an interface can be filtered by both a user-defined IPv6 filter and flowspec. Evaluation proceeds in this order:

1. user-defined IPv6 filter entries
2. flowspec-derived filter entries
3. user-defined IPv6 filter default-action

The no form of the command removes IPv6 flowspec filtering from an IP interface.

Default  No access interfaces have IPv6 flowspec enabled.

calling-station-id

Syntax  calling-station-id calling-station-id
no calling-station-id

Context  config>service>ies>if>sap

Description  This command enables the inclusion of the calling-station-id attribute in RADIUS authentication requests and RADIUS accounting messages. The value inserted is set at the SAP level. If no value is set at the SAP level, an empty string is included.

Default  This attribute is not sent by default.
ETH-CFM Service Commands

eth-cfm

Syntax
eth-cfm

Context
config>service>ies>
  config>service>ies>if>sap
  config>service>ies>if>spoke-sdp

Description
This command enables the context to configure ETH-CFM parameters.

mep

Syntax
mep mep-id domain md-index association ma-index [direction {up | down}]
no mep mep-id domain md-index association ma-index

Context
config>service>ies>if>sap>eth-cfm
  config>service>ies>if>spoke-sdp>eth-cfm

Description
This command configures the ETH-CFM maintenance endpoint (MEP).

Parameters
mep-id — Specifies the maintenance association end point identifier.
  Values 1 — 8191

md-index — Specifies the maintenance domain (MD) index value.
  Values 1 — 4294967295

ma-index — Specifies the MA index value.
  Values 1 — 4294967295

direction up|down — Indicates the direction in which the maintenance association (MEP) faces on the bridge port. Direction UP is not applicable to IES MEPs.
  down — Sends ETH-CFM messages away from the MAC relay entity.
  up — Sends ETH-CFM messages towards the MAC relay entity.

ais-enable

Syntax
[no] ais-enable

Context
config>service>ies>if>spoke-sdp>eth-cfm
  config>service>vpls>sap>eth-cfm>mep
  config>service>vpls>spoke-sdp>eth-cfm>mep
Description: This command configures the reception of Alarm Indication Signal (AIS) message.

interface-support-enable

**Syntax**

```
[no] interface-support-enable
```

**Context**

```
config>service>ies>sap>eth-cfm>mep>ais-enable
config>service>ies>spoke-sdp>eth-cfm>mep>ais-enable
```

**Description**

This command enables the AIS function to consider the operational state of the entity on which it is configured. With this command, ETH-AIS on DOWN MEPs will be triggered and cleared based on the operational status of the entity on which it is configured. If CCM is also enabled then transmission of the AIS PDU will be based on either the non operational state of the entity or on ANY CCM defect condition. AIS generation will cease if BOTH operational state is UP and CCM has no defect conditions. If the MEP is not CCM enabled then the operational state of the entity is the only consideration assuming this command is present for the MEP.

**Default**

```
[no] interface-support-enabled (AIS will not be generated or stopped based on the state of the entity on) which the DOWN MEP is configured.
```

ccm-enable

**Syntax**

```
[no] ccm-enable
```

**Context**

```
config>service>ies>if>sap>eth-cfm>mep
config>service>ies>if>spoke-sdp>eth-cfm>mep
```

**Description**

This command enables the generation of CCM messages.

The `no` form of the command disables the generation of CCM messages.

ccm-ltm-priority

**Syntax**

```
ccm-ltm-priority priority
no ccm-ltm-priority
```

**Context**

```
config>service>ies>if>sap>eth-cfm>mep
config>service>ies>if>spoke-sdp>eth-cfm>mep
```

**Description**

This command specifies the priority value for CCMs and LTMs transmitted by the MEP.

The `no` form of the command removes the priority value from the configuration.

**Default**

The highest priority on the bridge-port.

**Parameters**

```
priority — Specifies the priority of CCM and LTM messages.
```

**Values**

```
0 — 7
```
ccm-padding-size

**Syntax**  
\[no\] ccm-padding-size ccm-padding

**Context**  
config>service>ies>if>spoke-sdp>eth-cfm>mep

**Description**  
Set the byte size of the optional Data TLV to be included in the ETH-CC PDU. This will increase the size of the ETH-CC PDU by the configured value. The base size of the ETH-CC PDU, including the Interface Status TLV and Port Status TLV, is 83 bytes not including the Layer Two encapsulation. CCM padding is not supported when the CCM-Interval is less than one second.

**Default**  
ccm-padding-size

**Parameters**  
ccm-padding — specifies the byte size of the Optional Data TLV

**Values**  
3 — 1500

eth-test-enable

**Syntax**  
\[no\] eth-test-enable

**Context**  
config>service>ies>if>sap>eth-cfm>mep

**Default**  
For ETH-test to work, operators need to configure ETH-test parameters on both sender and receiver nodes. The ETH-test then can be done using the following OAM commands:

```
oam eth-cfm eth-test mac-address mep mep-id domain md-index association ma-index [priority priority] [data-length data-length]
```

A check is done for both the provisioning and test to ensure the MEP is an Y.1731 MEP (MEP provisioned with domain format none, association format icc-based). If not, the operation fails. An error message in the CLI and SNMP will indicate the problem.

test-pattern

**Syntax**  
test-pattern {all-zeros | all-ones} [crc-enable]  
\[no\] test-pattern

**Context**  
config>service>ies>if>sap>eth-cfm>mep>eth-test-enable

**Default**  
This command configures the test pattern for eth-test frames. The no form of the command removes the values from the configuration.

**Parameters**  
all-zeros — Specifies to use all zeros in the test pattern.  
all-ones — Specifies to use all ones in the test pattern.  
crc-enable — Generates a CRC checksum.

**Default**  
all-zeros
fault-propagation-enable

Syntax  
```plaintext
fault-propagation-enable \{use-if-tlv | suspend-ccm\}
```

no fault-propagation-enable

Context  
```plaintext
config>service>ies>if>sap>eth-cfm>mep
```

description  
This command configures the fault propagation for the MEP.

Parameters  
- **use-if-tlv** — Specifies to use the interface TLV.
- **suspend-ccm** — Specifies to suspend the continuity check messages.

low-priority-defect

Syntax  
```plaintext
low-priority-defect \{allDef|macRemErrXcon|remErrXcon|errXcon|xcon|noXcon\}
```

Context  
```plaintext
config>service>ies>if>sap>eth-cfm>mep
```

description  
This command specifies the lowest priority defect that is allowed to generate a fault alarm.

default  
macRemErrXcon

Values  
- **allDef** — DefRDICCM, DefMACstatus, DefRemoteCCM, DefErrorCCM, and DefXconCCM
- **macRemErrXcon** — Only DefMACstatus, DefRemoteCCM, DefErrorCCM, and DefXconCCM
- **remErrXcon** — Only DefRemoteCCM, DefErrorCCM, and DefXconCCM
- **errXcon** — Only DefErrorCCM and DefXconCCM
- **xcon** — Only DefXconCCM; or
- **noXcon** — No defects DefXcon or lower are to be reported

tunnel-fault

Syntax  
```plaintext
tunnel-fault \{accept | ignore\}
```

Context  
```plaintext
config>service>ies>eth-cfm
```  
```plaintext
config>service>ies>if>sap>eth-cfm
```

description  
Allows the individual service SAPs to react to changes in the tunnel MEP state. When tunnel-fault accept is configured at the service level, the SAP will react according to the service type, Epipe will set the operational flag and VPLS, IES and VPRN SAP operational state will become down on failure or up on clear. This command triggers the OAM mapping functions to mate SAPs and bindings in an Epipe service as well as setting the operational flag. If AIS generation is the requirement for the Epipe services this command is not required. See the command ais-enable under epipe>sap>eth-cfm>ais-enable for more details. This works in conjunction with the tunnel-fault accept on the individual SAPs. Both must be set to accept to react to the tunnel MEP state. By default the service level command is “ignore” and the sap level command is “accept”. This means simply changing the service level command to “accept” will enable the feature for all SAPs. This is not required for Epipe services that only wish to generate AIS on failure.
Parameters

accept — Share fate with the facility tunnel MEP
ignore — Do not share fate with the facility tunnel MEP

Default
ignore (Service Level)
accept (SAP Level for Epipe and VPLS)

one-way-delay-threshold

Syntax

one-way-delay-threshold time

Context
config>service>ies>if>sap>mep
config>service>ies>interface>spoke-sdp>eth-cfm>mep

Description
This command enables one way delay threshold time limit.

Default
3 seconds

Parameters
priority — Specifies the value for the threshold.
Values

0 — 600
IES Filter and QoS Policy Commands

**filter**

**Syntax**

filter ip ip-filter-id  
filter ipv6 ipv6-filter-id  
no filter [ip ip-filter-id] [ipv6 ipv6-filter-id]

**Context**

config>service>ies>if>sap>egress  
config>service>ies>if>sap>ingress  
config>service>ies>redundant-interface>egress  
config>service>ies>redundant-interface>ingress

**Description**

This command associates a filter policy with an ingress or egress Service Access Point (SAP). Filter policies control the forwarding and dropping of packets based on the matching criteria.

The `filter` command is used to associate a filter policy with a specified `ip-filter-id` with an ingress or egress SAP. The filter policy must already be defined before the `filter` command is executed. If the filter policy does not exist, the operation will fail and an error message returned.

In general, filters applied to SAPs (ingress or egress) apply to all packets on the SAP. One exception is non-IP packets are not applied to the match criteria, so the default action in the filter policy applies to these packets.

The `no` form of this command removes any configured filter ID association with the SAP. The filter ID itself is not removed from the system unless the scope of the created filter is set to local. To avoid deletion of the filter ID and only break the association with the service object, use `scope` command within the filter definition to change the scope to `local` or `global`. The default scope of a filter is `local`.

**Special Cases**

IES — Only IP filters are supported on an IES IP interface, and the filters only apply to routed traffic.

**Parameters**

- **ip** — Keyword indicating the filter policy is an IP filter.
- **ip-filter-id** — Specifies the ID for the IP filter policy. Allowed values are an integer in the range of 1 and 65535 that corresponds to a previously created IP filter policy in the `configure>filter>ip-filter` context.

---

**filter**

**Syntax**

filter ip ip-filter-id  
filter ipv6 ipv6-filter-id  
no filter

**Context**

config>service>ies>if>spoke-sdp>egress  
config>service>ies>if>spoke-sdp>ingress

**Description**

This command associates an IP filter policy filter policy with an ingress or egress spoke SDP. Filter policies control the forwarding and dropping of packets based on matching criteria.
MAC filters are only allowed on Epipe and Virtual Private LAN Service (VPLS) SAPs. The `filter` command is used to associate a filter policy with a specified `ip-filter-id` with an ingress or egress spoke SDP. The `ip-filter-id` must already be defined in the `configure>filter` context before the `filter` command is executed. If the filter policy does not exist, the operation will fail and an error message returned.

In general, filters applied to SAPs or spoke SDPs (ingress or egress) apply to all packets on the SAP or spoke SDPs. One exception is non-IP packets are not applied to IP match criteria, so the default action in the filter policy applies to these packets.

The `no` form of this command removes any configured filter ID association with the SAP or IP interface. The filter ID itself is not removed from the system unless the scope of the created filter is set to local. To avoid deletion of the filter ID and only break the association with the service object, use `scope` command within the filter definition to change the scope to `local` or `global`. The default scope of a filter is `local`.

**SpecCases**
- **IES** — Only IP filters are supported on IES IP interfaces, and the filters only apply to routed traffic.

**Parameters**
- **ip** — Keyword indicating the filter policy is an IP filter.
- **ip-filter-id** — The filter name acts as the ID for the IP filter policy. Allowed values are an integer in the range of 1 and 65535 that corresponds to a previously created IP filter policy. The filter ID must already exist within the created IP filters.

### egress

**Syntax**
- `egress`

**Context**
- `config>service>ies>if>sap`

**Description**
- This command enables the context to apply egress policies.
- If no sap-egress QoS policy is defined, the system default sap-egress QoS policy is used for egress processing. If no egress filter is defined, no filtering is performed.

### ingress

**Syntax**
- `ingress`

**Context**
- `config>service>ies>if>sap`

**Description**
- This command enables the context to apply ingress policies.
- If no sap-ingress QoS policy is defined, the system default sap-ingress QoS policy is used for ingress processing. If no ingress filter is defined, no filtering is performed.
**Syntax**

match-qinq-dot1p {top | bottom}

no match-qinq-dot1p

**Context**

config>service>ies>if>sap>ingress

**Description**

This command specifies which Dot1Q tag position Dot1P bits in a QinQ encapsulated packet should be used to evaluate Dot1P QoS classification.

The **match-qinq-dot1p** command allows the top or bottom PBits to be used when evaluating the applied sap-ingress QoS policy’s Dot1P entries. The **top** and **bottom** keywords specify which position should be evaluated for QinQ encapsulated packets.

The **no** form of the command restores the default dot1p evaluation behavior for the SAP.

By default, the bottom most service delineating Dot1Q tags Dot1P bits are used. **Table 18** defines the default behavior for Dot1P evaluation when the **match-qinq-dot1p** command is not executed.

**Table 18: Default QinQ and TopQ SAP Dot1P Evaluation**

<table>
<thead>
<tr>
<th>Port / SAP Type</th>
<th>Existing Packet Tags</th>
<th>PBits Used for Match</th>
</tr>
</thead>
<tbody>
<tr>
<td>Null Null</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>Null Dot1P (VLAN-ID 0)</td>
<td>Dot1P PBits</td>
<td></td>
</tr>
<tr>
<td>Null Dot1Q</td>
<td>Dot1Q PBits</td>
<td></td>
</tr>
<tr>
<td>Null TopQ BottomQ</td>
<td>TopQ PBits</td>
<td></td>
</tr>
<tr>
<td>Null TopQ (No BottomQ)</td>
<td>TopQ PBits</td>
<td></td>
</tr>
<tr>
<td>Dot1Q None (Default SAP)</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>Dot1Q Dot1P (Default SAP VLAN-ID 0)</td>
<td>Dot1P PBits</td>
<td></td>
</tr>
<tr>
<td>Dot1Q Dot1Q</td>
<td>Dot1Q PBits</td>
<td></td>
</tr>
<tr>
<td>QinQ / TopQ TopQ</td>
<td>TopQ PBits</td>
<td></td>
</tr>
<tr>
<td>QinQ / TopQ TopQ BottomQ</td>
<td>TopQ PBits</td>
<td></td>
</tr>
<tr>
<td>QinQ / QinQ TopQ BottomQ</td>
<td>BottomQ PBits</td>
<td></td>
</tr>
</tbody>
</table>

**Default**

no match-qinq-dot1p — No filtering based on p-bits.

Top or bottom must be specified to override the default QinQ dot1p behavior.
Parameters

**top** — The top parameter is mutually exclusive to the bottom parameter. When the top parameter is specified, the top most PBits are used (if existing) to match any dot1p dot1p-value entries. Table 19 defines the dot1p evaluation behavior when the top parameter is specified.

**bottom** — The bottom parameter is mutually exclusive to the top parameter. When the bottom parameter is specified, the bottom most PBits are used (if existing) to match any dot1p dot1p-value entries. Table 20 defines the dot1p evaluation behavior when the bottom parameter is specified.

### Table 19: Top Position QinQ and TopQ SAP Dot1P Evaluation

<table>
<thead>
<tr>
<th>Port / SAP Type</th>
<th>Existing Packet Tags</th>
<th>PBits Used for Match</th>
</tr>
</thead>
<tbody>
<tr>
<td>Null</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>Null</td>
<td>Dot1P (VLAN-ID 0)</td>
<td>Dot1P PBits</td>
</tr>
<tr>
<td>Null</td>
<td>Dot1Q</td>
<td>Dot1Q PBits</td>
</tr>
<tr>
<td>Null</td>
<td>TopQ BottomQ</td>
<td>TopQ PBits</td>
</tr>
<tr>
<td>Null</td>
<td>TopQ (No BottomQ)</td>
<td>TopQ PBits</td>
</tr>
<tr>
<td>Dot1Q</td>
<td>None (Default SAP)</td>
<td>None</td>
</tr>
<tr>
<td>Dot1Q</td>
<td>Dot1P (Default SAP VLAN-ID 0)</td>
<td>Dot1P PBits</td>
</tr>
<tr>
<td>Dot1Q</td>
<td>Dot1Q</td>
<td>Dot1Q PBits</td>
</tr>
<tr>
<td>QinQ / TopQ</td>
<td>TopQ</td>
<td>TopQ PBits</td>
</tr>
<tr>
<td>QinQ / TopQ</td>
<td>TopQ BottomQ</td>
<td>TopQ PBits</td>
</tr>
<tr>
<td>QinQ / QinQ</td>
<td>TopQ BottomQ</td>
<td>TopQ PBits</td>
</tr>
</tbody>
</table>

### Table 20: Bottom Position QinQ and TopQ SAP Dot1P Evaluation

<table>
<thead>
<tr>
<th>Port / SAP Type</th>
<th>Existing Packet Tags</th>
<th>PBits Used for Match</th>
</tr>
</thead>
<tbody>
<tr>
<td>Null</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>Null</td>
<td>Dot1P (VLAN-ID 0)</td>
<td>Dot1P PBits</td>
</tr>
<tr>
<td>Null</td>
<td>Dot1Q</td>
<td>Dot1Q PBits</td>
</tr>
<tr>
<td>Null</td>
<td>TopQ BottomQ</td>
<td>BottomQ PBits</td>
</tr>
<tr>
<td>Null</td>
<td>TopQ (No BottomQ)</td>
<td>TopQ PBits</td>
</tr>
<tr>
<td>Dot1Q</td>
<td>None (Default SAP)</td>
<td>None</td>
</tr>
<tr>
<td>Dot1Q</td>
<td>Dot1P (Default SAP VLAN-ID 0)</td>
<td>Dot1P PBits</td>
</tr>
<tr>
<td>Dot1Q</td>
<td>Dot1Q</td>
<td>Dot1Q PBits</td>
</tr>
</tbody>
</table>
### Table 20: Bottom Position QinQ and TopQ SAP Dot1P Evaluation (Continued)

<table>
<thead>
<tr>
<th>Port / SAP Type</th>
<th>Existing Packet Tags</th>
<th>PBits Used for Match</th>
</tr>
</thead>
<tbody>
<tr>
<td>QinQ / TopQ</td>
<td>TopQ</td>
<td>TopQ PBits</td>
</tr>
<tr>
<td>QinQ / TopQ</td>
<td>TopQ BottomQ</td>
<td>BottomQ PBits</td>
</tr>
<tr>
<td>QinQ / QinQ</td>
<td>TopQ BottomQ</td>
<td>BottomQ PBits</td>
</tr>
</tbody>
</table>

### Table 21: Default Dot1P Explicit Marking Actions

<table>
<thead>
<tr>
<th>Egress SAP Type</th>
<th>Ingress Packet Preserved Dot1P State</th>
<th>Marked (or Remarked) PBits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Null</td>
<td>No preserved Dot1P bits</td>
<td>None</td>
</tr>
<tr>
<td>Null</td>
<td>Preserved Dot1P bits</td>
<td>Preserved tag PBits remarked using dot1p-value</td>
</tr>
<tr>
<td>Dot1Q</td>
<td>No preserved Dot1P bits</td>
<td>New PBits marked using dot1p-value</td>
</tr>
<tr>
<td>Dot1Q</td>
<td>Preserved Dot1P bits</td>
<td>Preserved tag PBits remarked using dot1p-value</td>
</tr>
<tr>
<td>TopQ</td>
<td>No preserved Dot1P bits</td>
<td>TopQ PBits marked using dot1p-value</td>
</tr>
<tr>
<td>TopQ</td>
<td>Preserved Dot1P bits (used as TopQ and BottomQ PBits)</td>
<td>TopQ PBits and BottomQ PBits marked using dot1p-value</td>
</tr>
<tr>
<td>QinQ</td>
<td>No preserved Dot1P bits</td>
<td>TopQ PBits and BottomQ PBits marked using dot1p-value</td>
</tr>
<tr>
<td>QinQ</td>
<td>Preserved Dot1P bits (used as TopQ and BottomQ PBits)</td>
<td>TopQ PBits and BottomQ PBits marked using dot1p-value</td>
</tr>
</tbody>
</table>

### Table 22: QinQ Mark Top Only Explicit Marking Actions

<table>
<thead>
<tr>
<th>Egress SAP Type</th>
<th>Ingress Packet Preserved Dot1P State</th>
<th>Marked (or Remarked) PBits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Null</td>
<td>No preserved Dot1P bits</td>
<td>None</td>
</tr>
<tr>
<td>Null</td>
<td>Preserved Dot1P bits</td>
<td>Preserved tag PBits remarked using dot1p-value</td>
</tr>
<tr>
<td>Dot1Q</td>
<td>No preserved Dot1P bits</td>
<td>New PBits marked using dot1p-value</td>
</tr>
<tr>
<td>Dot1Q</td>
<td>Preserved Dot1P bits</td>
<td>Preserved tag PBits remarked using dot1p-value</td>
</tr>
<tr>
<td>TopQ</td>
<td>No preserved Dot1P bits</td>
<td>TopQ PBits marked using dot1p-value</td>
</tr>
</tbody>
</table>
IES Filter and QoS Policy Commands

Table 22: QinQ Mark Top Only Explicit Marking Actions

<table>
<thead>
<tr>
<th>Egress SAP Type</th>
<th>Ingress Packet Preserved Dot1P State</th>
<th>Marked (or Remarked) PBits</th>
</tr>
</thead>
<tbody>
<tr>
<td>TopQ</td>
<td>Preserved Dot1P bits (used as TopQ and BottomQ PBits)</td>
<td>TopQ PBits marked using dot1p-value, BottomQ PBits preserved</td>
</tr>
<tr>
<td>QinQ</td>
<td>No preserved Dot1P bits</td>
<td>TopQ PBits marked using dot1p-value, BottomQ PBits marked with zero</td>
</tr>
<tr>
<td>QinQ</td>
<td>Preserved Dot1P bits (used as TopQ and BottomQ PBits)</td>
<td>TopQ PBits marked using dot1p-value, BottomQ PBits marked using preserved value</td>
</tr>
</tbody>
</table>

The QinQ and TopQ SAP PBit/DEI bit marking follows the default behavior defined in the above tables when `qinq-mark-top-only` is not specified.

The dot1p dot1p-value command must be configured without the qinq-mark-top-only parameter to remove the TopQ P Bits only marking restriction.

**agg-rate-limit**

**Syntax**

```
agg-rate-limit agg-rate [queue-frame-based-accounting]
no agg-rate-limit
```

**Context**

```
config>service>ies>if>sap>egress
```

**Description**

This command defines a maximum total rate for all egress queues on a service SAP or multi-service site. The `agg-rate-limit` command is mutually exclusive with the egress scheduler policy. When an egress scheduler policy is defined, the `agg-rate-limit` command will fail. If the `agg-rate-limit` command is specified, at attempt to bind a `scheduler-policy` to the SAP or multi-service site will fail.

A multi-service site must have a port scope defined that ensures all queues associated with the site are on the same port or channel. If the scope is not set to a port, the agg-rate-limit command will fail. Once an agg-rate-limit has been assigned to a multi-service site, the scope cannot be changed to card level.

A port scheduler policy must be applied on the egress port or channel the SAP or multi-service site are bound to in order for the defined agg-rate-limit to take effect. The egress port scheduler enforces the aggregate queue rate as it distributes its bandwidth at the various port priority levels. The port scheduler stops offering bandwidth to member queues once it has detected that the aggregate rate limit has been reached.

If a port scheduler is not defined on the egress port, the queues are allowed to operate based on their own bandwidth parameters.

The `no` form of the command removes the aggregate rate limit from the SAP or multi-service site.

**Parameters**

- `agg-rate` — Defines the rate, in kilobits-per-second, that the maximum aggregate rate that the queues on the SAP or MSS can operate.
  
  **Values**
  
  1 — 40000000, max

- `queue-frame-based-accounting` — This keyword enables frame based accounting on all queues associated...
with the SAP or Multi-Service Site. If frame based accounting is required when an aggregate limit is not necessary, the max keyword should precede the queue-frame-based-accounting keyword. If frame based accounting must be disabled, execute agg-rate-limit without the queue-frame-based-accounting keyword present.

**Default**  
Frame based accounting is disabled by default

### agg-rate

**Syntax**  
```
[no] agg-rate
```

**Context**  
```
config>service>ies>if>sap>egress
```

**Description**  
This command is used to control an HQoS aggregate rate limit. It is used in conjunction with the following parameter commands: `rate`, `limit-unused-bandwidth`, and `queue-frame-based-accounting`.

### rate

**Syntax**  
```
rate {max | rate}
no rate
```

**Context**  
```
config>service>ies>if>sap>egress>agg-rate
```

**Description**  
This command defines the enforced aggregate rate for all queues associated with the agg-rate context. A rate must be specified for the agg-rate context to be considered to be active on the context’s object (SAP, subscriber, VPORT etc.).

### limit-unused-bandwidth

**Syntax**  
```
[no] limit-unused-bandwidth
```

**Context**  
```
config>service>ies>if>sap>egress>agg-rate
```

**Description**  
This command is used to enable (or disable) aggregate rate overrun protection on the agg-rate context.

### queue-frame-based-accounting

**Syntax**  
```
[no] queue-frame-based-accounting
```

**Context**  
```
config>service>ies>if>sap>egress>agg-rate
```

**Description**  
This command is used to enabled (or disable) frame based accounting on all queues associated with the agg-rate context. Only supported on Ethernet ports. Not supported on HSMDA Ethernet ports.
qinq-mark-top-only

Syntax  [no] qinq-mark-top-only

Context  config>service>ies>if>sap>egress

Description  When enabled (the encapsulation type of the access port where this SAP is defined as qinq), the qinq-mark-
top-only command specifies which P-bits/DEI bit to mark during packet egress. When disabled, both set of
P-bits/DEI bit are marked. When the enabled, only the P-bits/DEI bit in the top Q-tag are marked.

Default  no qinq-mark-top-only

QOS

Syntax  qos policy-id [port-redirect-group queue-group-name instance instance-id]

no qos

Context  config>service>ies>if>sap>egress
config>service>ies>sub-if>grp-if>sap>egress

Description  This command associates a Quality of Service (QoS) policy with an egress Service Access Point (SAP).
QoS ingress and egress policies are important for the enforcement of SLA agreements. The policy ID must
be defined prior to associating the policy with a SAP. If the policy-id does not exist, an error will be
returned.

The qos command is used to associate both ingress and egress QoS policies. The qos command only allows
ingress policies to be associated on SAP ingress and egress policies on SAP egress. Attempts to associate a
QoS policy of the wrong type returns an error.

Only one ingress and one egress QoS policy can be associated with a SAP at one time. Attempts to associate
a second QoS policy of a given type will return an error.

When an ingress QoS policy is defined on IES ingress IP interface that is bound to a VPLS, the policy
becomes associated with every SAP on the VPLS and augments the QoS policy that is defined on each SAP.
Packets that are bridged will be processed using the policy defined on the VPLS SAP; packets that are
routed will be processed using the policy defined in the IES IP interface-binding context.

By default, no specific QoS policy is associated with the SAP for ingress or egress, so the default QoS policy
is used.

The no form of this command removes the QoS policy association from the SAP, and the QoS policy reverts
to the default.

Default  none

Parameters  policy-id — The ingress/egress policy ID to associate with SAP or IP interface on ingress/egress. The policy
ID must already exist.

1 — 65535

port-redirect-group — This keyword associates a SAP egress with an instance of a named queue group
template on the egress port of a given IOM/IMM/XMA. The queue-group-name and instance instance-id are
mandatory parameters when executing the command.

queue-group-name — Specifies the name of the egress port queue group of the IOM/IMM/XMA, up to 32
characters in length. The queue-group-name must correspond to a valid egress queue group, created under config>port>ethernet>access>egress.

instance instance-id — Specifies the instance of the named egress port queue group on the IOM/IMM/XMA.

Values  
1 — 40960

Default  
1

QOS

Syntax qos policy-id [shared-queuing |multipoint-shared] [fp-redirect-group queue-group-name instance instance-id]  
no qos

Context config>service>vprn>if>sap>ingress  
config>service>vprn>sub-if>grp-if>sap>ingress  
config>service>vprn>ipsec-if>sap>ingress

Description This command associates a Quality of Service (QoS) policy with an ingress Service Access Point (SAP). QoS ingress and egress policies are important for the enforcement of SLA agreements. The policy ID must be defined prior to associating the policy with a SAP. If the policy-id does not exist, an error will be returned.

The qos command is used to associate both ingress and egress QoS policies. The qos command only allows ingress policies to be associated on SAP ingress and egress policies on SAP egress. Attempts to associate a QoS policy of the wrong type returns an error.

Only one ingress and one egress QoS policy can be associated with a SAP or IP interface at one time. Attempts to associate a second QoS policy of a given type will return an error.

By default, no specific QoS policy is associated with the SAP for ingress or egress, so the default QoS policy is used.

The no form of this command removes the QoS policy association from the SAP, and the QoS policy reverts to the default.

The no form of this command removes the QoS policy association from the SAP or IP interface, and the QoS policy reverts to the default.

Default none

Parameters  

policy-id — The ingress/egress policy ID to associate with SAP or IP interface on ingress/egress. The policy ID must already exist.

1 — 65535

shared-queuing — Specifies the ingress shared queue policy used by this SAP. When the value of this object is null it means that the SAP will use individual ingress QoS queues instead of the shared ones.

multipoint-shared — This keyword specifies that this queue-id is for multipoint forwarded traffic only. This queue-id can only be explicitly mapped to the forwarding class multicast, broadcast, or unknown unicast ingress traffic. Attempting to map forwarding class unicast traffic to a multipoint queue generates an error; no changes are made to the current unicast traffic queue mapping.
A queue must be created as multipoint. The **multipoint** designator cannot be defined after the queue is created. If an attempt is made to modify the command to include the multipoint keyword, an error is generated and the command will not execute.

The **multipoint** keyword can be entered in the command line on a pre-existing multipoint queue to edit queue-id parameters.

**Default** Present (the queue is created as non-multipoint).

**Values** Multipoint or not present.

**fp-redirect-group** — This keyword creates an instance of a named queue group template on the ingress forwarding plane of a given IOM/IMM/XMA. The **queue-group-name** and **instance instance-id** are mandatory parameters when executing the command. The named queue group template can contain only policers. If it contains queues, then the command will fail.

**queue-group-name** — Specifies the name of the queue group template to be instantiated on the forwarding plane of the IOM/IMM/XMA, up to 32 characters in length. The **queue-group-name** must correspond to a valid ingress queue group template name, configured under `config>qos>queue-group-templates`.

**instance-id** — Specifies the instance of the named queue group to be created on the IOM/IMM/XMA ingress forwarding plane.

### queue-override

**Syntax** 

```
[no] queue-override
```

**Context**

```
config>service>ies>if>sap>egress
config>service>ies>if>sap>ingress
```

**Description**

This command enables the context to configure override values for the specified SAP egress QoS queue. These values override the corresponding ones specified in the associated SAP egress or ingress QoS policy.

### queue

**Syntax** 

```
[no] queue queue-id
```

**Context**

```
config>service>ies>if>sap>egress
config>service>ies>if>sap>ingress
```

**Description**

This command specifies the ID of the queue whose parameters are to be overridden.

**Parameters**

- **queue-id** — The queue ID whose parameters are to be overridden.

  **Values**

  - 1 — 32
adaptation-rule

Syntax  
adaptation-rule [pir {max | min | closest}] [cir {max | min | closest}]

no adaptation-rule

Context  
config>service>ies>if>sap>egress>queue-override>queue
cfg>service>ies>if>sap>ingress>queue-override>queue

Description  
This command can be used to override specific attributes of the specified queue’s adaptation rule parameters. The adaptation rule controls the method used by the system to derive the operational CIR and PIR settings when the queue is provisioned in hardware. For the CIR and PIR parameters individually, the system attempts to find the best operational rate depending on the defined constraint.

The no form of the command removes any explicitly defined constraints used to derive the operational CIR and PIR created by the application of the policy. When a specific adaptation-rule is removed, the default constraints for rate and cir apply.

Default  
no adaptation-rule

Parameters  
pir — The pir parameter defines the constraints enforced when adapting the PIR rate defined within the queue queue-id rate command. The pir parameter requires a qualifier that defines the constraint used when deriving the operational PIR for the queue. When the rate command is not specified, the default applies.

max — The max (maximum) option is mutually exclusive with the min and closest options. When max is defined, the operational PIR for the queue will be equal to or less than the administrative rate specified using the rate command.

min — The min (minimum) option is mutually exclusive with the max and closest options. When min is defined, the operational PIR for the queue will be equal to or greater than the administrative rate specified using the rate command.

closest — The closest parameter is mutually exclusive with the min and max parameter. When closest is defined, the operational PIR for the queue will be the rate closest to the rate specified using the rate command.

cir — The cir parameter defines the constraints enforced when adapting the CIR rate defined within the queue queue-id rate command. The cir parameter requires a qualifier that defines the constraint used when deriving the operational CIR for the queue. When the cir parameter is not specified, the default constraint applies.

avg-frame-overhead

Syntax  
avg-frame-overhead percent

no avg-frame-overhead

Context  
config>service>ies>if>sap>egress>queue-override
cfg>service>ies>if>sap>ingress>queue-override>queue

Description  
This command configures the average frame overhead to define the average percentage that the offered load to a queue will expand during the frame encapsulation process before sending traffic on-the-wire. While the avg-frame-overhead value may be defined on any queue, it is only used by the system for queues that egress a Sonet or SDH port or channel. Queues operating on egress Ethernet ports automatically calculate the frame
encapsulation overhead based on a 20 byte per packet rule (8 bytes for preamble and 12 bytes for inter-frame gap).

When calculating the frame encapsulation overhead for port scheduling purposes, the system determines the following values:

- **Offered-load** — The offered-load of a queue is calculated by starting with the queue depth in octets, adding the received octets at the queue and subtracting queue discard octets. The result is the number of octets the queue has available to transmit. This is the packet based offered-load.

- **Frame encapsulation overhead** — Using the avg-frame-overhead parameter, the frame encapsulation overhead is simply the queue’s current offered-load (how much has been received by the queue) multiplied by the avg-frame-overhead. If a queue had an offered load of 10000 octets and the avg-frame-overhead equals 10%, the frame encapsulation overhead would be 10000 x 0.1 or 1000 octets.

For egress Ethernet queues, the frame encapsulation overhead is calculated by multiplying the number of offered-packets for the queue by 20 bytes. If a queue was offered 50 packets then the frame encapsulation overhead would be 50 x 20 or 1000 octets.

- **Frame based offered-load** — The frame based offered-load is calculated by adding the offered-load to the frame encapsulation overhead. If the offered-load is 10000 octets and the encapsulation overhead was 1000 octets, the frame based offered-load would equal 11000 octets.

- **Packet to frame factor** — The packet to frame factor is calculated by dividing the frame encapsulation overhead by the queue’s offered-load (packet based). If the frame encapsulation overhead is 1000 octets and the offered-load is 10000 octets then the packet to frame factor would be 1000 / 10000 or 0.1. When in use, the avg-frame-overhead will be the same as the packet to frame factor making this calculation unnecessary.

- **Frame based CIR** — The frame based CIR is calculated by multiplying the packet to frame factor with the queue’s configured CIR and then adding that result to that CIR. If the queue CIR is set at 500 octets and the packet to frame factor equals 0.1, the frame based CIR would be 500 x 1.1 or 550 octets.

- **Frame based within-cir offered-load** — The frame based within-cir offered-load is the portion of the frame based offered-load considered to be within the frame-based CIR. The frame based within-cir offered-load is the lesser of the frame based offered-load and the frame based CIR. If the frame based offered-load equaled 11000 octets and the frame based CIR equaled 550 octets, the frame based within-cir offered-load would be limited to 550 octets. If the frame based offered-load equaled 450 octets and the frame based CIR equaled 550 octets, the frame based within-cir offered-load would equal 450 octets (or the entire frame based offered-load).

As a special case, when a queue or associated intermediate scheduler is configured with a CIR-weight equal to 0, the system automatically sets the queue’s frame based within-cir offered-load to 0, preventing it from receiving bandwidth during the port scheduler’s within-cir pass.

- **Frame based PIR** — The frame based PIR is calculated by multiplying the packet to frame factor with the queue’s configured PIR and then adding the result to that PIR. If the queue PIR is set to 7500 octets and the packet to frame factor equals 0.1, the frame based PIR would be 7500 x 1.1 or 8250 octets.

- **Frame based within-pir offered-load** — The frame based within-pir offered-load is the portion of the frame based offered-load considered to be within the frame based PIR. The frame based within-pir offered-load is the lesser of the frame based offered-load and the frame based PIR. If the frame based offered-load equaled 11000 octets and the frame based PIR equaled 8250 octets, the frame based within-pir offered-load would be limited to 8250 octets. If the frame based offered-load equaled 7000 octets and the frame based PIR equaled 8250 octets, the frame based within-pir offered load would equal 7000 octets.
Port scheduler operation using frame transformed rates — The port scheduler uses the frame based rates to
determine the maximum rates that each queue may receive during the within-cir and above-cir bandwidth
allocation passes. During the within-cir pass, a queue may receive up to its frame based within-cir offered-
load. The maximum it may receive during the above-cir pass is the difference between the frame based
within-pir offered load and the amount of actual bandwidth allocated during the within-cir pass.

SAP and subscriber SLA-profile average frame overhead override — The average frame overhead
parameter on a sap-egress may be overridden at an individual egress queue basis. On each SAP and within
the sla-profile policy used by subscribers an avg-frame-overhead command may be defined under the queue-
override context for each queue. When overridden, the queue instance will use its local value for the average
frame overhead instead of the sap-egress defined overhead.

The no form of this command restores the average frame overhead parameter for the queue to the default
value of 0 percent. When set to 0, the system uses the packet based queue statistics for calculating port
scheduler priority bandwidth allocation. If the no avg-frame-overhead command is executed in a queue-
override queue id context, the avg-frame-overhead setting for the queue within the sap-egress QoS policy
takes effect.

Default 0

Parameters percent — This parameter sets the average amount of packet-to-frame encapsulation overhead expected for
the queue. This value is not used by the system for egress Ethernet queues.

Values 0 — 100

cbs

Syntax cbs size-in-kbytes
no cbs

Context config>service>ies>if>sap>egress>queue-override>queue
config>service>ies>if>sap>ingress>queue-override>queue

Description This command can be used to override specific attributes of the specified queue’s CBS parameters. It is
permissible, and possibly desirable, to oversubscribe the total CBS reserved buffers for a given access port
egress buffer pool. Oversubscription may be desirable due to the potential large number of service queues
and the economy of statistical multiplexing the individual queue’s CBS setting into the defined reserved
total.

When oversubscribing the reserved total, it is possible for a queue depth to be lower than its CBS setting and
still not receive a buffer from the buffer pool for an ingress frame. As more queues are using their CBS
buffers and the total in use exceeds the defined reserved total, essentially the buffers are being removed from
the shared portion of the pool without the shared in use average and total counts being decremented. This
can affect the operation of the high and low priority RED slopes on the pool, causing them to miscalculate
when to start randomly drop packets.

If the CBS value is larger than the MBS value, an error will occur, preventing the CBS change.

The no form of this command returns the CBS size to the default value.

Default no cbs
IES Filter and QoS Policy Commands

Parameters

size-in-kbytes — The size parameter is an integer expression of the number of kilobytes reserved for the queue. If a value of 10KBytes is desired, enter the value 10. A value of 0 specifies that no reserved buffers are required by the queue (a minimal reserved size can still be applied for scheduling purposes).

Values

0 — 131072, default

high-prio-only

Syntax

high-prio-only percent
no high-prio-only

Context

config>service>ies>if>sap>egress>queue-override>queue
config>service>ies>if>sap>ingress>queue-override>queue

Description

This command can be used to override specific attributes of the specified queue’s high-prio-only parameters. The high-prio-only command configures the percentage of buffer space for the queue, used exclusively by high priority packets.

The priority of a packet can only be set in the SAP ingress QoS policy and is only applicable on the ingress queues for a SAP. The high-prio-only parameter is used to override the default value derived from the network-queue command.

The defined high-prio-only value cannot be greater than the MBS size of the queue. Attempting to change the MBS to a value smaller than the high priority reserve will generate an error and fail execution.

Attempting to set the high-prio-only value larger than the current MBS size will also result in an error and fail execution.

The no form of this command restores the default high priority reserved size.

Parameters

percent — The percent parameter is the percentage reserved for high priority traffic on the queue. If a value of 10KBytes is desired, enter the value 10. A value of 0 specifies that none of the MBS of the queue will be reserved for high priority traffic. This does not affect RED slope operation for packets attempting to be queued.

Values

0 — 100, default

mbs

Syntax

mbs {size-in-kbytes | default}
no mbs

Context

config>service>ies>if>sap>egress>queue-override>queue
config>service>ies>if>sap>ingress>queue-override>queue
config>service>ies>if>sap>hsmda-queue-override>queue

Description

This command can be used to override specific attributes of the specified queue’s MBS parameters. The MBS is a mechanism to override the default maximum size for the queue.

The sum of the MBS for all queues on an egress access port can oversubscribe the total amount of buffering available. When congestion occurs and buffers become scarce, access to buffers is controlled by the RED slope a packet is associated with. A queue that has not exceeded its MBS size is not guaranteed that a buffer will be available when needed or that the packet’s RED slope will not force the discard of the packet. Setting
proper CBS parameters and controlling CBS oversubscription is one major safeguard to queue starvation (when a queue does not receive its fair share of buffers). Another is properly setting the RED slope parameters for the needs of services on this port or channel.

If the CBS value is larger than the MBS value, an error will occur, preventing the MBS change.

The no form of this command returns the MBS size assigned to the queue.

**Default**
default

**Parameters**

- **size-in-kbytes** — The size parameter is an integer expression of the maximum number of kilobytes of buffering allowed for the queue. For a value of 100 kbps, enter the value 100. A value of 0 causes the queue to discard all packets.

<table>
<thead>
<tr>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 — 131072 or default</td>
</tr>
</tbody>
</table>

**rate**

**Syntax**

```
rate pir-rate [cir cir-rate]
no rate
```

**Context**

```
config>service>ies>if>egress>queue-override>queue
config>service>ies>if>ingress>queue-override>queue
config>service>ies>if>egress>sched-override>scheduler
```

**Description**

This command can be used to override specific attributes of the specified queue’s Peak Information Rate (PIR) and the Committed Information Rate (CIR) parameters.

The PIR defines the maximum rate that the queue can transmit packets out an egress interface (for SAP egress queues). Defining a PIR does not necessarily guarantee that the queue can transmit at the intended rate. The actual rate sustained by the queue can be limited by oversubscription factors or available egress bandwidth.

The CIR defines the rate at which the system prioritizes the queue over other queues competing for the same bandwidth. In-profile packets are preferentially queued by the system at egress and at subsequent next hop nodes where the packet can traverse. To be properly handled as in- or out-of-profile throughout the network, the packets must be marked accordingly for profiling at each hop.

The CIR can be used by the queue’s parent commands cir-level and cir-weight parameters to define the amount of bandwidth considered to be committed for the child queue during bandwidth allocation by the parent scheduler.

The **rate** command can be executed at any time, altering the PIR and CIR rates for all queues created through the association of the SAP egress QoS policy with the **queue-id**.

The no form of the command returns all queues created with the **queue-id** by association with the QoS policy to the default PIR and CIR parameters (**max**, 0).

**Default**

```
rate max cir 0 — The max default specifies the amount of bandwidth in kilobits per second (thousand bits per second). The max value is mutually exclusive to the pir-rate value.
```

**Parameters**

- **pir-rate** — Defines the administrative PIR rate, in kilobits, for the queue. When the **rate** command is executed, a valid PIR setting must be explicitly defined. When the **rate** command has not been executed, the default PIR of **max** is assumed.
  Fractional values are not allowed and must be given as a positive integer.
IES Filter and QoS Policy Commands

The actual PIR rate is dependent on the queue’s adaptation-rule parameters and the actual hardware where the queue is provisioned.

**Values**

1 — 100000000

**Default**

max

**cir** — The cir parameter overrides the default administrative CIR used by the queue. When the rate command is executed, a CIR setting is optional. When the rate command has not been executed or the cir parameter is not explicitly specified, the default CIR (0) is assumed. Fractional values are not allowed and must be given as a positive integer. The sum keyword specifies that the CIR be used as the summed CIR values of the children schedulers or queues.

**Values**

0 — 100000000, max, sum

**Default**

0

### scheduler-override

**Syntax**

[no] scheduler-override

**Context**

config>service>ies>if>sap>egress
config>service>ies>if>sap>ingress

**Description**

This command specifies the set of attributes whose values have been overridden via management on this virtual scheduler. Clearing a given flag will return the corresponding overridden attribute to the value defined on the SAP's ingress scheduler policy.

### scheduler

**Syntax**

[no] scheduler scheduler-name

**Context**

config>service>ies>if>sap>egress>sched-override
config>service>ies>if>sap>ingress>sched-override

**Description**

This command can be used to override specific attributes of the specified scheduler name.

A scheduler defines a bandwidth controls that limit each child (other schedulers and queues) associated with the scheduler. Scheduler objects are created within the hierarchical tiers of the policy. It is assumed that each scheduler created will have queues or other schedulers defined as child associations. The scheduler can be a child (take bandwidth from a scheduler in a higher tier, except for schedulers created in tier 1). A total of 32 schedulers can be created within a single scheduler policy with no restriction on the distribution between the tiers.

Each scheduler must have a unique name within the context of the scheduler policy; however the same name can be reused in multiple scheduler policies. If scheduler-name already exists within the policy tier level (regardless of the inclusion of the keyword create), the context changes to that scheduler name for the purpose of editing the scheduler parameters. Modifications made to an existing scheduler are executed on all instantiated schedulers created through association with the policy of the edited scheduler. This can cause queues or schedulers to become orphaned (invalid parent association) and adversely affect the ability of the system to enforce service level agreements (SLAs).

If the scheduler-name exists within the policy on a different tier (regardless of the inclusion of the keyword create)...
create), an error occurs and the current CLI context will not change.

If the scheduler-name does not exist in this or another tier within the scheduler policy, it is assumed that an attempt is being made to create a scheduler of that name. The success of the command execution is dependent on the following:

1. The maximum number of schedulers has not been configured.
2. The provided scheduler-name is valid.
3. The create keyword is entered with the command if the system is configured to require it (enabled in the environment create command).

When the maximum number of schedulers has been exceeded on the policy, a configuration error occurs and the command will not execute, nor will the CLI context change.

If the provided scheduler-name is invalid according to the criteria below, a name syntax error will occur, the command will not execute, and the CLI context will not change.

**Parameters**

scheduler-name — The name of the scheduler.

**Values**

Valid names consist of any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

**Default**

None. Each scheduler must be explicitly created.

create — This optional keyword explicitly specifies that it is acceptable to create a scheduler with the given scheduler-name. If the create keyword is omitted, scheduler-name is not created when the system environment variable create is set to true. This safeguard is meant to avoid accidental creation of system objects (such as schedulers) while attempting to edit an object with a mistyped name or ID. The keyword has no effect when the object already exists.

**rate**

**Syntax**

rate pir-rate [cir cir-rate]
no rate

**Context**

config>service>ies>if>egress>sched-override>scheduler
config>service>ies>if>ap ingress>sched-override>scheduler

**Description**

This command can be used to override specific attributes of the specified scheduler rate. The rate command defines the maximum bandwidth that the scheduler can offer its child queues or schedulers. The maximum rate is limited to the amount of bandwidth the scheduler can receive from its parent scheduler. If the scheduler has no parent, the maximum rate is assumed to be the amount available to the scheduler. When a parent is associated with the scheduler, the CIR parameter provides the amount of bandwidth to be considered during the parent scheduler’s ‘within CIR’ distribution phase.

The actual operating rate of the scheduler is limited by bandwidth constraints other than its maximum rate. The scheduler’s parent scheduler may not have the available bandwidth to meet the scheduler’s needs or the bandwidth available to the parent scheduler could be allocated to other child schedulers or child queues on the parent based on higher priority. The children of the scheduler may not need the maximum rate available to the scheduler due to insufficient offered load or limits to their own maximum rates.

When a scheduler is defined without specifying a rate, the default rate is max. If the scheduler is a root scheduler (no parent defined), the default maximum rate must be changed to an explicit value. Without this
explicit value, the scheduler will assume that an infinite amount of bandwidth is available and allow all child queues and schedulers to operate at their maximum rates.

The **no** form of this command returns all queues created with this *queue-id* by association with the QoS policy to the default PIR and CIR parameters.

**Parameters**

*pir-rate* — The *pir* parameter accepts a step-multiplier value that specifies the multiplier used to determine the PIR rate at which the queue will operate. A value of 0 to 100000000 or the keyword **max** is accepted. Any other value will result in an error without modifying the current PIR rate.

To calculate the actual PIR rate, the rate described by the queue’s *rate* is multiplied by the *pir-rate*.

The SAP ingress context for PIR is independent of the defined forwarding class (fc) for the queue. The default *pir* and definable range is identical for each class. The PIR in effect for a queue defines the maximum rate at which the queue will be allowed to forward packets in a given second, thus shaping the queue’s output.

The PIR parameter for SAP ingress queues do not have a negate (**no**) function. To return the queue’s PIR rate to the default value, that value must be specified as the PIR value.

**Values**

1 — 100000000, **max**

**Default**

**max**

*cir-rate* — This parameter accepts a step-multiplier value that specifies the multiplier used to determine the CIR rate at which the queue will operate. A value of 0 — 10000000 or the keyword **max** or **sum** is accepted. Any other value will result in an error without modifying the current CIR rate.

To calculate the actual CIR rate, the rate described by the *rate pir-rate* is multiplied by the *cir-rate*. If the *cir* is set to max, then the CIR rate is set to infinity.

The SAP ingress context for CIR is dependent on the defined forwarding class (fc) for the queue. The default CIR and definable range is different for each class. The CIR in effect for a queue defines both its profile (in or out) marking level as well as the relative importance compared to other queues for scheduling purposes during congestion periods. The **sum** keyword specifies that the CIR be used as the summed CIR values of the children schedulers or queues.

**Values**

0 — 10000000, **max**, **sum**

**Default**

**sum**

**scheduler-policy**

**Syntax**

`scheduler-policy scheduler-policy-name`

`no scheduler-policy`

**Context**

`config>service>ies>sap>ingress`

`config>service>ies>sap>egress`

**Description**

This command applies an existing scheduler policy to an ingress or egress scheduler used by SAP queues associated with this multi-service customer site. The schedulers defined in the scheduler policy can only be created once the customer site has been appropriately assigned to a chassis port, channel or slot. Scheduler policies are defined in the `config>qos>scheduler-policy scheduler-policy-name` context.

The **no** form of this command removes the configured ingress or egress scheduler policy from the multi-service customer site. When the policy is removed, the schedulers created due to the policy are removed also.
making them unavailable for the ingress SAP queues associated with the customer site. Queues that lose their parent scheduler association are deemed to be orphaned and are no longer subject to a virtual scheduler. The SAPs that have ingress queues reliant on the removed schedulers enter into an operational state depicting the orphaned status of one or more queues. When the no scheduler-policy command is executed, the customer site ingress or egress node will not contain an applied scheduler policy.

scheduler-policy-name: — The scheduler-policy-name parameter applies an existing scheduler policy that was created in the config>qos>scheduler-policy scheduler-policy-name context to create the hierarchy of ingress or egress virtual schedulers. The scheduler names defined within the policy are created and made available to any ingress or egress queues created on associated SAPs.

Values  Any existing valid scheduler policy name.
IES Interface VRRP Commands

vrrp

Syntax:  
```
  vrrp virtual-router-id [owner]
  no vrrp virtual-router-id
```

Context:  
```
config>service>ies>if
```

Description:  
This command creates or edits a Virtual Router ID (VRID) on the service IP interface. A VRID is internally represented in conjunction with the IP interface name. This allows the VRID to be used on multiple IP interfaces while representing different virtual router instances.

Two VRRP nodes can be defined on an IP interface. One, both, or none may be defined as owner. The nodal context of `vrrp virtual-router-id` is used to define the configuration parameters for the VRID.

The `no` form of this command removes the specified VRID from the IP interface. This terminates VRRP participation for the virtual router and deletes all references to the vrid. The VRID does not need to be shutdown in order to remove the virtual router instance.

Default:  
No default

Parameters:  
```
virtual-router-id — The virtual-router-id parameter specifies a new virtual router ID or one that can be modified on the IP interface.
```

Values:  
```
1 — 255
```

authentication-key

Syntax:  
```
  authentication-key [authentication-key | hash-key] [hash | hash2]
  no authentication-key
```

Context:  
```
config>service>ies>if>vrrp
```

Description:  
The `authentication-key` command, within the `vrrp virtual-router-id` context, is used to assign a simple text password authentication key to generate master VRRP advertisement messages and validating received VRRP advertisement messages.

The authentication-key command is one of the few commands not affected by the presence of the owner keyword. If simple text password authentication is not required, the authentication-key command is not required. If the command is re-executed with a different password key defined, the new key will be used immediately. If a `no` authentication-key command is executed, the password authentication key is restored to the default value. The authentication-key command may be executed at any time, altering the simple text password used when authentication-type password authentication method is used by the virtual router instance. The authentication-type password command does not need to be executed prior to defining the authentication-key command.

To change the current in-use password key on multiple virtual router instances:

- Identify the current master
- Shutdown the virtual router instance on all backups
• Execute the authentication-key command on the master to change the password key
• Execute the authentication-key command and no shutdown command on each backup key

The no form of this command restores the default null string to the value of key.

**Default**
No default. The authentication data field contains the value 0 in all 16 octets.

**Parameters**
- **authentication-key** — The key parameter identifies the simple text password used when VRRP Authentication Type 1 is enabled on the virtual router instance. Type 1 uses a string eight octets long that is inserted into all transmitted VRRP advertisement messages and compared against all received VRRP advertisement messages. The authentication data fields are used to transmit the key.

The key parameter is expressed as a string consisting up to eight alpha-numeric characters. Spaces must be contained in quotation marks (" "). The quotation marks are not considered part of the string.

The string is case sensitive and is left-justified in the VRRP advertisement message authentication data fields. The first field contains the first four characters with the first octet (starting with IETF RFC bit position 0) containing the first character. The second field holds the fifth through eighth characters. Any unspecified portion of the authentication data field is padded with the value 0 in the corresponding octet.

**Values**
Any 7-bit printable ASCII character.

**Exceptions:**
- Double quote (") ASCII 34
- Carriage Return ASCII 13
- Line Feed ASCII 10
- Tab ASCII 9
- Backspace ASCII 8

**hash-key** — The hash key. The key can be any combination of ASCII characters up to 22 characters in length (encrypted). If spaces are used in the string, enclose the entire string in quotation marks (“ ”). This is useful when a user must configure the parameter, but, for security purposes, the actual unencrypted key value is not provided.

**hash** — Specifies the key is entered in an encrypted form. If the hash parameter is not used, the key is assumed to be in a non-encrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the hash parameter specified.

**hash2** — Specifies the key is entered in a more complex encrypted form. If the hash2 parameter is not used, the less encrypted hash form is assumed.

---

**authentication-type**

**Syntax**
```
authentication-type {password | message-digest}
```

**no authentication-type**

**Context**
```
config>service>ies>if>vrrp
```

**Description**
The **authentication-type** command, within the **vrrp virtual-router-id** context, is used to assign the authentication method to generate master VRRP advertisement messages and validate received VRRP advertisement messages.

**NOTE:** The authentication management for VRRP closely follows the authentication management format used for IS-IS.

The **authentication-type** command is one of the commands not affected by the presence of the owner
keyword. If authentication is not required, the authentication-type command must not be executed. If the command is re-executed with a different authentication type defined, the new type will be used. If the no authentication-type command is executed, authentication is removed and no authentication is performed. The authentication-type command may be executed at any time, altering the authentication method used by the virtual router instance.

The **no** form of this command removes authentication from the virtual router instance. All VRRP Advertisement messages sent will have the Authentication Type field set to 0 and the Authentication Data fields will contain 0 in all octets. VRRP Advertisement messages received with Authentication Type fields containing a value other than 0 will be discarded.

**password** — The password keyword identifies VRRP Authentication Type 1. Type 1 requires the definition of a string of eight octets long using the authentication-key command. All transmitted VRRP Advertisement messages must have the Authentication Type field set to 1 and the Authentication Data fields must contain the authentication-key password.

All received VRRP advertisement messages must contain a value of 1 in the Authentication Type field and the Authentication Data fields must match the defined authentication-key. All other received messages will be silently discarded.

**message-digest** — The message-digest keyword identifies VRRP Authentication Type 2. Type 2 defines a lower IP layer MD5 authentication mechanism using HMAC and IP authentication header standards. An MD5 key must be defined using the message-digest-key command. All transmitted VRRP advertisement messages must have the Authentication Type field set to 2 and the Authentication Data fields must contain 0 in all octets. The message-digest key is used in the hashing process when populating the IP Authentication Header fields. A sequential incrementing counter (set to zero when the message-digest-key is set) is incremented and then used in the IP Authentication Header to prevent replay attacks on authorized participating virtual router instances.

All received VRRP advertisement messages must contain a value of 2 in the Authentication Type field and the Authentication Data fields are ignored. The message must have been authorized by the lower layer IP Authentication Header process with the sequential counter field and the source IP address presented to the virtual router instance. To track the validity of the received counter, the virtual router instance maintains a master counter table containing up to 32 source IP addresses and the last received counter value. Populate the table as follows:

1. Check to see if source IP address exists in table.
   
   **Output**
   
   If non-existent, create an entry if available.
   
   - If no entry is available, delete the oldest and create an entry.
     The new entry should have a counter value of zero.
   
   2. Compare the message counter value to the entry value (0 if new entry or equal to the previous message counter from the source IP address).
     
     - If the message counter is not greater than the entry counter value, silently discard the packet.
     
     - If the message counter is greater than the entry counter value, accept the message for further checking and replace the entry counter value with the message counter value and time stamp the entry.
backup

Syntax  [no] backup ip-address

Context  config>service>ies>if>vrrp

Description  This command configures virtual router IP addresses for the interface.

bfd-enable

Syntax  [no] bfd-enable [service-id] interface interface-name dst-ip ip-address

Context  config>service>ies>if>vrrp
          config>service>ies>if>ipv6>vrrp

Description  This command assigns a bi-directional forwarding (BFD) session providing heart-beat mechanism for the given VRRP/SRRP instance. There can be only one BFD session assigned to any given VRRP/SRRP instance, but there can be multiple SRRP/VRRP sessions using the same BFD session.

BFD control the state of the associated interface. By enabling BFD on a given protocol interface, the state of the protocol interface is tied to the state of the BFD session between the local node and the remote node. The parameters used for the BFD are set via the BFD command under the IP interface. The specified interface may not be configured with BFD; however, when it is, the virtual router will then initiate the BFD session.

The no form of this command removes BFD from the configuration.

Default  none

Parameters  service-id — Specifies the service ID of the interface running BFD.

          Values  service-id: 1 — 2147483648

          Values  No service ID indicates a network interface.

          interface interface-name — Specifies the name of the interface running BFD.

          dst-ip ip-address — Specifies the destination address to be used for the BFD session.

init-delay

Syntax  init-delay seconds
          no init-delay

Context  config>service>ies>if>vrrp

Description  This command configures a VRRP initialization delay timer.

Default  no init-delay

Parameters  seconds — Specifies the initialization delay timer for VRRP, in seconds.

          Values  1 — 65535
IES Filter and QoS Policy Commands

mac

Syntax  
```
mac mac-address
no mac
```

Context  config>service>ies>if>vrrp

Description  This command assigns a specific MAC address to an IES IP interface. The no form of the command returns the MAC address of the IP interface to the default value.

Default  The physical MAC address associated with the Ethernet interface that the SAP is configured on (the default MAC address assigned to the interface, assigned by the system).

Parameters  
- `mac-address` — Specifies the 48-bit MAC address for the static ARP in the form aa:bb:cc:dd:ee:ff or aa-bb-cc-dd-ee-ff where aa, bb, cc, dd, ee, and ff are hexadecimal numbers. Allowed values are any non-broadcast, non-multicast MAC and non-IEEE reserved MAC addresses.

master-int-inherit

Syntax  
```
[no] master-int-inherit
```

Context  config>service>ies>if>vrrp

Description  This command allows the master instance to dictate the master down timer (non-owner context only).

Default  no master-int-inherit

message-interval

Syntax  
```
message-interval {{seconds} {milliseconds milliseconds}}
no message-interval
```

Context  config>service>ies>if>vrrp

Description  This command sets the advertisement timer and indirectly sets the master down timer on the virtual router instance. The message-interval setting must be the same for all virtual routers participating as a virtual router. Any VRRP advertisement message received with an Advertisement Interval field different than the virtual router instance configured message-interval value will be silently discarded.

The message-interval command is available in both non-owner and owner vrrp virtual-router-id nodal contexts. If the message-interval command is not executed, the default message interval of 1 second will be used.

The no form of this command restores the default message interval value of 1 second to the virtual router instance.

Parameters  
- `seconds` — The number of seconds that will expire before the advertisement timer expires.
  - Values  
    - 1 — 255
  - Default  
    - 1

7950 SR  OS Services Guide
milliseconds milliseconds — Specifies the time interval, in milliseconds, between sending advertisement messages. This parameter is not supported on non-redundant chassis.

Values 100 — 900

ping-reply

Syntax ping-reply
no ping-reply

Context config>service>ies>if>vrrp

Description This command enables the non-owner master to reply to ICMP Echo Requests directed at the virtual router instances IP addresses. The ping request can be received on any routed interface.

Ping must not have been disabled at the management security level (either on the parental IP interface or based on the Ping source host address). When ping-reply is not enabled, ICMP Echo Requests to non-owner master virtual IP addresses are silently discarded.

Non-owner backup virtual routers never respond to ICMP Echo Requests regardless of the setting of ping-reply configuration.

The ping-reply command is only available in non-owner vrrp virtual-router-id nodal context. If the ping-reply command is not executed, ICMP Echo Requests to the virtual router instance IP addresses will be silently discarded.

The no form of this command restores the default operation of discarding all ICMP Echo Request messages destined to the non-owner virtual router instance IP addresses.

Default no ping-reply

policy

Syntax policy vrrp-policy-id
no policy

Context config>service>ies>if>vrrp

Description This command creates VRRP control policies. The VRRP policy ID must be created by the policy command prior to association with the virtual router instance.

The policy command provides the ability to associate a VRRP priority control policy to a virtual router instance. The policy may be associated with more than one virtual router instance. The priority events within the policy either override or diminish the base-priority dynamically affecting the in-use priority. As priority events clear in the policy, the in-use priority may eventually be restored to the base-priority value.

The policy command is only available in the non-owner vrrp virtual-router-id nodal context. The priority of owner virtual router instances is permanently set to 255 and cannot be changed by VRRP priority control policies. For non-owner virtual router instances, if the policy command is not executed, the base-priority will be used as the in-use priority.

The no form of this command removes any existing VRRP priority control policy association from the virtual router instance. All such associations must be removed prior to the policy being deleted from the system.
IES Filter and QoS Policy Commands

**Default** None

**Parameters**
- `vrrp-policy-id` — The vrrp-policy-id parameter associated the corresponding VRRP priority control policy-id with the virtual router instance. The vrrp-policy-id must already exist in the system for the policy command to be successful.

**Values** 1 to 9999

### preempt

**Syntax**
- `preempt`
- `no preempt`

**Context** `config>service>ies>if>vrrp`

**Description**
The preempt command provides the ability of overriding an existing non-owner master to the virtual router instance. Enabling preempt mode is almost required for proper operation of the base-priority and vrrp-policy-id definitions on the virtual router instance. If the virtual router cannot preempt an existing non-owner master, the affect of the dynamic changing of the in-use priority is greatly diminished.

The preempt command is only available in the non-owner vrrp virtual-router-id nodal context. The owner may not be preempted due to the fact that the priority of non-owners can never be higher than the owner. The owner will always preempt all other virtual routers when it is available.

Non-owner virtual router instances will only preempt when preempt is set and the current master has an in-use message priority value less than the virtual router instances in-use priority.

A master non-owner virtual router will only allow itself to be preempted when the incoming VRRP Advertisement message Priority field value is one of the following:

- Greater than the virtual router in-use priority value
- Equal to the in-use priority value and the source IP address (primary IP address) is greater than the virtual router instance primary IP address

The `no` form of this command prevents a non-owner virtual router instance from preempting another, less desirable virtual router. Use the preempt command to restore the default mode.

**Default** `preempt`

### priority

**Syntax**
- `priority base-priority`
- `no priority`

**Context** `config>service>ies>if>vrrp`

**Description**
The priority command provides the ability to configure a specific priority value to the virtual router instance. In conjunction with an optional policy command, the base-priority is used to derive the in-use priority of the virtual router instance.

The priority command is only available in the non-owner vrrp virtual-router-id nodal context. The priority of owner virtual router instances is permanently set to 255 and cannot be changed. For non-owner virtual router instances, if the priority command is not executed, the base-priority will be set to 100.
The **no** form of this command restores the default value of 100 to base-priority.

**Parameters**

*base-priority* — The base-priority parameter configures the base priority used by the virtual router instance. If a VRRP Priority Control policy is not also defined, the base-priority will be the in-use priority for the virtual router instance.

<table>
<thead>
<tr>
<th>Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 — 254</td>
<td>100</td>
</tr>
</tbody>
</table>

**standby-forwarding**

**Syntax**  

[no] standby-forwarding

**Context**  

config>service>ies>if>vrrp

**Description**  

This command allows the forwarding of packets by a standby router. The **no** form of the command specifies that a standby router should not forward traffic sent to virtual router's MAC address. However, the standby router should forward traffic sent to the standby router’s real MAC address.

**Default**  

no standby-forwarding

**ssh-reply**

**Syntax**  

[no] ssh-reply

**Context**  

config>service>ies>if>vrrp

**Description**  

This command enables the non-owner master to reply to SSH Requests directed at the virtual router instances IP addresses. The SSH request can be received on any routed interface. SSH must not have been disabled at the management security level (either on the parental IP interface or based on the SSH source host address). Proper login and CLI command authentication is still enforced.

When ssh-reply is not enabled, SSH packets to non-owner master virtual IP addresses are silently discarded. Non-owner backup virtual routers never respond to SSH regardless of the ssh-reply configuration.

The ssh-reply command is only available in non-owner vrrp virtual-router-id nodal context. If the ssh-reply command is not executed, SSH packets to the virtual router instance IP addresses will be silently discarded. The **no** form of this command restores the default operation of discarding all SSH packets destined to the non-owner virtual router instance IP addresses.

**Default**  

no ssh-reply

**telnet-reply**

**Syntax**  

[no] telnet-reply

**Context**  

config>service>ies>if>vrrp
IES Filter and QoS Policy Commands

**Description**  
The telnet-reply command enables the non-owner master to reply to TCP port 23 Telnet Requests directed at the virtual router instances IP addresses. The Telnet request can be received on any routed interface. Telnet must not have been disabled at the management security level (either on the parental IP interface or based on the Telnet source host address). Proper login and CLI command authentication is still enforced.

When telnet-reply is not enabled, TCP port 23 Telnet packets to non-owner master virtual IP addresses are silently discarded.

Non-owner backup virtual routers never respond to Telnet Requests regardless of the telnet-reply configuration.

The telnet-reply command is only available in non-owner VRRP nodal context. If the telnet-reply command is not executed, Telnet packets to the virtual router instance IP addresses will be silently discarded.

The **no** form of this command restores the default operation of discarding all Telnet packets destined to the non-owner virtual router instance IP addresses.

**Default**  
no telnet-reply

**traceroute-reply**

**Syntax**  
[no] traceroute-reply

**Context**  
config>service>ies>if>vrrp

**Description**  
This command is valid only if the VRRP virtual router instance associated with this entry is a non-owner.

When this command is enabled, a non-owner master can reply to traceroute requests directed to the virtual router instance IP addresses.

A non-owner backup virtual router never responds to such traceroute requests regardless of the **trace-route-reply** status.

**Default**  
no traceroute-reply
Virtual Private Routed Network Service

In This Chapter

This chapter provides information about the Virtual Private Routed Network (VPN) service and implementation notes.

Topics in this chapter include:

- VPRN Service Overview on page 1188
- VPRN Features on page 1205
  - IP Interfaces on page 1205
  - Object Grouping and State Monitoring on page 1207
  - SAPs on page 1209
  - QoS Policies on page 1210
  - Filter Policies on page 1210
  - DSCP Marking on page 1211
  - CE to PE Routing Protocols on page 1214
  - PE to PE Tunneling Mechanisms on page 1214
  - Per VRF Route Limiting on page 1214
  - Spoke SDPs on page 1215
  - Carrier Supporting Carrier (CsC) on page 1220
  - Traffic Leaking to GRT on page 1223
  - Service Label Mode of a VPRN on page 1228
  - Multicast in IP-VPN Applications on page 1229
- Configuring a VPRN Service with CLI on page 1253
- Common Configuration Tasks on page 1256
- Service Management Tasks on page 1269
RFC 2547b is an extension to the original RFC 2547, *BGP/MPLS VPNs*, which details a method of distributing routing information using BGP and MPLS forwarding data to provide a Layer 3 Virtual Private Network (VPN) service to end customers.

Each Virtual Private Routed Network (VPRN) consists of a set of customer sites connected to one or more PE routers. Each associated PE router maintains a separate IP forwarding table for each VPRN. Additionally, the PE routers exchange the routing information configured or learned from all customer sites via MP-BGP peering. Each route exchanged via the MP-BGP protocol includes a Route Distinguisher (RD), which identifies the VPRN association and handles the possibility of IP address overlap.

The service provider uses BGP to exchange the routes of a particular VPN among the PE routers that are attached to that VPN. This is done in a way which ensures that routes from different VPNs remain distinct and separate, even if two VPNs have an overlapping address space. The PE routers peer with locally connected CE routers and exchange routes with other PE routers in order to provide end-to-end connectivity between CEs belonging to a given VPN. Since the CE routers do not peer with each other there is no overlay visible to the CEs.

When BGP distributes a VPN route, it also distributes an MPLS label for that route. On a SR-Series, the label distributed with a VPN route depends on the configured label-mode of the VPRN that is originating the route.

Before a customer data packet travels across the service provider's backbone, it is encapsulated with the MPLS label that corresponds, in the customer's VPN, to the route which best matches the packet's destination address. The MPLS packet is further encapsulated with one or additional MPLS labels or GRE tunnel header so that it gets tunneled across the backbone to the proper PE router. Each route exchanged by the MP-BGP protocol includes a route distinguisher (RD), which identifies the VPRN association. Thus the backbone core routers do not need to know the VPN routes. Figure 145 displays a VPRN network diagram example.
Figure 145: Virtual Private Routed Network
Routing Prerequisites

RFC4364 requires the following features:

- Multi-protocol extensions to BGP
- Extended BGP community support
- BGP capability negotiation

Tunneling protocol options are as follows:

- Label Distribution Protocol (LDP)
- MPLS RSVP-TE tunnels
- Generic Router Encapsulation (GRE) tunnels
- BGP route tunnel (RFC3107)
Core MP-BGP Support

BGP is used with BGP extensions mentioned in Routing Prerequisites on page 1190 to distribute VPRN routing information across the service provider’s network.

BGP was initially designed to distribute IPv4 routing information. Therefore, multi-protocol extensions and the use of a VPN-IP address were created to extend BGP’s ability to carry overlapping routing information. A VPN-IPv4 address is a 12-byte value consisting of the 8-byte route distinguisher (RD) and the 4-byte IPv4 IP address prefix. A VPN-IPv6 address is a 24-byte value consisting of the 8-byte RD and 16-byte IPv6 address prefix. Service providers typically assign one or a small number of RDs per VPN service network-wide.
Route Distinguishers

The route distinguisher (RD) is an 8-byte value consisting of two major fields, the **Type** field and **Value** field. The **Type** field determines how the **Value** field should be interpreted. The SR-OS implementation supports the three (3) **Type** values as defined in the standard.

| Type Field (2-bytes) | Value Field (6-bytes) |

**Figure 146: Route Distinguisher**

The three Type values are:

- **Type 0: Value Field** — Administrator subfield (2 bytes)
  Assigned number subfield (4 bytes)
  The administrator field must contain an AS number (using private AS numbers is discouraged). The Assigned field contains a number assigned by the service provider.

- **Type 1: Value Field** — Administrator subfield (4 bytes)
  Assigned number subfield (2 bytes)
  The administrator field must contain an IP address (using private IP address space is discouraged). The Assigned field contains a number assigned by the service provider.

- **Type 2: Value Field** — Administrator subfield (4 bytes)
  Assigned number subfield (2 bytes)
  The administrator field must contain a 4-byte AS number (using private AS numbers is discouraged). The Assigned field contains a number assigned by the service provider.

**eiBGP Load Balancing**

eiBGP load balancing allows a route to have multiple nexthops of different types, using both IPv4 nexthops and MPLS LSPs simultaneously.

**Figure 147** displays a basic topology that could use eiBGP load balancing. In this topology CE1 is dual homed and thus reachable by two separate PE routers. CE 2 (a site in the same VPRN) is also attached to PE1. With eiBGP load balancing, PE1 will utilize its own local IPv4 nexthop as well as the route advertised by MP-BGP, by PE2.
Another example displayed in Figure 148 shows an extra net VPRN (VRF). The traffic ingressing the PE that should be load balanced is part of a second VPRN and the route over which the load balancing is to occur is part of a separate VPRN instance and are leaked into the second VPRN by route policies.

Here, both routes can have a source protocol of VPN-IPv4 but one will still have an IPv4 nexthop and the other can have a VPN-IPv4 nexthop pointing out a network interface. Traffic will still be load balanced (if eiBGP is enabled) as if only a single VRF was involved.
Figure 148: Extranet Load Balancing

Traffic will be load balanced across both the IPv4 and VPN-IPv4 next hops. This helps to use all available bandwidth to reach a dual-homed VPRN.
Route Reflector

The use of Route Reflectors is supported in the service provider core. Multiple sets of route reflectors can be used for different types of BGP routes, including IPv4 and VPN-IPv4.
**CE to PE Route Exchange**

Routing information between the Customer Edge (CE) and Provider Edge (PE) can be exchanged by the following methods:

- Static Routes
- E-BGP
- RIP
- OSPF
- OSPF3

Each protocol provides controls to limit the number of routes learned from each CE router.

---

**Route Redistribution**

Routing information learned from the CE-to-PE routing protocols and configured static routes should be injected in the associated local VPN routing/forwarding (VRF). In the case of dynamic routing protocols, there may be protocol specific route policies that modify or reject certain routes before they are injected into the local VRF.

Route redistribution from the local VRF to CE-to-PE routing protocols is to be controlled via the route policies in each routing protocol instance, in the same manner that is used by the base router instance.

The advertisement or redistribution of routing information from the local VRF to or from the MP-BGP instance is specified per VRF and is controlled by VRF route target associations or by VRF route policies.

VPN-IP routes imported into a VPRN, have the protocol type bgp-vpn to denote that it is an VPRN route. This can be used within the route policy match criteria.
CPE Connectivity Check

Static routes are used within many IES services. Unlike dynamic routing protocols, there is no way to change the state of routes based on availability information for the associated CPE. CPE connectivity check adds flexibility so that unavailable destinations will be removed from the VPRN routing tables dynamically and minimize wasted bandwidth.

Figure 149: Directly Connected IP Target

Figure 150: Multiple Hops to IP Target

The availability of the far-end static route is monitored through periodic polling. The polling period is configured. If the poll fails a specified number of sequential polls, the static route is marked as inactive.

Either ICMP ping or unicast ARP mechanism can be used to test the connectivity. ICMP ping is preferred.

If the connectivity check fails and the static route is de-activated, the SR-Series router will continue to send polls and re-activate any routes that are restored.
Constrained Route Distribution (RT Constraint)

Constrained VPN Route Distribution Based on Route Targets

Constrained Route Distribution (or RT Constraint) is a mechanism that allows a router to advertise Route Target membership information to its BGP peers to indicate interest in receiving only VPN routes tagged with specific Route Target extended communities. Upon receiving this information, peers restrict the advertised VPN routes to only those requested, minimizing control plane load in terms of protocol traffic and possibly also RIB memory.

The Route Target membership information is carried using MP-BGP, using an AFI value of 1 and SAFI value of 132. In order for two routers to exchange RT membership NLRI they must advertise the corresponding AFI/SAFI to each other during capability negotiation. The use of MP-BGP means RT membership NLRI are propagated, loop-free, within an AS and between ASes using well-known BGP route selection and advertisement rules.

ORF can also be used for RT-based route filtering, but ORF messages have a limited scope of distribution (to direct peers) and therefore do not automatically create pruned inter-cluster and inter-AS route distribution trees.

Configuring the Route Target Address Family

RT Constraint is supported only by the base router BGP instance. When the family command at the BGP router group or neighbor CLI context includes the route-target keyword, the RT Constraint capability is negotiated with the associated set of EBGP and IBGP peers.

ORF is mutually exclusive with RT Constraint on a particular BGP session. The CLI will not attempt to block this configuration, but if both capabilities are enabled on a session, the ORF capability will not be included in the OPEN message sent to the peer.

Originating RT Constraint Routes

When the base router has one or more RTC peers (BGP peers with which the RT Constraint capability has been successfully negotiated), one RTC route is created for each RT extended community imported (for unicast connectivity) by locally-configured VPRN services.

By default, these RTC routes are automatically advertised to all RTC peers, without the need for an export policy to explicitly “accept” them. Each RTC route has a prefix, a prefix length and path attributes. The prefix value is the concatenation of the origin AS (a 4 byte value representing the 2- or 4-octet AS of the originating router, as configured using the config>router>autonomous-system command) and 0 or 16-64 bits of a route target extended community encoded in one of the
following formats: 2-octet AS specific extended community, IPv4 address specific extended community, or 4-octet AS specific extended community.

A SR-OS may be configured to send the default RTC route to any RTC peer. This is done using the new `default-route-target` group/neighbor CLI command. The default RTC route is a special type of RTC route that has zero prefix length. Sending the default RTC route to a peer conveys a request to receive all VPN routes (regardless of route target extended community) from that peer. The default RTC route is typically advertised by a route reflector to its clients. The advertisement of the default RTC route to a peer does not suppress other more specific RTC routes from being sent to that peer.

---

**Receiving and Re-Advertising RT Constraint Routes**

All received RTC routes that are deemed valid are stored in the RIB-IN. An RTC route is considered invalid and treated as withdrawn, if any of the following applies:

- The prefix length is 1-31.
- The prefix length is 33-47.
- The prefix length is 48-96 and the 16 most-significant bits are not 0x0002, 0x0102 or 0x0202.

If multiple RTC routes are received for the same prefix value then standard BGP best path selection procedures are used to determine the best of these routes.

The best RTC route per prefix is re-advertised to RTC peers based on the following rules:

- The best path for a default RTC route (prefix-length 0, origin AS only with prefix-length 32, or origin AS plus 16 bits of an RT type with prefix-length 48) is never propagated to another peer.
- A PE with only IBGP RTC peers that is neither a route reflector or an ASBR does not re-advertise the best RTC route to any RTC peer due to standard IBGP split horizon rules.
- A route reflector that receives its best RTC route for a prefix from a client peer re-advertises that route (subject to export policies) to all of its client and non-client IBGP peers (including the originator), per standard RR operation. When the route is re-advertised to client peers, the RR (i) sets the ORIGINATOR_ID to its own router ID and (ii) modifies the NEXT_HOP to be its local address for the sessions (for example, system IP).
- A route reflector that receives its best RTC route for a prefix from a non-client peer re-advertises that route (subject to export policies) to all of its client peers, per standard RR operation. If the RR has a non-best path for the prefix from any of its clients, it advertises the best of the client-advertised paths to all non-client peers.
• An ASBR that is neither a PE nor a route reflector that receives its best RTC route for a prefix from an IBGP peer re-advertises that route (subject to export policies) to its EBGP peers. It modifies the NEXT_HOP and AS_PATH of the re-advertised route per standard BGP rules. No aggregation of RTC routes is supported.

• An ASBR that is neither a PE nor a route reflector that receives its best RTC route for a prefix from an EBGP peer re-advertises that route (subject to export policies) to its EBGP and IBGP peers. When re-advertised routes are sent to EBGP peers, the ASBR modifies the NEXT_HOP and AS_PATH per standard BGP rules. No aggregation of RTC routes is supported.

Note: These advertisement rules do not handle hierarchical RR topologies properly. This is a limitation of the current RT constraint standard.

Using RT Constraint Routes

In general (ignoring IBGP-to-IBGP rules, Add-Path, Best-external, etc.), the best VPN route for every prefix/NLRI in the RIB is sent to every peer supporting the VPN address family, but export policies may be used to prevent some prefix/NLRI from being advertised to specific peers. These export policies may be configured statically or created dynamically based on the support of ORF with specific peers. RT Constraint introduces another mechanism for dynamic modification of export policies. In R10, ORF and RT Constraint are mutually exclusive on a session.

When RT Constraint is configured on a session that also supports VPN address families using route targets (that is, L2-VPN, VPN-IPv4, VPN-IPv6, MVPN, MDT-SAFI), the advertisement of the VPN routes is affected as follows:

• When the session comes up, all L2-VPN, MVPN, and MDT-SAFI routes (subject to manually configured export policies) are advertised immediately, but the advertisement of VPN-IPv4 and VPN-IPv6 routes is delayed for a short while to allow all RTC routes to first be received from the peer.

• After the initial delay, the received RTC routes are acted upon immediately. If S1 is the set of routes previously advertised to the peer and S2 is the set of routes that should be advertised based on the most recent received RTC routes then:
  → Set of routes in S1 but not in S2 should be withdrawn immediately (subject to MRAI).
  → Set of routes in S2 but not in S1 should be advertised immediately (subject to MRAI).

• If a default RTC route is received from an EBGP or IBGP peer P1, the VPN routes that are advertised to P1 is the set of VPN-IPv4 and VPN-IPv6 routes in the LOC-RIB that:
  → (a) are eligible for advertisement to P1 per BGP route advertisement rules AND
  → (b) have not been rejected by manually configured export policies AND
  → (c) have not been advertised to the peer

Note: This applies whether or not P1 advertised the best route for the default RTC prefix.
No MVPN, MDT-SAFI, or L2-VPN routes are sent as a result of receiving the default RTC route.

In this context, a default RTC route is any of the following:

1. a route with NLRI length = zero
2. a route with NLRI value = origin AS and NLRI length = 32
3. a route with NLRI value = {origin AS+0x0002 | origin AS+0x0102 | origin AS+0x0202} and NLRI length = 48

- If an RTC route for prefix A (origin-AS = A1, RT = A2/n, n > 48) is received from an IBGP peer I1 in autonomous system A1, the VPN routes that are advertised to I1 is the set of VPN-IPv4 and VPN-IPv6 routes in the LOC_RIB that:
  a. are eligible for advertisement to I1 per BGP route advertisement rules AND
  b. have not been rejected by manually configured export policies AND
  c. carry at least one route target extended community with value A2 in the n most-significant bits AND
  d. have not been advertised to the peer

  Note: This applies whether or not I1 advertised the best route for A.

No MVPN, MDT-SAFI or L2-VPN routes are sent as a result of receiving the RTC route.

- If the best RTC route for a prefix A (origin-AS = A1, RT = A2/n, n > 48) is received from an IBGP peer I1 in autonomous system B, the VPN routes that are advertised to I1 is the set of VPN-IPv4 and VPN-IPv6 routes in the LOC_RIB that:
  a. are eligible for advertisement to I1 per BGP route advertisement rules AND
  b. have not been rejected by manually configured export policies AND
  c. carry at least one route target extended community with value A2 in the n most-significant bits AND
  d. have not been advertised to the peer

  Note: This applies only if I1 advertised the best route for A.

No MVPN, MDT-SAFI, or L2-VPN routes are sent as a result of receiving the RTC route.

- If the best RTC route for a prefix A (origin-AS = A1, RT = A2/n, n > 48) is received from an EBGP peer E1, the VPN routes that are advertised to E1 is the set of VPN-IPv4 and VPN-IPv6 routes in the LOC_RIB that:
  a. are eligible for advertisement to E1 per BGP route advertisement rules AND
  b. have not been rejected by manually configured export policies AND
  c. carry at least one route target extended community with value A2 in the n most-significant bits AND
  d. have not been advertised to the peer

  Note: This applies only if E1 advertised the best route for A.
No MVPN, MDT-SAFI or L2-VPN routes are sent as a result of receiving the RTC route.
BGP Fast Reroute in a VPRN

BGP fast reroute is a feature that brings together indirection techniques in the forwarding plane and pre-computation of BGP backup paths in the control plane to support fast reroute of BGP traffic around unreachable/failed next-hops. In a VPRN context BGP fast reroute is supported using unlabeled IPv4, unlabeled IPv6, VPN-IPv4, and VPN-IPv6 VPN routes. The supported VPRN scenarios are outlined in Table 23.

Note that BGP fast reroute information specific to the base router BGP context is described in the BGP Fast Reroute section of the 7x50 SR OS Routing Protocols Guide.

Table 23: BGP Fast Reroute Scenarios (VPRN Context)

<table>
<thead>
<tr>
<th>Ingress Packet</th>
<th>Primary Route</th>
<th>Backup Route</th>
<th>Prefix Independent Convergence</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4 (ingress PE)</td>
<td>IPv4 route with next-hop A resolved by an IPv4 route</td>
<td>IPv4 route with next-hop B resolved by an IPv4 route</td>
<td>Yes</td>
</tr>
<tr>
<td>IPv4 (ingress PE)</td>
<td>VPN-IPv4 route with next-hop A resolved by a GRE, LDP, RSVP or BGP tunnel</td>
<td>VPN-IPv4 route with next-hop A resolved by a GRE, LDP, RSVP or BGP tunnel</td>
<td>Yes, but if the VPN-IP routes are label-per-prefix the ingress card must be FP2 or better</td>
</tr>
<tr>
<td>MPLS (egress PE)</td>
<td>IPv4 route with next-hop A resolved by an IPv4 route</td>
<td>IPv4 route with next-hop B resolved by an IPv4 route</td>
<td>Yes</td>
</tr>
<tr>
<td>MPLS (egress PE)</td>
<td>IPv4 route with next-hop A resolved by an IPv4 route</td>
<td>VPN-IPv4 route* with next-hop B resolved by a GRE, LDP, RSVP or BGP tunnel</td>
<td>Yes, but if the VPN-IP routes are label-per-prefix the ingress card must be FP2 or better</td>
</tr>
<tr>
<td>IPv6 (ingress PE)</td>
<td>IPv6 route with next-hop A resolved by an IPv6 route</td>
<td>IPv6 route with next-hop B resolved by an IPv6 route</td>
<td>Yes</td>
</tr>
<tr>
<td>IPv6 (ingress PE)</td>
<td>VPN-IPv6 route with next-hop A resolved by a GRE, LDP, RSVP or BGP tunnel</td>
<td>VPN-IPv6 route with next-hop B resolved by a GRE, LDP, RSVP or BGP tunnel</td>
<td>Yes, but if the VPN-IP routes are label-per-prefix the ingress card must be FP2 or better</td>
</tr>
<tr>
<td>MPLS (egress)</td>
<td>IPv6 route with next-hop A resolved by an IPv6 route</td>
<td>IPv6 route with next-hop B resolved by an IPv6 route</td>
<td>Yes</td>
</tr>
</tbody>
</table>
BGP Fast Reroute in a VPRN Configuration

Configuring the `backup-path` command under `config>service>vprn>bgp` causes only routes learned from CE BGP peers to be considered when selecting the primary and backup paths.

Configuring the `enable-bgp-vpn-backup` command under `config>service>vprn` causes imported BGP-VPN routes to be compared to CE BGP routes when selecting the primary and backup paths. This command is required to support fast failover of ingress traffic from one remote PE to another remote PE and to support fast failover of egress traffic from a locally connected CE to a remote PE.

---

Table 23: BGP Fast Reroute Scenarios (VPRN Context)

<table>
<thead>
<tr>
<th>Ingress Packet</th>
<th>Primary Route</th>
<th>Backup Route</th>
<th>Prefix Independent Convergence</th>
</tr>
</thead>
<tbody>
<tr>
<td>MPLS (egress)</td>
<td>IPv6 route with next-hop A resolved by an IPv6 route</td>
<td>Yes, but if the VPN-IP routes are label-per-prefix the ingress card must be FP2 or better for PIC</td>
<td>VPRN label mode must be VRF. VPRN must export its VPN-IP routes with RD ≠ y. For the best performance the backup next-hop must advertise the same VPRN label value with all routes (e.g. per VRF label).</td>
</tr>
</tbody>
</table>
VPRN Features

This section describes various VPRN features and any special capabilities or considerations as they relate to VPRN services.

- IP Interfaces on page 1205
- SAPs on page 1209
  - Encapsulations on page 1209
  - QoS Policies on page 1210
  - Filter Policies on page 1210
- CE to PE Routing Protocols on page 1214
  - PE to PE Tunneling Mechanisms on page 1214
  - Per VRF Route Limiting on page 1214
  - Using OSPF in IP-VPNs on page 1217
- Spoke SDPs on page 1215
  - Carrier Supporting Carrier (CsC) on page 1220
- Multicast in IP-VPN Applications on page 1229

IP Interfaces

VPRN customer IP interfaces can be configured with most of the same options found on the core IP interfaces. The advanced configuration options supported are:

- VRRP
- Cflowd
- Secondary IP addresses
- ICMP Options

Configuration options found on core IP interfaces not supported on VPRN IP interfaces are:

- NTP broadcast receipt
QoS Policy Propagation Using BGP (QPPB)

This section discusses QPPB as it applies to VPRN, IES, and router interfaces. Refer to the QoS Policy Propagation Using BGP (QPPB) on page 1056 section on page 1053 and the IP Router Configuration section in the 7x50 OS Router Configuration Guide.
Object Grouping and State Monitoring

This feature introduces a generic operational group object which associates different service endpoints (pseudowires and SAPs) located in the same or in different service instances. The operational group status is derived from the status of the individual components using certain rules specific to the application using the concept. A number of other service entities, the monitoring objects, can be configured to monitor the operational group status and to perform certain actions as a result of status transitions. For example, if the operational group goes down, the monitoring objects will be brought down.

VPRN IP Interface Applicability

This concept is used by an IPv4 VPRN interface to affect the operational state of the IP interface monitoring the operational group. Individual SAP and spoke SDPs are supported as monitoring objects.

The following rules apply:

- An object can only belong to one group at a time.
- An object that is part of a group cannot monitor the status of a group.
- An object that monitors the status of a group cannot be part of a group.
- An operational group may contain any combination of member types: SAP or Spoke-SDPs.
- An operational group may contain members from different VPLS service instances.
- Objects from different services may monitor the oper-group.

There are two steps involved in enabling the functionality:

1. Identify a set of objects whose forwarding state should be considered as a whole group then group them under an operational group using the `oper-group` command.
2. Associate the IP interface to the oper-group using the `monitor-group` command

The status of the operational group (oper-group) is dictated by the status of one or more members according to the following rule:

- The oper-group goes down if all the objects in the oper-group go down. The oper-group comes up if at least one of the components is up.
- An object in the group is considered down if it is not forwarding traffic in at least one direction. That could be because the operational state is down or the direction is blocked through some validation mechanism.
- If a group is configured but no members are specified yet then its status is considered up.
• As soon as the first object is configured the status of the operational group is dictated by the status of the provisioned member(s).

The simple configuration below shows the oper-group g1, the VPLS SAP that is mapped to it and the IP interfaces in VPRN service 2001 monitoring the oper-group g1. This is example uses an R-VPLS context. The VPLS instance includes the allow-ip-int-binding and the service-name v1. The VPRN interface links to the VPLS using the vpls v1 option. All commands are under the configuration service hierarchy.

To further explain the configuration. Oper-group g1 has a single SAP (1/1/1:2001) mapped to it and the IP interfaces in the VPRN service 2001 will derive its state from the state of oper-group g1.

```plaintext
oper-group g1 create
vpls 1 customer 1 create
  allow-ip-int-binding
  stp
  shutdown
  exit
  service-name "v1"
sap 1/1/1:2001 create
  oper-group g1
  eth-cfm
    mep domain 1 association 1 direction down
    ccm-enable
    no shutdown
    exit
  exit
  sap 1/1/2:2001 create
  exit
  sap 1/1/3:2001 create
  exit
no shutdown

vprn 2001 customer 1 create
  interface "i2001" create
    address 21.1.1.1/24
    monitor-oper-group "g1"
    vpls "v1"
  exit
no shutdown
exit
```
SAPs

Encapsulations

The following SAP encapsulations are supported on the SR-OS VPRN service:

- Ethernet null
- Ethernet dot1q
**QoS Policies**

When applied to a VPRN SAP, service ingress QoS policies only create the unicast queues defined in the policy if PIM is not configured on the associated IP interface; if PIM is configured, the multipoint queues are applied as well.

With VPRN services, service egress QoS policies function as with other services where the class-based queues are created as defined in the policy.

Note that both Layer 2 or Layer 3 criteria can be used in the QoS policies for traffic classification in an VPRN.

**Filter Policies**

Ingress and egress IPv4 and IPv6 filter policies can be applied to VPRN SAPs.
DSCP Marking

Specific DSCP, forwarding class, and Dot1P parameters can be specified to be used by every protocol packet generated by the VPRN. This enables prioritization or de-prioritization of every protocol (as required). The markings effect a change in behavior on ingress when queuing. For example, if OSPF is not enabled, then traffic can be de-prioritized to best effort (be) DSCP. This change de-prioritizes OSPF traffic to the CPU complex.

DSCP marking for internally generated control and management traffic by marking the DSCP value should be used for the given application. This can be configured per routing instance. For example, OSPF packets can carry a different DSCP marking for the base instance and then for a VPRN service. ISIS and ARP traffic is not an IP-generated traffic type and is not configurable.

When an application is configured to use a specified DSCP value then the MPLS EXP, Dot1P bits will be marked in accordance with the network or access egress policy as it applies to the logical interface the packet will be egressing.

The DSCP value can be set per application. This setting will be forwarded to the egress linecard. The egress linecard does not alter the coded DSCP value and marks the LSP-EXP and IEEE 802.1p (Dot1P) bits according to the appropriate network or access QoS policy.

Table 24: DSCP/FC Marking

<table>
<thead>
<tr>
<th>Protocol</th>
<th>IPv4</th>
<th>IPv6</th>
<th>DSCP Marking</th>
<th>Dot1P Marking</th>
<th>Default FC</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARP</td>
<td></td>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>NC</td>
</tr>
<tr>
<td>BGP</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>NC</td>
</tr>
<tr>
<td>BFD</td>
<td>Yes</td>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>NC</td>
</tr>
<tr>
<td>RIP</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>NC</td>
</tr>
<tr>
<td>PIM (SSM)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>NC</td>
</tr>
<tr>
<td>OSPF</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>NC</td>
</tr>
<tr>
<td>SMTP</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td>AF</td>
</tr>
<tr>
<td>IGMP/MLD</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>AF</td>
</tr>
<tr>
<td>Telnet</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>AF</td>
</tr>
<tr>
<td>TFTP</td>
<td>Yes</td>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>AF</td>
</tr>
<tr>
<td>FTP</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td>AF</td>
</tr>
</tbody>
</table>
### Table 24: DSCP/FC Marking (Continued)

<table>
<thead>
<tr>
<th>Protocol</th>
<th>IPv4</th>
<th>IPv6</th>
<th>DSCP Marking</th>
<th>Dot1P Marking</th>
<th>Default FC</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSH (SCP)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>AF</td>
</tr>
<tr>
<td>SNMP (get, set, etc.)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>AF</td>
</tr>
<tr>
<td>SNMP trap/log</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>AF</td>
</tr>
<tr>
<td>syslog</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>AF</td>
</tr>
<tr>
<td>OAM ping</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>AF</td>
</tr>
<tr>
<td>ICMP ping</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>AF</td>
</tr>
<tr>
<td>Traceroute</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>AF</td>
</tr>
<tr>
<td>TACPLUS</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>AF</td>
</tr>
<tr>
<td>DNS</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>AF</td>
</tr>
<tr>
<td>SNTP/NTP</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td>AF</td>
</tr>
<tr>
<td>RADIUS</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td>AF</td>
</tr>
<tr>
<td>Cflowd</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td>AF</td>
</tr>
<tr>
<td>Bootp</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td>AF</td>
</tr>
<tr>
<td>IPv6 Neighbor Discovery</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td>NC</td>
</tr>
</tbody>
</table>
## Default DSCP Mapping Table

<table>
<thead>
<tr>
<th>DSCP Name</th>
<th>DSCP Value</th>
<th>DSCP Value</th>
<th>DSCP Value</th>
<th>Label</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Decimal</td>
<td>Hexadecimal</td>
<td>Binary</td>
<td></td>
</tr>
<tr>
<td>Default</td>
<td>0</td>
<td>0x00</td>
<td>0b000000</td>
<td>be</td>
</tr>
<tr>
<td>ncl</td>
<td>48</td>
<td>0x30</td>
<td>0b110000</td>
<td>h1</td>
</tr>
<tr>
<td>nc2</td>
<td>56</td>
<td>0x38</td>
<td>0b111000</td>
<td>nc</td>
</tr>
<tr>
<td>ef</td>
<td>46</td>
<td>0x2e</td>
<td>0b101110</td>
<td>ef</td>
</tr>
<tr>
<td>af11</td>
<td>10</td>
<td>0x0a</td>
<td>0b001010</td>
<td>assured</td>
</tr>
<tr>
<td>af12</td>
<td>12</td>
<td>0x0c</td>
<td>0b001100</td>
<td>assured</td>
</tr>
<tr>
<td>af13</td>
<td>14</td>
<td>0x0e</td>
<td>0b001110</td>
<td>assured</td>
</tr>
<tr>
<td>af21</td>
<td>18</td>
<td>0x12</td>
<td>0b010010</td>
<td>l1</td>
</tr>
<tr>
<td>af22</td>
<td>20</td>
<td>0x14</td>
<td>0b010100</td>
<td>l1</td>
</tr>
<tr>
<td>af23</td>
<td>22</td>
<td>0x16</td>
<td>0b010110</td>
<td>l1</td>
</tr>
<tr>
<td>af31</td>
<td>26</td>
<td>0x1a</td>
<td>0b011010</td>
<td>l1</td>
</tr>
<tr>
<td>af32</td>
<td>28</td>
<td>0x1c</td>
<td>0b011100</td>
<td>l1</td>
</tr>
<tr>
<td>af33</td>
<td>30</td>
<td>0x1d</td>
<td>0b011110</td>
<td>l1</td>
</tr>
<tr>
<td>af41</td>
<td>34</td>
<td>0x22</td>
<td>0b100010</td>
<td>h2</td>
</tr>
<tr>
<td>af42</td>
<td>36</td>
<td>0x24</td>
<td>0b100100</td>
<td>h2</td>
</tr>
<tr>
<td>af43</td>
<td>38</td>
<td>0x26</td>
<td>0b100110</td>
<td>h2</td>
</tr>
</tbody>
</table>

*The default forwarding class mapping is used for all DSCP names/values for which there is no explicit forwarding class mapping.*
CE to PE Routing Protocols

The SR-OS VPRN supports the following PE to CE routing protocols:

- BGP
- Static
- RIP
- OSPF

PE to PE Tunneling Mechanisms

The SR-OS supports multiple mechanisms to provide transport tunnels for the forwarding of traffic between PE routers within the 2547bis network.

The SR-OS VPRN implementation supports the use of:

- RSVP-TE protocol to create tunnel LSP's between PE routers
- LDP protocol to create tunnel LSP's between PE routers
- GRE tunnels between PE routers.

These transport tunnel mechanisms provide the flexibility of using dynamically created LSPs where the service tunnels are automatically bound (the “autobind” feature) and the ability to provide certain VPN services with their own transport tunnels by explicitly binding SDPs if desired. When the autobind is used, all services traverse the same LSPs and do not allow alternate tunneling mechanisms (like GRE) or the ability to craft sets of LSP's with bandwidth reservations for specific customers as is available with explicit SDPs for the service.

Per VRF Route Limiting

The SR-OS allows setting the maximum number of routes that can be accepted in the VRF for a VPRN service. There are options to specify a percentage threshold at which to generate an event that the VRF table is near full and an option to disable additional route learning when full or only generate an event.
Spoke SDPs

Distributed services use service distribution points (SDPs) to direct traffic to another SR-Series router via service tunnels. SDPs are created on each participating SR-Series and then bound to a specific service. SDP can be created as either GRE or MPLS. Refer to Service Distribution Points (SDPs) on page 48 for information about configuring SDPs.

This feature provides the ability to cross-connect traffic entering on a spoke SDP, used for Layer 2 services (VLLs or VPLS), on to an IES or VPRN service. From a logical point of view, the spoke SDP entering on a network port is cross-connected to the Layer 3 service as if it entered by a service SAP. The main exception to this is traffic entering the Layer 3 service by a spoke SDP is handled with network QoS policies not access QoS policies.

Figure 151 depicts traffic terminating on a specific IES or VPRN service that is identified by the sdp-id and VC label present in the service packet.

Figure 151: SDP-ID and VC Label Service Identifiers
**T-LDP Status Signaling for Spoke-SDPs Terminating on IES/VPRN**

T-LDP status signaling and PW active/standby signaling capabilities are supported on ipipe and epipe spoke SDPs.

Spoke SDP termination on an IES or VPRN provides the ability to cross-connect traffic entering on a spoke SDP, used for Layer 2 services (VLLs or VPLS), on to an IES or VPRN service. From a logical point of view the spoke SDP entering on a network port is cross-connected to the Layer 3 service as if it had entered using a service SAP. The main exception to this is traffic entering the Layer 3 service using a spoke SDP is handled with network QoS policies instead of access QoS policies.

When a SAP down or SDP binding down status message is received by the PE in which the Ipipe or Ethernet spoke-sdp is terminated on an IES or VPRN interface, the interface is brought down and all associated routes are withdrawn in a similar way when the spoke-sdp goes down locally. The same actions are taken when the standby T-LDP status message is received by the IES/VPRN PE.

This feature can be used to provide redundant connectivity to a VPRN or IES from a PE providing a VLL service, as shown in Figure 152.

![Figure 152: Active/Standby VRF Using Resilient Layer 2 Circuits](image-url)
IP-VPNs

Using OSPF in IP-VPNs

Using OSPF as a CE to PE routing protocol allows OSPF that is currently running as the IGP routing protocol to migrate to an IP-VPN backbone without changing the IGP routing protocol, introducing BGP as the CE-PE or relying on static routes for the distribution of routes into the service providers IP-VPN. The following features are supported:

- Advertisement/redistribution of BGP-VPN routes as summary (type 3) LSAs flooded to CE neighbors of the VPRN OSPF instance. This occurs if the OSPF route type (in the OSPF route type BGP extended community attribute carried with the VPN route) is not external (or NSSA) and the locally configured domain-id matches the domain-id carried in the OSPF domain ID BGP extended community attribute carried with the VPN route.
- OSPF sham links. A sham link is a logical PE-to-PE unnumbered point-to-point interface that essentially rides over the PE-to-PE transport tunnel. A sham link can be associated with any area and can therefore appear as an intra-area link to CE routers attached to different PEs in the VPN.
IPCP Subnet Negotiation

This feature enables negotiation between Broadband Network Gateway (BNG) and customer premises equipment (CPE) so that CPE is allocated both ip-address and associated subnet.

Some CPEs use the network up-link in PPPoE mode and perform dhcp-server function for all ports on the LAN side. Instead of wasting 1 subnet for p2p uplink, CPEs use allocated subnet for LAN portion as shown in Figure 153.

![Diagram showing PPPoE Tunnel](image)

**Figure 153: CPEs Network Up-link Mode**

From a BNG perspective, the given PPPoE host is allocated a subnet (instead of /32) by RADIUS, external dhcp-server, or local-user-db. And locally, the host is associated with managed-route.
Cflowd for IP-VPNs

The cflowd feature allows service providers to collect IP flow data within the context of a VPRN. This data can be used to monitor types and general proportion of traffic traversing an VPRN context. This data can also be shared with the VPN customer to see the types of traffic traversing the VPN and use it for traffic engineering.

This feature should not be used for billing purposes. Existing queue counters are designed for this purpose and provide very accurate per bit accounting records.
Carrier Supporting Carrier (CsC)

Carrier Supporting Carrier (CSC) is a solution that allows one service provider (the “Customer Carrier”) to use the IP VPN service of another service provider (the “Super Carrier”) for some or all of its backbone transport. RFC 4364 defines a Carrier Supporting Carrier solution for BGP/MPLS IP VPNs that uses MPLS on the interconnections between the two service providers in order to provide a scalable and secure solution.

CsC support in SROS allows a 7x50 to be deployed as any of the following devices shown in Figure 154:

- PE1 (service provider PE)
- CSC-CE1, CSC-CE2 and CSC-CE3 (CE device from the point of view of the backbone service provider)
- CSC-PE1, CSC-PE2 and CSC-PE3 (PE device of the backbone service provider)
- ASBR1 and ASBR2 (ASBR of the backbone service provider)

![Carrier Supporting Carrier Reference Diagram](image)

**Figure 154: Carrier Supporting Carrier Reference Diagram**

Terminology

CE — Customer premises equipment dedicated to one particular business/enterprise.

PE — Service provider router that connects to a CE to provide a business VPN service to the associated business/enterprise.
CSC-CE — An ASBR/peering router that is connected to the CSC-PE of another service provider for purposes of using the associated CsC IP VPN service for backbone transport.

CSC-PE — A PE router belonging to the backbone service provider that supports one or more CSC IP VPN services.
CSC Connectivity Models

A PE router deployed by a customer service provider to provide Internet access, IP VPNs, and/or L2 VPNs may connect directly to a CSC-PE device, or it may back haul traffic within its local “site” to the CSC-CE that provides this direct connection. Here, “site” means a set of routers owned and managed by the customer service provider that can exchange traffic through means other than the CSC service. The function of the CSC service is to provide IP/MPLS reachability between isolated sites.

The CSC-CE is a “CE” from the perspective of the backbone service provider. There may be multiple CSC-CEs at a given customer service provider site and each one may connect to multiple CSC-PE devices for resiliency/multi-homing purposes.

The CSC-PE is owned and managed by the backbone service provider and provides CSC IP VPN service to connected CSC-CE devices. In many cases, the CSC-PE also supports other services, including regular business IP VPN services. A single CSC-PE may support multiple CSC IP VPN services. Each customer service provider is allocated its own VRF within the CSC-PE; VRFs maintain routing and forwarding separation and permit the use of overlapping IP addresses by different customer service providers.

A backbone service provider may not have the geographic span to connect, with reasonable cost, to every site of a customer service provider. In this case, multiple backbone service providers may coordinate to provide an inter-AS CSC service. Different inter-AS connectivity options are possible, depending on the trust relationships between the different backbone service providers.
Traffic Leaking to GRT

Traffic leaking to Global Route Table (GRT) allows service providers to offer VPRN and Internet services to their customers over a single VRF interface. This currently supports IPv4.

Packets entering a local VRF interface can have route processing results derived from the VPRN forwarding table or the GRT. The leaking and preferred lookup results are configured on a per VPRN basis. Configuration options can be general (for example, any lookup miss in the VPRN forwarding table can be resolved in the GRT), or specific (for example, specific route(s) should only be looked up in the GRT and ignored in the VPRN). In order to provide operational simplicity and improve streamlining, the CLI configuration is all contained within the context of the VPRN service.

This feature is enabled within the VPRN service context under `config>service>vprn>grt-lookup`. This is an administrative context and provides the container under which all specific commands can be entered, except for policy definition. Policy definitions remain unchanged but are referenced from this context.

The `enable-grt` command establishes the basic functionality. When it is configured, any lookup miss in the VRF table will be resolved in the GRT, if available. By itself, this only provides part of the solution. Packet forwarding within GRT must understand how to route packets back to the proper node and to the specific VPRN from which the destination exists. Destination prefixes must be leaked from the VPRN to the GRT through the use of policy. Policies are created under the `config>router>policy-options` hierarchy. By default, the number of prefixes leaked from the VPRN to the GRT is limited to five. The `export-limit` command under the `grt-lookup` hierarchy allows the service provider to override the default, or remove the limit.

When a VPRN forwarding table consists of a default route or an aggregate route, the customer may require the service provider to poke holes in those, or provide more specific route resolution in the GRT. In this case, the service provider may configure a “static-route”, under the “enable-grt” context. The lookup result will prefer any successful lookup in the GRT that is equal to or more specific than the static route, bypassing any successful lookup in the local VPRN.

This feature and Unicast Reverse Path Forwarding (uRPF) are mutually exclusive. When a VPRN service is configured with either of these functions, the other cannot be enabled. Also, prefixes leaked from any VPRN should never conflict with prefixes leaked from any other VPRN or existing prefixes in the GRT. Prefixes should be globally unique with the service provider network and if these are propagated outside of a single providers network, they must be from the public IP space and globally unique. Network Address Translation (NAT) is not supported as part of this feature. It is also important to note that aggregate routes, blackhole routes and BGP VPN extranet routes will not be leaked from the VPRN into the base routing table.
Traffic Leaking from VPRN to GRT for IPv6

This feature allows IPv6 destination lookups in two distinct routing tables. IPv6 packets within a Virtual Private Routed Network (VPRN) service is able to perform a lookup for IPv6 destination against the Global Route Table (GRT) as well as within the local VPRN.

Currently, VPRN to VPRN routing exchange is accomplished through the use of import and export policies based on Route Targets (RTs), the creation of extranets. This new feature allows the use of a single VPRN interface for both corporate VPRN routing and other services (for example, Internet) that are reachable outside the local routing context. This feature takes advantage of the dual lookup capabilities in two separate routing tables in parallel.

This feature enables IPv6 capability in addition to the existing IPv4 VPRN-to-GRT Route Leaking feature.
RIP Metric Propagation in VPRNs

When RIP is used as the PE-CE protocol for VPRNs (IP-VPNs), the RIP metric is only used by the local node running RIP with the Customer Equipment (CE). The metric is not used to or encoded into and MP-BGP path attributes exchanged between PE routers.

The RIP metric can also be used to exchanged between PE routers so if a customer network is dual homed to separate PEs the RIP metric learned from the CE router can be used to choose the best route to the destination subnet. By using the learned RIP metric to set the BGP MED attribute, remote PEs can choose the lowest MED and in turn the PE with the lowest advertised RIP metric as the preferred egress point for the VPRN.

![Figure 155: RIP Metric Propagation in VPRNs](image)
NTP Within a VPRN Service

The NTP within a VPRN service enables the service router to act as the NTP server to CPE devices on a VPRN interface. Individual VPRN interfaces may be configured to listen to and respond to client requests, or additionally may be configured to send NTP broadcast messages. Authentication keys are configurable on a per-VPRN basis.

Only a single instance of NTP remains in the node that is time sourced to as many as five NTP servers attached to the “base” or “management” network.

The NTP show command displays NTP servers and all known clients. Because NTP is UDP based only, no state is maintained. As a result, the show command output only displays when the last message from the client was received.

PTP Within a VPRN Service

The PTP within a VPRN service provides access to the PTP clock within the 7750 SR through one or more VPRN services. Only one VPRN or the base routing instance may have configured peers, but all may have discovered peers. If desired, a limit on the maximum number of dynamic peers allowed may be configured on a per routing instance basis.

For more detail on PTP see the SR OS Basic System Configuration Guide.
Service Label Mode of a VPRN

The mode used for allocating service labels to VPN routes is now configurable per VPRN service. When the label mode is configured in the default per-VRF mode, the SR-OS allocates one unique (platform-wide) service label per VRF. All VPN-IP routes exported by the PE from a particular VPRN service with that configuration have the same service label. When the PE receives a terminating MPLS packet, the service label value determines the VRF to which the packet belongs. A lookup of the IP packet DA in the forwarding table of the selected VRF determines the next-hop interface.

When, alternatively, a VPRN is configured in the new service label per next-hop mode, MPLS allocates one unique (platform-wide) service label per next-hop IP mode of the VPRN. All IP routes of the VPRN with a specific next-hop are advertised with the same service label value when exported as VPN-IP routes. When the PE receives a terminating MPLS packet and the service label value is associated with a VPRN next-hop address the IP packet is forwarded to that next-hop without any lookup of the IP packet DA in the VRF forwarding table.
Multicast in IP-VPN Applications

This section and its subsections focuses on Multicast in IP VPN functionality. A reader should familiarize itself first with Multicast section in SROS Routing Protocols Guide where multicast protocols (PIM, IGMP, MLD, MSDP) are described.

Applications for this feature include enterprise customer implementing a VPRN solution for their WAN networking needs, customer applications including stock-ticker information, financial institutions for stock and other types of trading data and video delivery systems.

Implementation of the draft-rosen-vpn-mcast, Multicast in MPLS/BGP IP VPNs, entails the support and separation of the providers core multicast domain from the various customer multicast domains and the various customer multicast domains from each other.

Figure 156: Multicast in IP-VPN Applications

Figure 156 depicts an example of multicast in an IP-VPN application. The provider’s domain encompasses the core routers (1 through 4) and the edge routers (5 through 10). The various IP-VPN customers each have their own multicast domain, VPN-1 (CE routers 12, 13 and 16) and VPN-2 (CE Routers 11, 14, 15, 17 and 18). Multicast in this VPRN example, the VPN-1 data generated by the customer behind router 16 will be multicast only by PE 9 to PE routers 6 and 7.
for delivery to CE routers 12 and 13 respectively. Data generated for VPN-2 generated by the
customer behind router 15 will be forwarded by PE 8 to PE routers 5, 7 and 10 for delivery to CE
routers 18, 11, 14 and 17 respectively.

The demarcation of these domains is in the PE’s (routers 5 through 10). The PE router participates
in both the customer multicast domain and the provider’s multicast domain. The customer’s CEs
are limited to a multicast adjacency with the multicast instance on the PE specifically created to
support that specific customer’s IP-VPN. This way, customers are isolated from the provider’s
core multicast domain and other customer multicast domains while the provider’s core routers
only participate in the provider’s multicast domain and are isolated from all customers’ multicast
domains.

The PE for a given customer’s multicast domain becomes adjacent to the CE routers attached to
that PE and to all other PE’s that participate in the IP-VPN (or customer) multicast domain. This is
achieved by the PE who encapsulates the customer multicast control data and multicast streams
inside the provider’s multicast packets. These encapsulated packets are forwarded only to the PE
nodes that are attached to the same customer’s edge routers as the originating stream and are part
of the same customer VPRN. This prunes the distribution of the multicast control and data traffic
to the PEs that participate in the customer’s multicast domain. The Rosen draft refers to this as the
default multicast domain for this multicast domain; the multicast domain is associated with a
unique multicast group address within the provider’s network.
Use of Data MDTs

Using the above method, all multicast data offered by a given CE is always delivered to all other CEs that are part of the same multicast. It is possible that a number of CEs do not require the delivery of a particular multicast stream because they have no downstream receivers for a specific multicast group. At low traffic volumes, the impact of this is limited. However, at high data rates this could be optimized by devising a mechanism to prune PEs from the distribution tree that although forming part of the customer multicast have no need to deliver a given multicast stream to the CE attached to them. To facilitate this optimization, the Rosen draft specifies the use of data MDTs. These data MDTs are signaled once the bandwidth for a given SG exceeds the configurable threshold.

Once a PE detects it is transmitting data for the SG in excess of this threshold, it sends an MDT join TLV (at 60 second intervals) over the default MDT to all PEs. All PEs that require the SG specified in the MDT join TLV will join the data MDT that will be used by the transmitting PE to send the given SG. PEs that do not require the SG will not join the data MDT, thus pruning the multicast distribution tree to just the PEs requiring the SG. After providing sufficient time for all PEs to join the data MDT, the transmitting PE switches the given multicast stream to the data MDT.

PEs that do not require the SG to be delivered, keep state to allow them to join the data MDT as required.

When the bandwidth requirement no longer exceeds the threshold, the PE stops announcing the MDT join TLV. At this point the PEs using the data MDT will leave this group and transmission resumes over the default MDT.

Sampling to check if an s,g has exceeded the threshold occurs every ten seconds. If the rate has exceeded the configured rate in that sample period then the data MDT is created. If during that period the transmission rate has not exceeded the configured threshold then the data MDT is not created. If the data MDT is active and the transmission rate in the last sample period has not exceeded the configured rate then the data MDT is torn down and the multicast stream resumes transmission over the default MDT.
**Multicast Protocols Supported in the Provider Network**

When MVPN auto-discovery is disabled, PIM-SM can be used for I-PMSI, and PIM-SSM or PIM-SM (Draft-Rosen Data MDT) can be used for S-PMSI; When MVPN S-PMSI auto-discovery is enabled, both PIM-SM and PIM SSM can be used for I-PMSI, and PIM-SSM can be used for S-PMSI. In the customer network, both PIM-SM and PIM-SSM are supported.

An MVPN is defined by two sets of sites: sender sites set and receiver sites set, with the following properties:

- Hosts within the sender sites set could originate multicast traffic for receivers in the receiver sites set.
- Receivers not in the receiver sites set should not be able to receive this traffic.
- Hosts within the receiver sites set could receive multicast traffic originated by any host in the sender sites set.
- Hosts within the receiver sites set should not be able to receive multicast traffic originated by any host that is not in the sender sites set.

A site could be both in the sender sites set and receiver sites set, which implies that hosts within such a site could both originate and receive multicast traffic. An extreme case is when the sender sites set is the same as the receiver sites set, in which case all sites could originate and receive multicast traffic from each other.

Sites within a given MVPN may be either within the same, or in different organizations, which implies that an MVPN can be either an intranet or an extranet. A given site may be in more than one MVPN, which implies that MVPNs may overlap. Not all sites of a given MVPN have to be connected to the same service provider, which implies that an MVPN can span multiple service providers.

Another way to look at MVPN is to say that an MVPN is defined by a set of administrative policies. Such policies determine both sender sites set and receiver site set. Such policies are established by MVPN customers, but implemented by MVPN service providers using the existing BGP/MPLS VPN mechanisms, such as route targets, with extensions, as necessary.
**MVPN Using BGP Control Plane**

Note that the next generation MVPN solution replaces the Rosen MVPN draft and is currently being defined at the IETF. Its IETF status is still a working group draft but it has strong support. It is quite stable for implementation from a technical point of view.

The Alcatel-Lucent implementation supports the following features:

- MVPN membership auto-discovery using BGP
- PE-PE Transmission of C-Multicast Routing using BGP
- IPv4 support
- Use of PIM default and data MDTs as PMSIs
- Inter-AS support with direct VRF connect (option A)
- Backward compatibility with existing Rosen implementation to provide an easy migration path

---

**MVPN Membership Auto-discovery using BGP**

BGP-based auto-discovery is performed by an multicast VPN address family. Any PE that attaches to an MVPN must issue a BGP update message containing an NLRI in this address family, along with a specific set of attributes.

The PE router uses route targets to specify MVPN route import and export. The route target may be the same as the one used for the corresponding unicast VPN, or it may be different. The PE router can specify separate import route targets for sender sites and receiver sites for a given MVPN.

The route distinguisher (RD) that is used for the corresponding unicast VPN can also be used for the MVPN.

When BGP auto-discovery is enabled, PIM peering on the I-PMSI is disabled, so no PIM hellos are sent on the I-PMSI. C-trees to P-tunnels bindings are also discovered using BGP S-PMSI AD routes, instead of PIM join TLVs. Configure PIM join TLVs when `c-mcast-signaling` is set to `pim` in the `config>service>vprn>mvpn>provider-tunnel>selective>auto-discovery-disable` context.

Table 25 and Table 26 describe the supported configuration combinations. If the CLI combination is not allowed, the system returns an error message. If the CLI command is marked as “ignored” in the table, the configuration is not blocked, but its value is ignored by the software.
For example, if auto-discovery is disabled, the `c-mcast-signaling bgp` command will fail with an error message stating:

**C-multicast signaling in BGP requires auto-discovery to be enabled**

If `c-mcast-signaling` is set to `bgp` then *no auto-discovery* will fail with an error message stating

**C-multicast signaling in BGP requires auto-discovery to be enabled**

When `c-mcast-signaling` is set to `bgp`, S-PMSI A-D is always enabled (its configuration is ignored);

When *auto-discovery* is disabled, S-PMSI A-D is always disabled (its configuration is ignored).

When auto-discovery is enabled and `c-multicast-signaling` is set to `pim`, S-PMSI A-D configuration value is used.

<table>
<thead>
<tr>
<th>Auto-Discovery</th>
<th>Inclusive PIM SSM</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Allowed</td>
</tr>
<tr>
<td>No</td>
<td>Yes</td>
<td>Not Allowed</td>
</tr>
<tr>
<td>Yes or No</td>
<td>No</td>
<td>Allowed</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Auto-Discovery</th>
<th>C-Mcast-Signaling</th>
<th>s-PMSI A-D</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>BGP</td>
<td>Ignored</td>
<td>Allowed</td>
</tr>
<tr>
<td>Yes</td>
<td>PIM</td>
<td>Yes</td>
<td>Allowed</td>
</tr>
<tr>
<td>Yes</td>
<td>PIM</td>
<td>No</td>
<td>Allowed</td>
</tr>
<tr>
<td>No</td>
<td>BGP</td>
<td>Ignored</td>
<td>Not Allowed</td>
</tr>
<tr>
<td>No</td>
<td>PIM</td>
<td>Ignored</td>
<td>Allowed</td>
</tr>
</tbody>
</table>
**MVPN (Rosen) Membership Auto-Discovery using BGP MDT-SAFI**

MVPN implementation based on the draft -Rosen can support membership auto discovery using BGP MDT-SAFI. A CLI option is provided per MVPN instance to enable auto discovery either using BGP MDT-SAFI or NG-MVPN. Only PIM-MDT is supported with BGP MDT-SAFI method.

---

**PE-PE Transmission of C-Multicast Routing using BGP**

MVPN c-multicast routing information is exchanged between PEs by using c-multicast routes that are carried using MCAST-VPN NLRI.

---

**MVPN (NG-MVPN) Upstream Multicast Hop Fast Failover**

MVPN upstream PE or P node fast failover detection method is supported with RSVP P2MP I-PMSI only. A receiver PE achieves fast upstream failover based on the capability to subscribe multicast flow from multiple UMH nodes and the capability to monitor the health of the upstream PE and intermediate P nodes using an unidirectional multi-point BFD session running over the provider tunnel.

A receiver PE subscribes multicast flow from multiple upstream PE nodes to have active redundant multicast flow available during failure of primary flow. Active redundant multicast flow from standby upstream PE allows instant switchover of multicast flow during failure of primary multicast flow.

Faster detection of multicast flow failure is achieved by keeping track of unidirectional multi-point BFD sessions enabled on the provider tunnel. Multi-point BFD sessions must be configured with 10 ms transmit interval on sender (root) PE to achieve sub-50ms fast failover on receiver (leaf) PE.

UMH **tunnel-status** selection option must be enabled on the receiver PE for upstream fast failover. Primary and standby upstream PE pairs must be configured on the receiver PE to allow receiving active redundant multicast flow from the standby upstream PE.
Provider Tunnel Support

The following provider tunnels features are supported:

- PIM ASM inclusive provider tunnel
- PIM SSM inclusive provider tunnel (only supported when auto-discovery is enabled)
- PIM SSM selective provider tunnel

Migration from Existing Rosen Implementation

The existing Rosen implementation is compatible to provide an easy migration path.

The following migration procedure are supported:

- Upgrade all the PE nodes that need to support MVPN to the newer release.
- The old configuration will be converted automatically to the new style.
- Node by node, MCAST-VPN address-family for BGP is enabled. Enable auto-discovery using BGP.
- Change PE-to-PE signaling to BGP.

VRF Route Import Extended Community

VRF route import is an IP address-specific extended community, of an extended type, and is transitive across AS boundaries (RFC 4360, BGP Extended Communities Attribute).

To support MVPN, in addition to the import/export route target extended communities used by the unicast routing, each VRF on a PE must have an import route target extended community that controls imports of C-multicast routes into a particular VRF.

The c-multicast import RT uniquely identifies a VRF, and is constructed as follows:

- The Global Administrator field of the c-multicast import RT must be set to an IP address of the PE. This address should be common for all the VRFs on the PE (this address may be the PE’s loopback address).
- The Local Administrator field of the c-multicast import RT associated with a given VRF contains a 2 octets long number that uniquely identifies that VRF within the PE that contains the VRF.

A PE that has sites of a given MVPN connected to it communicates the value of the c-multicast import RT associated with the VRF of that MVPN on the PE to all other PEs that have sites of that MVPN. To accomplish this, a PE that originates a (unicast) route to VPN-IP addresses includes in the BGP updates message that carries this route the VRF route import extended community that
has the value of the c-multicast import RT of the VRF associated with the route, except if it is known a priori that none of these addresses will act as multicast sources and/or RP, in which case the (unicast) route need not carry the VRF Route Import extended community.

All c-multicast routes with the c-multicast import RT specific to the VRF must be accepted. In this release, vrf-import and vrftraget policies don’t apply to C-multicast routes.

The decision flow path is shown below.

```python
if (route-type == c-mcast-route)
    if (route_target_list includes C-multicast_Import_RT)
        else
            drop;
    else
        Run vrf_import and/or vrf-target;
```
**MVPN Sender-only/Receiver-only**

In multicast MVPN, by default, if multiple PE nodes form a peering with a common MVPN instance then each PE node originates a multicast tree locally towards the remaining PE nodes that are member of this MVPN instance. This behavior creates a mesh of I-PMSI across all PE nodes in the MVPN. It is often a case, that a given VPN has many sites that will host multicast receivers, but only few sites that either host both receivers and sources or sources only.

MVPN Sender-only/Receiver-only allows to optimize control and data plane resources by preventing unnecessary I-PMSI mesh when a given PE hosts multicast sources only or multicast receivers only for a given MVPN.

For PE nodes that host only multicast sources for a given VPN, operators can now block those PEs, through configuration, from joining I-PMSIs from other PEs in this MVPN. For PE nodes that host only multicast receivers for a given VPN, operators can now block those PEs, through configuration, to set-up a local I-PMSI to other PEs in this MVPN.

MVPN Sender-only/Receiver-only is supported with ng-mVPN using IPv4 RSVP-TE or IPv4 LDP provider tunnels for both IPv4 and IPv6 customer multicast. Figure 157 depicts 4-site MVPN with sender-only, receiver-only and sender-receiver (default) sites:
A extra attention needs to be placed to BSR/RP placement when Sender-only/Receiver-only is enabled. Source DR sends unicast encapsulated traffic towards RP, therefore, RP shall be at sender-receiver or sender-only site, so that *G traffic can be sent over the tunnel. BSR shall be deployed at the sender-receiver site. BSR can be at sender-only site if the RPs are at the same site. BSR needs to receive packets from other candidate-BSR and candidate-RPs and also needs to send BSM packets to everyone.
Multicast VPN Extranet

Multicast VPN extranet distribution allows multicast traffic to flow across VPRN instances. VPRN instance that received a PIM/IGMP JOIN but cannot reach source of multicast source directly within its VPRN is selected as receiver VPRN instance. VPRN instance that has source of multicast stream and accepts PIM/IGMP JOIN from other VPRN instances is selected as source VPRN instance.

Routing information is exchanged between source and receiver VPRN instances of extranet based on route import/export policies. Routing information for multicast source in source VPRN instance is exported using RT export policy. Routing information for multicast source is imported in receiver VPRN instance using RT import policy.

Multicast receiver host in a receiver VPRN instance of extranet can subscribe to stream from a multicast source node reachable via source VPRN instance of extranet. Source VPRN instance and receiver VPRN instance of extranet must exist on a common PE node. PIM/IGMP JOIN received in a VPRN instance is propagated to source VPRN instance based on routing information.

Figure 158: Multicast VPN Traffic Flow

In Figure 158, VPRN-1 is source VPRN instance. VPRN-2 and VPRN-3 are receiver VPRN instances. PIM/IGMP JOIN received on VPRN-2 or VPRN-3 is for (S1,G1) multicast flow. Source
S1 belongs to VPRN-1. Due to route export policy in VPRN-1 and import policy in VPRN-2 and VPRN-3, receiver host in VPRN-2 or VPRN-3 can subscribe to stream (S1,G1).

Multicast VPN extranet based on draft Rosen (MDT-SAFI) is supported. Only PIM-SSM is supported for extranet multicast distribution.
IPv6 MVPN Support

IPv6 multicast support in SROS allows operators to offer customers IPv6 multicast MVPN service. An operator utilizes IPv4 mLDP or RSVP-TE core to carry IPv6 c-multicast traffic inside IPv4 mLDP or RSVP-TE provider tunnels (p-tunnels). The IPv6 customer multicast on a given MVPN can be blocked, enabled on its own or in addition to IPv4 multicast per PE or per interface. When both IPv4 and IPv6 multicast is enabled for a given MVPN, a single tree is used to carry both IPv6 and IPv4 traffic. Figure 159 shows an example of an operator with IPv4 MPLS backbone providing IPv6 MVPN service to Customer 1 and Customer 2.

Figure 159: IPv6 MVPN Example

SROS IPv6 MVPN multicast implementation provides the following functionality:

- IPv6 C-PIM-SM (ASM and SSM)
- MLDv1 and MLDv2
- SSM mapping for MLDv1
- I-PMSI and S-PMSI using IPv4 P2MP mLDP p-tunnels
- I-PMSI and S-PMSI using IPv4 P2MP RSVP p-tunnels
- BGP auto-discovery
- PE-PE transmission of C-multicast routing using BGP mvpn-ipv6 address family
- IPv6 BSR/RP functions on functional par with IPv4 (auto-RP using IPv4 only)
- Embedded RP
- Inter-AS Option A

The following known caveats exist for IPv6 MVPN support:

1. IPv6 MVPN requires chassis mode D
2. Non-congruent topologies are not supported
3. IPv6 is not supported in MCAC
4. If IPv4 and IPv6 multicast is enabled, per-MVPN multicast limits apply to entire IPv4 and IPv6 multicast traffic as it is carried in a single PMSI. For example IPv4 AND IPv6 S-PMSIs are counted against a single S-PMSI maximum per MVPN.
5. IPv6 Auto-RP is not supported
NG-MVPN Multicast Source Geo-Redundancy

Multicast source geo-redundancy is targeted primarily for MVPN deployments for multicast delivery services like IPTV. The solutions allow operators to configure a list of geographically dispersed redundant multicast sources (with different source IPs) and then, using configured BGP policies, ensure that each Receiver PE (a PE with receivers in its C-instance) selects only a single, most-preferred multicast source for a given group from the list. Although the data may still be replicated in P-instance (each multicast source sends (C-S, C-G) traffic onto its I-IPMSI tree or S-PMSI tree), each Receiver PE only forwards data to its receivers from the preferred multicast source. This allows operators to support multicast source geo-redundancy without the replication of traffic for each (C-S, C-G) in the C-instance while allowing fast recovery of service when an active multicast source fails.

Figure 160 shows an operational example of multicast source geo-redundancy:

Operators can configure a list of prefixes for multicast source redundancy per MVPN on Receiver PEs:

- Up to 8 multicast source prefixes per VPRN are supported.
- Any multicast source that is not part of the source prefix list is treated as a unique source and automatically joined in addition to joining the most preferred source from the redundant multicast source list.
A Receiver PE selects a single, most-preferred multicast source from the list of pre-configured sources for a given MVPN during (C-*, C-G) processing as follows:

- A single join for the group is sent to the most preferred multicast source from the operator-configured multicast source list. Joins to other multicast sources for a given group are suppressed. Operator can see active and suppressed joins on a Receiver PE. Although a join is sent to a single multicast source only, (C-S, C-G) state is created for every source advertising Type-5 S-A route on the Receiver PE.

- The most preferred multicast source is a reachable source with the highest local preference for Type-5 SA route based on the BGP policy, as described later in this section.

- On a failure of the preferred multicast source or when a new multicast source with a better local preference is discovered, Receiver PE will join the new most-preferred multicast source. The outage experienced will depend on how quickly Receiver PE receives Type-5 S-A route withdrawal or looses unicast route to multicast source, and how quickly the network can process joins to the newly selected preferred multicast source(s).

- Note: Local multicast sources on a Receiver PE are not subject to the most-preferred source selection, regardless of whether they are part of redundant source list or not.

BGP policy on Type-5 SA advertisements is used to determine the most preferred multicast source based on the best local preference as following:

- Each Source PE (a PE with multicast sources in its C-instance) tags Type-5 SA routes with a unique standard community attribute using global BGP policy or MVPN vrf-export policy. Depending on multicast topology, the policy may require source-aware tagging in the policy. Either all MVPN routes or Type 5 SA routes only can be tagged in the policy (new attribute `mvpn-type 5`).

- Each receiver PE has a BGP VRF import policy that sets local preference using match on Type-5 SA routes (new attribute `mvpn-type 5`) and standard community attribute value (as tagged by the Source PEs). Using policy statements that also include group address match, allows receiver PEs to select the best multicast source per group. The BGP VRF import policy must be applied as `vrf-import` under `config>service>vprn>mvpn` context. It must have default-action `accept` specified, or all MVPN routes other than those matched by specified entries will be rejected. In addition, it must have `vrf-target` as a community match condition, because `vrf-target mvpn` configuration is ignored when `vrf-import` policy is defined.

Operators can change redundant source list or BGP policy affecting source selection in service. If such a change of the list/policy results in a new preferred multicast source election, make-before-break is used to join the new source and prune the previously best source.
For the proper operations, MVPN multicast source geo-redundancy requires the router:

- To maintain the list of eligible multicast sources on Receiver PEs, Source PE routers must generate Type-5 S-A route even if the Source PE sees no active joins from any receiver for a given group.
- To trigger a switch from a currently active multicast source on a Receiver PE, Source PE routers must withdraw Type-5 S-A route when the multicast source fails or alternatively unicast route to multicast source must be withdrawn or go down on a Receiver PE.

MVPN multicast source redundancy solutions is supported for the following configurations only. Enabling the feature in unsupported configuration must be avoided:

1. NG-MVPN with RSVP-TE or mLDP or PIM with BGP c-multicast signaling in P-instance. Both I-PMSI and S-PMSI trees are supported.
2. IPv4 (C-*, C-G) PIM ASM joins in the C-instance.
3. Both intersite-shared enabled and disabled are supported. For intersite-shared enabled, operators must enable generation of Type-5 S-A routes even in the absence of receivers seen on Source PEs (intersite-shared persistent-type5-adv must be enabled).
4. The Source PEs must be configured as a sender-receiver, the Receiver PEs can be configured as a sender-receiver or a receiver-only.
5. The RP(s) must be on the Source PE(s) side. Static RP, anycast-RP, embedded-RP types are supported.
6. UMH redundancy can be deployed to protect Source PE to any multicast source. When deployed, UMH selection is executed independently of source selection after the most preferred multicast source had been chosen. Supported umh-selection options include: highest-ip, hash-based, and unicast-rt-pref (no support for tunnel-status).
Multicast Core Diversity for Rosen MDT_SAFI MVPNs

Figure 161 shows a Rosen VPN core diversity deployment.

Core diversity allows operators to optionally deploy multicast MVPN in either default IGP instance, or one of two non-default IGP instances to provide; for example, topology isolation or different level of services. The following describes the main feature attributes:

- Rosen MVPN IPv4 multicast with MDT SAFI is supported with default and data MDTs.
- Rosen MVPN can use a non-default OSPF or ISIS instance (using their loopback addresses instead of a system address).
- Up to 3 distinct core instances are supported: system + 2 non-default OSPF instances shown in Figure 161.
- Note that the BGP Connector also uses non-default OSPF loopback as NH, allowing Inter-AS option B/C functionality to work with Core diversity as well.
- The feature is supported with CSC-VPRN.
On source PEs (PE1: UMH, PE2: UMH in the above picture), an MVPN is assigned to a non-default IGP core instance as follows:

- MVPN is statically pointed to use one of the non-default IGP instances loopback addresses as source address instead of system loopback IP.
- MVPN export policy is used to change unicast route next-hop VPN address.

The configuration shown above ensures that MDT SAFI and IPVPN routes for the non-default core instance use non-default IGP loopback instead of system IP. This ensures PIM advertisement/joins run in the proper core instance and GRE tunnels for multicast can be set-up using and terminated on non-system IP. Note that if unicast traffic must be forwarded in non-default core instances 1 or 2, LDP or RSVP (terminating on non-system IP) must be used. GRE unicast traffic termination on non-system IP is not supported and any GRE traffic arriving at the PE in instances 1 or 2, destined to non-default IGP loopback IP will be forwarded to CPM (ACL or CPM filters can be used to prevent the traffic from reaching the CPM).

No configuration is required on non-source PEs.

Known feature caveats include:

- VPRN instance must be shutdown to change the mdt-safi source-address. Note that CLI rollback that includes change of the auto-discovery is thus service impacting.
- To reset mdt-safi source-address to system IP, operator must first execute no auto-discovery (or auto-discovery default) then auto-discovery mdt-safi
- Configuring system IP as a source-address will consume one of the 2 IP addresses allowed, thus it should not be done.
- When Rosen MVPN Core Diversity is deployed, only the default core instance (one using system IP) may use GRE tunnels for unicast traffic.
- Operators must configure proper IGP instance loopback IP addresses within Rosen MVPN context and configure proper BGP policies for the feature to operate as expected. There is no verification that the address entered for MVPN provider tunnel source-address is such an address or is not a system IP address.
- The feature requires all ports to be present on IOM3-XP or newer (Chassis Mode D). The restriction is not enforced. Failing to observe this restriction will prevent the feature to operate properly in the network.
Inter-AS MVPN

The Inter-AS MVPN feature allows set-up of Multicast Distribution Trees (MDTs) that span multiple Autonomous Systems (ASes). See Chapter, Virtual Private Routed Network Service, on page 1441 section of this guide for background on Inter-AS VPN support in SROS. This section focuses on multicast aspects of the Inter-AS MVPN solution.

To support Inter-AS option for MVPNs, a mechanism is required that allows setup of Inter-AS multicast tree across multiple ASes. Due to limited routing information across AS domains, it is not possible to setup the tree directly to the source PE. Inter-AS VPN Option A does not require anything specific to inter-AS support as customer instances terminate on ASBR and each customer instance is handed over to the other AS domain via a unique instance. This approach allows operators to provide full isolation of ASes, but the solution is the least scalable case, as customer instances across the network have to exist on ASBR.

Inter-AS MVPN Option B allows operators to improve upon the Option A scalability while still maintaining AS isolation, while Inter-AS MVPN option C further improves Inter-AS scale solution but requires exchange of Inter-AS routing information and thus is typically deployed when a common management exists across all ASes involved in the Inter-AS MVPN. The following sub-sections provide further details on Inter-AS Option B and Option C functionality.

BGP Connector Attribute

BGP connector attribute is a transitive attribute (unchanged by intermediate BGP speaker node) that is carried with VPNv4 advertisements. It specifies the address of source PE node that originated the VPNv4 advertisement.

With Inter-AS MVPN Option B, BGP next-hop is modified by local and remote ASBR during re-advertisement of VPNv4 routes. On BGP next-hop change, information regarding the originator of prefix is lost as the advertisement reaches the receiver PE node.

BGP connector attribute allows source PE address information to be available to receiver PE, so that a receiver PE is able to associate VPNv4 advertisement to the corresponding source PE.

PIM RPF Vector

In case of Inter-AS MVPN Option B, routing information towards the source PE is not available in a remote AS domain, since IGP routes are not exchanged between ASes. Routers in an AS other than that of a source PE, have no routes available to reach the source PE and thus PIM JOINs would never be sent upstream. To enable setup of MDT towards a source PE, BGP next-hop (ASBR) information from that PE's MDT-SAFI advertisement is used to fake a route to the PE. If the BGP next-hop is a PIM neighbor, the PIM JOINs would be sent upstream. Otherwise, the PIM
JOINs would be sent to the immediate IGP next-hop (P) to reach the BGP next-hop. Since the IGP next-hop does not have a route to source PE, the PIM JOIN would not be propagated forward unless it carried extra information contained in RPF Vector.

In case of Inter-AS MVPN Option C, unicast routing information towards the source PE is available in a remote AS PEs/ASBRs as BGP 3107 tunnels, but unavailable at remote P routers. If the tunnelled next-hop (ASBR) is a PIM neighbor, the PIM JOINs would be sent upstream. Otherwise, the PIM JOINs would be sent to the immediate IGP next-hop (P) to reach the tunnelled next-hop. Since the IGP next-hop does not have a route to source PE, the PIM JOIN would not be propagated forward unless it carried extra information contained in RPF Vector.

To enable setup of MDT towards a source PE, PIM JOIN thus carries BGP next hop information in addition to source PE IP address and RD for this MVPN. For option-B, both these pieces of information are derived from MDT-SAFI advertisement from the source PE. For option-C, both these pieces of information are obtained from the BGP tunnelled route.

The RPF vector is added to a PIM join at a PE router when configure router `pim rpfv` option is enabled. P routers and ASBR routers must also have the option enabled to allow RPF Vector processing. If the option is not enabled, the RPF Vector is dropped and the PIM JOIN is processed as if the PIM Vector were not present.

For further details about RPF Vector processing please refer to [RFCs 5496, 5384 and 6513]

---

**Inter-AS MVPN Option B**

Inter-AS Option B is supported for Rosen MVPN PIM SSM using BGP MDT SAFI, PIM RPF Vector and BGP Connector attribute. The Figure 162 depict set-up of a default MDT:

![Figure 162: Inter-AS Option B Default MDT Setup](al_0165)

---

Page 1250  7950 SR OS Services Guide
SROS inter-AS Option B is designed to be standard compliant based on the following RFCs:

- RFC 5384 - The Protocol Independent Multicast (PIM) Join Attribute Format
- RFC 5496 - The Reverse Path Forwarding (RPF) Vector TLV
- RFC 6513 - Multicast in MPLS/BGP IP VPNs

The SROS implementation was designed also to interoperate with older routers Inter-AS implementations that do not comply with the RFC 5384 and RFC 5496.

**Inter-AS MVPN Option C**

Inter-AS Option C is supported for Rosen MVPN PIM SSM using BGP MDT SAFI and PIM RPF Vector. Figure 163 depicts a default MDT setup:

Additional caveats for Inter-AS MVPN Option B and C support are the following:

1. Inter-AS MVPN option B is not supported with duplicate PE addresses.
2. For Inter-AS Option C, BGP 3107 routes are installed into unicast rtm (rtable-u), unless routes are installed by some other means into multicast rtm (rtable-m), and option C will not build core MDTs, therefore, rpf-table is configured to rtable-u or both.
3. Additional Cisco interoperability notes are the following:
   - RFC 5384 - The Protocol Independent Multicast (PIM) Join Attribute Format
   - RFC 5496 - The Reverse Path Forwarding (RPF) Vector TLV
   - RFC 6513 - Multicast in MPLS/BGP IP VPNs
The SROS implementation was designed to inter-operate with Cisco routers Inter-AS implementations that do not comply with the RFC5384 and RFC5496.

When `configure router pim rpfv mvpn` option is enabled, Cisco routers need to be configured to include RD in an RPF vector using the following command: `ip multicast vrf vrf-name rpf proxy rd vector` for interoperability. When Cisco routers are not configured to include RD in an RPF vector, operator should configure SROS router (if supported) using `configure router pim rpfv core mvpn`: PIM joins received can be a mix of core and mvpn RPF vectors.
Configuring a VPRN Service with CLI

This section provides information to configure Virtual Private Routed Network (VPRN) services using the command line interface.

Topics in this section include:

- Basic Configuration on page 1254
- Common Configuration Tasks on page 1256
  - Configuring VPRN Components on page 1257
    - Creating a VPRN Service on page 1257
    - Configuring Global VPRN Parameters on page 1258
    - Configuring VPRN Protocols - BGP on page 1261
    - Configuring VPRN Protocols - OSPF on page 1265
    - Configuring a VPRN Interface on page 1266
    - Configuring a VPRN Interface SAP on page 1267
- Service Management Tasks on page 1269
  - Modifying VPRN Service Parameters on page 1269
  - Deleting a VPRN Service on page 1270
  - Disabling a VPRN Service on page 1271
  - Re-enabling a VPRN Service on page 1272
Basic Configuration

The following fields require specific input (there are no defaults) to configure a basic VPRN service:

- Customer ID (refer to Configuring Customers on page 84)
- Specify interface parameters
- Specify spoke SDP parameters

The following example displays a sample configuration of a VPRN service.

*A:ALA-1>config>service>vprn# info
----------------------------------------------
vrf-import "vrfImpPolCust1"
vrf-export "vrfExpPolCust1"
ecmp 8
autonomous-system 10000
route-distinguisher 10001:1
auto-bind ldp
vrf-target target:10001:1
interface "to-ce1" create
    address 11.1.0.1/24
    proxy-arp
    exit
    sap 1/1/10:1 create
        ingress
            qos 100
            egress
                qos 1010
                filter ip 10
            exit
        exit
        dhcp
            description "DHCP test"
        exit
        vrrp 1
        exit
    exit
static-route 6.5.0.0/24 next-hop 10.1.1.2
bgp
    router-id 10.0.0.1
    group "to-cel"
        export "vprnBgpExpPolCust1"
        peer-as 65101
        neighbor 10.1.1.2
        exit
    exit
pim
    apply-to all
    rp
        static
        exit
        bsr-candidate
        shutdown
exit
rp-candidate
shutdown
exit
exit
exit
exit
rip
export "vprnRipExpPolCust1"
group "cel"
neighbor "to-ce1"
exit
exit
exit
no shutdown

----------------------------------------------
*A:ALA-1>config>service>vprn#
Common Configuration Tasks

This section provides a brief overview of the tasks that must be performed to configure a VPRN service and provides the CLI commands.

1. Associate a VPRN service with a customer ID.
2. Define an autonomous system (optional).
3. Define a route distinguisher (mandatory).
4. Define VRF route-target associations or VRF import/export policies.
5. Define PIM parameters (optional).
6. Create an interface.
7. Define SAP parameters on the interface.
   - Select node(s) and port(s).
   - Optional - select QoS policies other than the default (configured in `config>qos` context).
   - Optional - select filter policies (configured in `config>filter` context).
   - Optional - select accounting policy (configured in `config>log` context).
8. Define BGP parameters (optional).
   - BGP must be enabled in the `config>router>bgp` context.
10. Define spoke SDP parameters (optional).
11. Create confederation autonomous systems within an AS. (optional).
12. Enable the service.
Configuring VPRN Components

This section provides VPRN configuration examples for the following entities:

- Creating a VPRN Service on page 1257
- Configuring Global VPRN Parameters on page 1258
- Configuring Router Interfaces on page 1260
- Configuring VPRN Protocols - OSPF on page 1265
- Configuring a VPRN Interface SAP on page 1267
- Configuring VPRN Protocols - BGP on page 1261
- Configuring VPRN Protocols - RIP on page 1483

Creating a VPRN Service

Use the following CLI syntax to create a VPRN service. A route distinguisher must be defined in order for VPRN to be operationally active.

CLI Syntax: config>service# vprn service-id [customer customer-id]
            route-distinguisher [ip-address:number1 | asn:number2]
            description description-string
            no shutdown

The following example displays a VPRN service configuration.

*A:ALA-1>config>service# info
----------------------------------------------
...vprn 1 customer 1 create
        route-distinguisher 10001:0
        no shutdown
        exit
...----------------------------------------------
*A:ALA-1>config>service>vprn#
Configuring Global VPRN Parameters

Refer to VPRN Services Command Reference on page 1273 for CLI syntax to configure VPRN parameters.

The following example displays a VPRN service with configured parameters.

```
*A:ALA-1>config>service# info
----------------------------------------------
... vprn 1 customer 1 create
    vrf-import "vrfImpPolCust1"
    vrf-export "vrfExpPolCust1"
    autonomous-system 10000
    route-distinguisher 10001:1
    spoke-sdp 2 create
    exit
    no shutdown
    exit
...----------------------------------------------
*A:ALA-1>config>service#
```
Configuring a Spoke-SDP

Use the following CLI syntax to configure spoke SDP parameters:

CLI Syntax:

```
config>service# vprn service-id [customer customer-id]
    spoke-sdp sd-p-id
    no shutdown
    interface ip-int-name
    spoke-sdp sd-p-id:vc-id [vc-type {ether|vlan}]
    egress
    filter [ip ip-filter-id]
    vc-label egress-vc-label
    ingress
    filter [ip ip-filter-id]
    vc-label ingress-vc-label
    tos-marking-state {trusted|untrusted}
    no shutdown
```

The following output displays a spoke SDP configuration

```
A:ALA-48>config>service>vprn# info
---------------------------------------------
... interface "SpokeSDP" create
    spoke-sdp 3:4 create
    ingress
    vc-label 3000
    filter ip 10
    exit
    egress
    vc-label 2000
    filter ip 10
    exit
    exit
... spoke-sdp 3 create
    exit
    no shutdown
---------------------------------------------
A:ALA-48>config>service>vprn#
```
Configuring Router Interfaces

Refer to the for command descriptions and syntax information to configure router interfaces.

The following example displays a router interface configurations:

```
ALA48>config>router# info
#------------------------------------------
echo "IP Configuration"
#------------------------------------------
... interface "if1"
    address 2.2.2.1/24
    port 1/1/33
exit
interface "if2"
    address 10.49.1.46/24
    port 1/1/34
exit
interface "if3"
    address 11.11.1.1/24
    port 1/1/35
exit
...
#------------------------------------------
ALA48>config>router#
```
Configuring VPRN Protocols - BGP

The autonomous system number and router ID configured in the VPRN context only applies to that particular service.

The minimal parameters that should be configured for a VPRN BGP instance are:

- Specify an autonomous system number for the router. See Configuring Global VPRN Parameters on page 1258.
- Specify a router ID - Note that if a new or different router ID value is entered in the BGP context, then the new values takes precedence and overwrites the VPRN-level router ID. See Configuring Global VPRN Parameters on page 1258.
- Specify a VPRN BGP peer group.
- Specify a VPRN BGP neighbor with which to peer.
- Specify a VPRN BGP peer-AS that is associated with the above peer.

VPRN BGP is administratively enabled upon creation. Minimally, to enable VPRN BGP in a VPRN instance, you must associate an autonomous system number and router ID for the VPRN service, create a peer group, neighbor, and associate a peer AS number. There are no default VPRN BGP groups or neighbors. Each VPRN BGP group and neighbor must be explicitly configured.

All parameters configured for VPRN BGP are applied to the group and are inherited by each peer, but a group parameter can be overridden on a specific basis. VPRN BGP command hierarchy consists of three levels:

- The global level
- The group level
- The neighbor level
For example:

**CLI Syntax:**
```plaintext
config>service>vprn>bgp# (global level)
group (group level)
neighbor (neighbor level)
```

Note that the local-address must be explicitly configured if two systems have multiple BGP peer sessions between them for the session to be established.

For more information about the BGP protocol, refer to the OS Router Configuration Guide.

---

**Configuring VPRN BGP Group and Neighbor Parameters**

A group is a collection of related VPRN BGP peers. The group name should be a descriptive name for the group. Follow your group, name, and ID naming conventions for consistency and to help when troubleshooting faults.

All parameters configured for a peer group are applied to the group and are inherited by each peer (neighbor), but a group parameter can be overridden on a specific neighbor-level basis.

After a group name is created and options are configured, neighbors can be added within the same autonomous system to create IBGP connections and/or neighbors in different autonomous systems to create EBGP peers. All parameters configured for the peer group level are applied to each neighbor, but a group parameter can be overridden on a specific neighbor basis.

---

**Configuring Route Reflection**

Route reflection can be implemented in autonomous systems with a large internal BGP mesh to reduce the number of IBGP sessions required. One or more routers can be selected to act as focal points, for internal BGP sessions. Several BGP-speaking routers can peer with a route reflector. A route reflector forms peer connections to other route reflectors. A router assumes the role as a route reflector by configuring the `cluster cluster-id` command. No other command is required unless you want to disable reflection to specific peers.

If you configure the `cluster` command at the global level, then all subordinate groups and neighbors are members of the cluster. The route reflector cluster ID is expressed in dotted decimal notation. The ID should be a significant topology-specific value. No other command is required unless you want to disable reflection to specific peers.

If a route reflector client is fully meshed, the `disable-client-reflect` command can be enabled to stop the route reflector from reflecting redundant route updates to a client.
Configuring BGP Confederations

A VPRN can be configured to belong to a BGP confederation. BGP confederations are one technique for reducing the degree of IBGP meshing within an AS. When the confederation command is in the configuration of a VPRN the type of BGP session formed with a VPRN BGP neighbor is determined as follows:

- The session is of type IBGP if the peer AS is the same as the local AS.
- The session is of type confed-EBGP if the peer AS is different than the local AS AND the peer AS is listed as one of the members in the confederation command.
- The session is of type EBGP if the peer AS is different than the local AS AND the peer AS is not listed as one of the members in the confederation command.

When a VPRN is configured to belong to a confederation, the following VPRN commands cannot be configured:

- vrf-target
- vrf-import
- vrf-export
- grt-lookup
**VPRN BGP CLI Syntax**

Use the CLI syntax to configure VPRN BGP parameters (BGP Configuration Commands on page 1293).

The following example displays a VPRN BGP configuration:

*A:ALA-1>config>service# info
----------------------------------------------
...  
vprn 1 customer 1 create 
  vrf-import "vrfImpPolCust1"
vrf-export "vrfExpPolCust1"
ecmp 8
  autonomous-system 10000
  route-distinguisher 10001:1
  auto-bind ldp
  vrf-target target:10001:1
  interface "to-cel" create
    address 11.1.0.1/24
    sap 1/1/10:1 create
      ingress
        scheduler-policy "SLA2"
        qos 100
      exit
      egress
        scheduler-policy "SLA1"
        qos 1010
    filter ip 6
    exit
  exit
exit
static-route 6.5.0.0/24 next-hop 10.1.1.2
bgp
  router-id 10.0.0.1
  group "to-cel"
    export "vprnBgpExpPolCust1"
  peer-as 65101
  neighbor 10.1.1.2
    exit
  exit
  exit
  spoke-sdp 2 create
  exit
  no shutdown
  exit
...  
----------------------------------------------
*A:ALA-1>config>service#*
Configuring VPRN Protocols - OSPF

Each VPN routing instance is isolated from any other VPN routing instance, and from the routing used across the backbone. OSPF can be run with any VPRN, independently of the routing protocols used in other VPRNs, or in the backbone itself. For more information about the OSPF protocol, refer to the SR-OS Router Configuration Guide.

**CLI Syntax:** `config>service>vprn>ospf#`

---

**VPRN OSPF CLI Syntax**

Refer to [OSPF Configuration Commands on page 1298](#) for CLI syntax to configure VPRN parameters.

The following example displays the VPRN OSPF configuration shown above:

```bash
*A:ALA-48>config>service# info
----------------------------------------------
vprn 2 customer 1 create
    interface "test" create
    exit
    no shutdown
    exit
area 0.0.0.0
    virtual-link 1.2.3.4 transit-area 1.2.3.4
    hello-interval 9
    dead-interval 40
    exit
    exit
----------------------------------------------
*A:ALA-48>config>service#
```

For more information about the OSPF protocol, refer to the SR-OS Router Configuration Guide.
Configuring a VPRN Interface

Interface names associate an IP address to the interface, and then associate the IP interface with a physical port. The logical interface can associate attributes like an IP address, port, Link Aggregation Group (LAG) or the system.

There are no default interfaces.

Note that you can configure a VPRN interface as a loopback interface by issuing the `loopback` command instead of the `sap sap-id` command. The loopback flag cannot be set on an interface where a SAP is already defined and a SAP cannot be defined on a loopback interface.

When using mtrace/mstat in a Layer 3 VPN context then the configuration for the VPRN should have a loopback address configured which has the same address as the core instance's system address (BGP next-hop).

Refer to OSPF Configuration Commands on page 1298 for CLI commands and syntax.

The following example displays a VPRN interface configuration:

```
*A:ALA-1>config>service>vprn# info
----------------------------------------------
... vprn 1 customer 1 create
 vrf-import "vrfImpPolCust1"
 vrf-export "vrfExpPolCust1"
 ecmp 8
 autonomous-system 10000
 route-distinguisher 10001:1
 auto-bind ldp
 vrf-target target:10001:1
 interface "to-ce1" create
     address 11.1.0.1/24
     exit
 exit
 static-route 6.5.0.0/24 next-hop 10.1.1.2
 spoke-sdp 2 create
 exit
 no shutdown
 exit
... ----------------------------------------------
*A:ALA-1>config>service#
```
Configuring a VPRN Interface SAP

A SAP is a combination of a port and encapsulation parameters which identifies the service access point on the interface and within the SR. Each SAP must be unique within a router. A SAP cannot be defined if the interface `loopback` command is enabled.

When configuring VPRN interface SAP parameters, a default QoS policy is applied to each ingress and egress SAP. Additional QoS policies and scheduler policies must be configured in the `config>qos` context. Filter policies are configured in the `config>filter` context and must be explicitly applied to a SAP. There are no default filter policies.

Refer to OSPF Configuration Commands on page 1298 for CLI commands and syntax.

The following example displays a VPRN interface SAP configuration:

```
*A:ALA-1>config>service# info
----------------------------------------------
... vprn 1 customer 1 create
  vrf-import "vrfImpPolCust1"
  vrf-export "vrfExpPolCust1"
  ecmp 8
  autonomous-system 10000
  route-distinguisher 10001:1
  auto-bind ldp
  vrf-target target:10001:1
  interface "to-ce1" create
    address 11.1.0.1/24
    sap 1/1/10:1 create
    ingress
      scheduler-policy "SLA2"
      qos 100
    exit
    egress
      scheduler-policy "SLA1"
      qos 1010
      filter ip 6
    exit
  exit
  exit
  static-route 6.5.0.0/24 next-hop 10.1.1.2
  spoke-sdp 2 create
  exit
  no shutdown
  exit
... ----------------------------------------------
*A:ALA-1>config>service#
```
Configuring IPSec Parameters

The following output displays service with IPSec parameters configured.

+A:ALA-49>config# info
----------------------------------------------
... service
ies 100 customer 1 create
    interface "ipsec-public" create
    address 10.10.10.1/24
    sap ipsec-1.public:1 create
    exit
    exit
    no shutdown
    exit
vprn 200 customer 1 create
ipsec
    security-policy 1 create
    entry 1 create
    local-ip 172.17.118.0/24
    remote-ip 172.16.91.0/24
    exit
    exit
    exit
route-distinguisher 1:1
ipsec-interface "ipsec-private" create
    sap ipsec-1.private:1 create
    tunnel "remote-office" create
    security-policy 1
    local-gateway-address 10.10.10.118 peer 10.10.7.91 delivery-service
100
    dynamic-keying
    ike-policy 1
    pre-shared-key "humptydumpty"
    transform 1
    exit
    no shutdown
    exit
    exit
    exit
interface "corporate-network" create
    address 172.17.118.118/24
    sap 1/1/2 create
    exit
    exit
    exit
    static-route 172.16.91.0/24 ipsec-tunnel "remote-office"
    no shutdown
    exit
    exit
...----------------------------------------------
+A:ALA-49>config#
Service Management Tasks

This section discusses the following service management tasks:

- Modifying VPRN Service Parameters on page 1269
- Deleting a VPRN Service on page 1270

Modifying VPRN Service Parameters

Use the CLI syntax to modify VPRN parameters (VPRN Services Command Reference on page 1273).

The following example displays the VPRN service creation output.

*A:ALA-1>config>service# info
-------------------------------------------------
... vprn 1 customer 1 create
    shutdown
    vrf-import "vrfImpPolCust1"
    vrf-export "vrfExpPolCust1"
    ecmp 8
    maximum-routes 2000
    autonomous-system 10000
    route-distinguisher 10001:1
    interface "to-ce1" create
        address 10.1.1.1/24
        sap 1/1/10:1 create
        exit
    exit
    static-route 6.5.0.0/24 next-hop 10.1.1.2
    bgp
        router-id 10.0.0.1
        group "to-ce1"
            export "vprnBgpExpPolCust1"
            peer-as 65101
            neighbor 10.1.1.2
            exit
        exit
    exit
    spoke-sdp 2 create
    exit
    exit
...
-------------------------------------------------
*A:ALA-1>config>service>vprn#
Deleting a VPRN Service

An VPRN service cannot be deleted until SAPs and interfaces are shut down and deleted. If protocols and/or a spoke-SDP are defined, they must be shut down and removed from the configuration as well.

Use the following CLI syntax to delete a VPRN service:

**CLI Syntax:**
```
config>service#
[no] vprn service-id [customer customer-id]
  shutdown
[no] interface ip-int-name
  shutdown
[no] sap sap-id
[no] bgp
  shutdown
[no] rip
  shutdown
[no] spoke-sdp sdp-id
[no] shutdown
```
Disabling a VPRN Service

A VPRN service can be shut down without deleting any service parameters.

**CLI Syntax:**
```
config>service#
  vprn service-id [customer customer-id]
  shutdown
```

**Example:**
```
config>service# vprn 1
  config>service>vprn# shutdown
  config>service>vprn# exit

*A:ALA-1>config>service# info
----------------------------------------------
...  vprn 1 customer 1 create
    shutdown
    vrf-import "vrfImpPolCust1"
    vrf-export "vrfExpPolCust1"
    ecmp 8
    autonomous-system 10000
    route-distinguisher 10001:1
    auto-bind ldp
    vrf-target target:10001:1
    interface "to-cel" create
      address 11.1.0.1/24
      sap 1/1/10:1 create
        ingress
          scheduler-policy "SLA2"
          qos 100
        exit
        egress
          scheduler-policy "SLA1"
          qos 1010
          filter ip 6
        exit
    exit
  exit
  static-route 6.5.0.0/24 next-hop 10.1.1.2
  bgp
    router-id 10.0.0.1
    group "to-cel"
      export "vprnBgpExpPolCust1"
      peer-as 65101
      neighbor 10.1.1.2
    exit
  exit
  rip
    export "vprnRipExpPolCust1"
    group "cel"
    neighbor "to-cel"
  exit
  exit
  spoke-sdp 2 create
  exit
  exit
  exit
...```

*A:ALA-1>config>service#*
Re-enabling a VPRN Service

To re-enable a VPRN service that was shut down.

**CLI Syntax:**
```
config>service#
  vprn service-id [customer customer-id]
  no shutdown
```
VPRN Services Command Reference

Command Hierarchies

- VPRN Service Configuration Commands on page 1274
  → IGMP Commands on page 1277
  → Multicast VPN Commands on page 1279
  → Interface Commands on page 1282
    - Interface Spoke SDP Commands on page 1286
    - Interface SAP Commands on page 1290
    - IPSec Gateway Commands on page 1689
    - Interface VRRP Commands on page 1288
  → Network Interface Commands on page 1284
  → BGP Configuration Commands on page 1293
  → OSPF Configuration Commands on page 1298
  → PIM Configuration Commands on page 1301
- Show Commands on page 1305
- Clear Commands on page 1307
- Debug Commands on page 1308
VPRN Service Configuration Commands

```
config
  service
    vprn service-id [customer customer-id]
    no vprn service-id
    aggregate ip-prefix/ip-prefix-length [summary-only] [as-set] [aggregator as-number: ip-address] [community comm-id] [black-hole | indirect ip-address]
    no aggregate ip-prefix/ip-prefix-length
    auto-bind {ldp | gre | rsvp-te | mpls}
    no auto-bind
    autonomous-system as-number
    no autonomous-system
    backup-path [ipv4]|ipv6
    no carrier-carrier-vpn
    confederation confed-as-num members as-number [as-number...(up to 15 max)]
    no confederation confed-as-num members as-number [as-number...(up to 15 max)]
    no confederation
    description description-string
    no description
    [no] dns
      ipv4-source-address ipv4-address
      no ipv4-source-address
      ipv6-source-address ipv6-address
      no ipv6-source-address
      primary-dns ip-address
      no primary-dns
      secondary-dns ip-address
      no secondary-dns
      [no] shutdown
      tertiary-dns ip-address
      no tertiary-dns
      ecmp max-ecmp-routes
      no ecmp
      eth-cfm
        tunnel-fault [accept | ignore]
      grt-lookup
        [no] enable-grt
          [no] allow-local-management
          static-route {ip-prefix/prefix-length | ip-prefix netmask} [preference preference] [metric metric] [enable|disable] grt
          no static-route
          export-grt policy-name [policy-name ...(up to 5 max)]
          export-limit num-routes
          no export-limit
          export-v6-limit
          no export-v6-limit
        [no] hash-label
        igmp-host-tracking
          expiry-time expiry-time
          no expiry-time
          [no] shutdown
        maximum-routes number [log-only] [threshold percent]
        no maximum-routes
```
— mc-maximum-routes number [log-only] [threshold percent]
— no mc-maximum-routes
— multicast-info-policy policy-name
— no multicast-info-policy
— mvpn
— [no] ptp
  — peer a.b.c.d [create]
    — no peer a.b.c.d
      — priority local-priority
    — no priority
      — [no] shutdown
    — peer-limit limit
    — no peer-limit
      — [no] shutdown
— reassembly-group nat-group-id
— route-distinguisher [ip-address:number1 | asn:number2]
— no route-distinguisher
— router-id ip-address
— no router-id
— service-name service-name
— no service-name
— sgt-qos
  — application dscp-app-name dscp [dscp-value \ dscp-name]
  — application dotlp-app-name dotlp dotlp-priority
  — no application [dscp-app-name \ dotlp-app-name]
  — dscp dscp-name fc fc-name
  — no dscp dscp-name
— [no] shutdown
— shutdown
— snmp-community community-name [version SNMP-version]
— no snmp-community community-name
— source-address
  — application app [ip-int-name \ ip-address]
  — no application app
— [no] spoke-sdp sdp-id
  — [no] control-word
  — [no] when used with IES and VPRN services hash-label
    — agi agi
    — no agi
    — saii-type2 global-id:node-id:ac-id
    — no saii-type2
    — taii-type2 global-id:node-id:ac-id
    — no taii-type2
— [no] shutdown
— [no] static-route [ip-prefix/prefix-length \ ip-prefix netmask] [preference preference] [metric metric] [tag tag] [community comm-id] [enable \ disable] [next-hop ip-int-name] [ip-address] [mcast-family] [ipsec-tunnel] [ipsec-tunnel-name] [bfd-enable] [cpe-check cpe-ip-address [interval seconds] [drop-count count] [log]]
— [no] static-route [ip-prefix/prefix-length \ ip-prefix netmask] [preference preference] [metric metric] [tag tag] [community comm-id] [enable \ disable] indirect ip-address [cpe-check cpe-ip-address [interval seconds] [drop-count count] [log]]
— [no] static-route [ip-prefix/prefix-length \ ip-prefix netmask] [preference preference] [metric metric] [tag tag] [community comm-id] [enable \ disable] black-hole [mcast-family]
— **type** {hub | spoke | subscriber-split-horizon}
— **no type**
— **vrf-export** policy-name [policy-name...(upto 16 max)]
— **no vrf-export**
— **vrf-import** policy-name [policy-name...(upto 16 max)]
— **no vrf-import**
— **vrf-target** {ext-comm|[export ext-comm][import ext-comm]} }]
— **no vrf-target**

—
—
— **no**
IGMP Commands

config
  — service
    — vprn service-id [customer customer-id]
    — no vprn service-id
      — [no] igmp
        — [no] group-interface ip-int-name
        — [no] group-interface fwd-service service-id ip-int-name
          — [no] disable-router-alert-check
          — import policy-name
          — no import
          — max-groups value
          — no max-groups
          — max-grp-sources [1..32000]
          — no max-grp-sources
          — max-sources [1..1000]
          — no max-sources
          — mcac
            — mc-constraints
              — [no] shutdown
              — policy policy-name
              — no policy
              — unconstrained-bw bandwidth mandatory-bw mandatory-bw
                — no unconstrained-bw
                — query-src-ip ip-address
                — no query-src-ip
                — [no] shutdown
                — [no] sub-hosts-only
                — [no] subnet-check
                — version version
                — no version
                — grp-if-query-src-ip ip-address
                — no grp-if-query-src-ip
              — [no] interface ip-int-name
                — [no] disable-router-alert-check
                — import policy-name
                — no import
                — max-groups value
                — no max-groups
                — max-sources [1..32000]
                — no max-sources
                — max-grp-sources [1..1000]
                — no max-grp-sources
                — mcac
                  — mc-constraints
                    — level level-id bw bandwidth
                    — no level level-id
                    — number-down number-lag-port-down
                    — number-down number-lag-port-down level level-id
                    — [no] shutdown
                    — policy policy-name
— no policy
  — unconstrained-bw bandwidth mandatory-bw mandatory-bw
  — no unconstrained-bw
— [no] shutdown
— ssm-translate
  — [no] grp-range start end
  — [no] source ip-address
— static
  — [no] group grp-ip-address
  — [no] source ip-address
  — [no] starg
— [no subnet-check
— version version
— no version
— [no] query-interval
— query-interval seconds
— [no] query-last-member-interval
— query-last-member-interval seconds
— [no] query-response-interval
— query-response-interval seconds
— [no] robust-count
— robust-count robust-count
— [no] shutdown
— ssm-translate
  — [no] grp-range start end
  — [no] source ip-address
Multicast VPN Commands

```plaintext
config
  service
    vprn service-id [customer customer-id]
    no vprn service-id
    mvpn
      [no] auto-discovery [default | mdt-safi] [source-address ip-address]
      c-mcast-signaling [bgp | pim]
      no c-mcast-signaling
      intersite-shared [persistend-type5-adv]
      no intersite-shared
      mdt-type {sender-receiver | sender-only | receiver-only}
      red-source-list
        src-prefix ip-address/mask [ip-address/mask> ...up to 8 maximum]
      no src-prefix ip-address/mask
      provider-tunnel
        inclusive
          mldp
            [no] shutdown
          pim {asm | ssm} grp-ip-address
          no pim
            hello-interval hello-interval
            no hello-interval
            hello-multiplier deci-units
            no hello-multiplier
            [no] improved-assert
            [no] shutdown
            [no] three-way-hello
            [no] tracking-support
        selective
          [no] auto-discovery-disable
          data-delay-interval value
          no data-delay-interval
          data-threshold {c.grp-ip-addr/mask|c.grp-ipv6-addr/prefix-length} s-pmsi-threshold
          no data-threshold {c.grp-ip-addr/mask|c.grp-ipv6-addr/prefix-length}
          [no] enable-asm-mdt
          [no] join-tlv-packing-disable
          [no] pim-asn {grp-ip-address/mask|grp-ipv6-addr/prefix-length}
          pim-ssm {grp-ip-address/mask|grp-ipv6-addr/prefix-length}
            [no] pim-asn
          umh-pe-backup
            umh-pe ip-address standby ip-address
            no umh-pe ip-address
          umh-selection {highest-ip|hash-based|tunnel-status|unicast-rt-pref}
          no umh-selection
```
— vrf-export \{unicast | policy-name [policy-name...(up to 5 max)]\}
— no vrf-export
— vrf-import \{unicast [policy-name [policy-name...(up to 5 max)]\]
— no vrf-import
— vrf-target \{unicast | ext-community | export unicast | ext-community | import unicast | ext-community\}
— no vrf-target
  — export \{unicast | ext-community\}
  — import \{unicast | ext-community\}
Redundant Interface Commands

```
config
  service
    vprn service-id [customer customer-id]
    no vprn service-id
    [no] redundant-interface ip-int-name
    [no] address {ip-address/mask | ip-address netmask} [remote-ip ip-address]
    no address
    [no] description description-string
    [no] shutdown
    [no] spoke-sdp sdp-id:vc-id
    egress
      filter [ip ip-filter-id]
      vc-label ingress-vc-label
      no vc-label [ingress-vc-label]
    ingress
      filter [ip ip-filter-id]
      no filter
      vc-label ingress-vc-label
      no vc-label [ingress-vc-label]
    [no] shutdown
  [no] enable-ingress-stats
      [no] squelch-ingress-levels [md-level [md-level...]]
```
Interface Commands

```
config
  service
  vprn
    [no] interface ip-int-name
    [no] active-cpm-protocols
    address ip-address[/mask] [netmask] [broadcast {all-ones | host-ones}]
    no address [ip-address/mask | ip-address netmask]
    [no] allow-directed-broadcasts
    [no] arp-populate
    arp-timeout [seconds]
    no arp-timeout
    authentication-policy name
    no authentication-policy
    bfd transmit-interval [receive receive-interval] [multiplier multiplier]
        [echo-receive echo-interval]
    no bfd
    cflowd {acl | interface} [direction]
    no cflowd
    delayed-enable seconds
    no delayed-enable
    description description-string
    no description [description-string]
    dynamic-tunnel-redundant-next-hop ip-address
    no dynamic-tunnel-redundant-next-hop
    egr-ip-load-balancing {src-if | dst-ip}
    [no] enable-ingress-stats
    [no] enable-mac-accounting
    host-connectivity-verify [source {vrrp | interface}] [interval interval]
        [action {remove | alarm}]
        icmp
        [no] mask-reply
        redirects number seconds
        no redirects [number seconds]
        ttl-expired number seconds
        no ttl-expired [number seconds]
        unreachables number seconds
        no unreachables [number seconds]
    if-attribute
    [no] admin-group group-name [group-name...(up to 5 max)]
    [no] admin-group
    [no] srlg-group group-name [group-name...(up to 5 max)]
    no srlg-group
    ip-mtu octets
    no ip-mtu
    ipcp
    dns ip-address [secondary ip-address]
    dns secondary ip-address
    no dns [ip-address] [secondary ip-address]
    peer-ip-address ip-address
    no peer-ip-address
    [no] ipv6
    address ipv6-address/prefix-length [eui-64] [preferred]
    no address ipv6-address/prefix-length
```
— bfd transmit-interval [receive receive-interval] [multiplier multiplier][echo-receive echo-interval] [type cpm-np]
  — no bfd
— [no] dhcp6-relay
  — lease-populate [nbr-of-leases]
  — no lease-populate
  — [no] neighbor-resolution
— [no] dhcp6-server
— icmp6
— [no] local-proxy-nd
— neighbor ipv6-address mac-address
  — no neighbor ipv6-address
— proxy-nd-policy policy-name [policy-name...(up to 5 max)]
  — no proxy-nd-policy
— [no] qos-route-lookup
— [no] urpf-check
  — mode {strict | loose |strict-no-ecmp}
  — no mode
— local-dhcp-server local-server-name
  — no local-dhcp-server
— [no] local-proxy-arp
  — no loopback
— mac ieee-address
  — no mac [ieee-address]
— monitor-oper-group name
  — no monitor-oper-group
— [no] proxy-arp-policy
  — [no] ptp-hw-assist
— qos-route-lookup [source | destination]
  — no qos-route-lookup
— [no] remote-proxy-arp
  — secondary {ip-address/mask | ip-address netmask} [broadcast all-ones | host-ones] [igp-inhibit]
  — no secondary {ip-address/mask | ip-address netmask}
  — [no] shutdown
— static-arp ip-address ieee-address
  — no static-arp ip-address [ieee-address]
— static-tunnel-redundant-next-hop ip-address
  — no static-tunnel-redundant-next-hop
— [no] teid-load-balancing
— tos-marking-state [trusted | untrusted]
  — no tos-marking-state
— unnumbered [ip-int-name | ip-address]
  — no unnumbered
— [no] urpf-check
  — mode {strict | loose |strict-no-ecmp}
  — no mode
Network Interface Commands

config
  — service
  — vprn
    — network-interface interface-name [create]
    — no network-interface interface-name
      — address ip-address[/mask] [netmask] [broadcast {all-ones | host-ones}]
      — no address
      — [no] allow-directed-broadcasts
      — [no] arp-populate
      — arp-timeout [seconds]
      — no arp-timeout
      — bfd transmit-interval [receive receive-interval] [multiplier multiplier][echo-receive echo-interval]
      — no bfd
      — cflowd {acl | interface} [direction]
      — no cflowd
      — [mac-monitoring] | [eth-cfm-monitoring|aggregate][car] delayed-enable seconds
      — no delayed-enable
      — description description-string
      — no description [description-string]
      — dist-cpu-protection policy-name
      — no dist-cpu-protection
      — egr-ip-load-balancing {src-if | dst-ip}
      — ingress
        — filter ip ip-filter-id
        — filter ipv6 ipv6-filter-id
        — no filter [ip ip-filter-id] [ipv6 ipv6-filter-id]
    — icmp
      — [no] mask-reply
      — redirects number seconds
      — no redirects [number seconds]
      — ttl-expired number seconds
      — no ttl-expired [number seconds]
      — unreachableables number seconds
      — no unreachableables [number seconds]
    — ingress
      — filter ip ip-filter-id
      — filter ipv6 ipv6-filter-id
      — no filter [ip ip-filter-id] [ipv6 ipv6-filter-id]
      — [no] flowspec-ipv6
      — [no] flowspec-ipv6
    — lag lag-id[:encap-val]
    — no lag
    — [no] loopback
    — lsr-load-balancing hashing-algorithm
    — no lsr-load-balancing
    — mac ieee-address
    — no mac
    — [no] ntp-broadcast
    — qos network-policy-id port-redirect-group queue-group-name egress-instance instance-id fp-redirect-group queue-group-name ingress-instance instance-id
— no-qos
— secondary \{ip-address/mask | ip-address netmask\} [broadcast all-ones | host-ones] [igp-inhibit]
— no secondary \{ip-address/mask | ip-address netmask\}
— static-arp ieee-mac-address unnumbered
— no static-arp unnumbered
— [no] teid-load-balancing
— tos-marking-state \{trusted | untrusted\}
— no tos-marking-state
— [no] urpf-check
  — mode \{strict | loose | strict-no-ecmp\}
Interface Spoke SDP Commands

```
config
  service
    vprn service-id [customer customer-id]
    no vprn service-id
    interface ip-int-name
      spoke-sdp sdp-id [vc-id] vc-type {ether|pipe} [create]
      no spoke-sdp sdp-id [vc-id] vc-type {ether|pipe} [create]
      aarp aarpId type
      no aarp
      accounting-policy acct-policy-id
      no accounting-policy
      [no] collect-stats
      egress
      filter ip ip-filter-id
      no filter
      qos network-policy-id port-redirect-group queue-group-name
      [instance instance-id]
      no qos
      vc-label egress-vc-label
      no vc-label [egress-vc-label]
    eth-cfm
      mep mep-id domain md-index association ma-index
      [direction {up | down}]
      no mep mep-id domain md-index association ma-index
      [no] ais-enable
      [no] interface-support-enable
      [no] ccm-enable
      ccm-ltm-priority priority
      no ccm-ltm-priority
      ccm-padding-size ccm-padding
      no ccm-padding-size ccm-padding
      [no] csf-enable
      multiplier multiplier-value
      no multiplier
      [no] description
      [no] eth-test-enable
      [no] test-pattern {all-zeros | all-ones} [crc-enable]
      fault-propagation-enable {use-if-tlv | suspend-cmc}
      no fault-propagation-enable
      low-priority-defect {allDef | macRemErrXcon | remErrXcon | errXcon | xcon | noXcon}
      one-way-delay-threshold seconds
      [no] squelch-ingress-levels [md-level [md-level...]]
      [no] flowspec
      [no] flowspec-ipv6
    ingress
      filter ip ip-filter-id
      filter ipv6 ipv6-filter-id
      no filter
      [no] flowspec
```
— [no] flowspec
— qos network-policy-id fp-redirect-group queue-group-name instance instance-id
— no qos
— vc-label ingress-vc-label
— no vc-label [ingress-vc-label]
— [no] shutdown
VPRN Services Command Reference

Interface VRRP Commands

```text
cfg service
do vprn service-id [customer customer-id]
do vprn service-id
  interface ip-int-name
  ipv6
      vrrp virtual-router-id [owner]
do vrrp virtual-router-id 
      [no] backup ip-address
      bfd-enable interface interface-name dst-ip ip-address
      bfd-enable service-id interface interface-name dst-ip ip-address
      no bfd-enable interface interface-name dst-ip ip-address
      no bfd-enable service-id interface interface-name dst-ip ip-address
      init-delay seconds
      no init-delay
      mac ieee-address
      no mac
      [no] master-int-inherit
      message-interval {[seconds] [milliseconds milliseconds]}
do message-interval
      [no] ping-reply
      policy vrrp-policy-id
      no policy
      [no] preempt
      priority priority
      no priority
      [no] shutdown
      [no] ssh-reply
      [no] standby-forwarding
      [no] telnet-reply
      [no] traceroute-reply
      vrrp virtual-router-id [owner]
do vrrp virtual-router-id
      authentication-key {authentication-key | hash-key} [hash | hash2]
do authentication-key
      authentication-type {password | message-digest}
do authentication-type
      [no] backup ip-address
      [no] bfd-enable [service-id] interface interface-name dst-ip ip-address
      init-delay seconds
      no init-delay
      mac ieee-address
      no mac
      [no] master-int-inherit
      message-interval {[seconds] [milliseconds milliseconds]}
do message-interval
```
— [no] ping-reply
— policy vrrp-policy-id
— no policy
— [no] preempt
— priority priority
— no priority
— [no] shutdown
— [no] ssh-reply
— [no] standby-forwarding
— [no] telnet-reply
— [no] traceroute-reply
Interface SAP Commands

```
config
  — service
    — vprn service-id [customer customer-id]
    — no vprn service-id
    — [no] interface ip-int-name [create] [tunnel]
      — [no] sap sap-id
        — aarp aarpId type
        — no aarp
        — accounting-policy acct-policy-id
        — no accounting-policy [acct-policy-id]
        — anti-spoof {ip | mac | ip-mac}
        — no anti-spoof
        — calling-station-id calling-station-id
        — no calling-station-id
        — [no] collect-stats
        — description description-string
        — no description [description-string]
        — dist-cpu-protection policy-name
        — no dist-cpu-protection
        — egress
          — [no] agg-rate
            — [no] limit-unused-bandwidth
            — [no] queue-frame-based-accounting
            — rate {max | rate}
            — no rate
          — filter ip ip-filter-id
            — no filter [ip ip-filter-id]
            — [no] qinq-mark-top-only
          — qos policy-id [port-redirect-group queue-group-name instance instance-id]
            — no qos
            — [no] queue-override
              — [no] queue queue-id
                — adaptation-rule [pir adaptation-rule]
                  — cir adaptation-rule
                  — no adaptation-rule
                  — avg-frame-overhead percentage
                  — no avg-frame-overhead
                  — cbs size-in-kbytes
                  — no cbs
                  — high-prio-only percent
                  — no high-prio-only
                  — mbs {size-in-kbytes | default}
                  — no mbs
                  — rate pir-rate [cir cir-rate]
                  — no rate
                — [no] scheduler-override
                  — [no] scheduler scheduler-name
                    — rate pir-rate [cir cir-rate]
                    — no rate
                  — scheduler-policy scheduler-policy-name
                  — no scheduler-policy
```
--- eth-cfm
  --- mep mep-id domain md-index association ma-index
    [direction {up | down}]
  --- no mep mep-id domain md-index association ma-index
    [no] ais-enable
    [no] interface-support-enable
  --- [no] ccm-enable
  --- ccm-letm-priority priority
  --- no ccm-letm-priority
  --- [no] ccm-padding-size ccm-padding
  --- [no] csf-enable
    --- multiplier multiplier-value
    --- no multiplier
  --- [no] description
  --- [no] eth-test-enable
    [no] test-pattern {all-zeros | all-ones}
    [crc-enable]
  --- fault-propagation-enable {use-if-tlv | suspend-ccm}
  --- no fault-propagation-enable
  --- low-priority-defect {allDef | macRemErrXcon | remErrXcon | errXcon | noXcon}
    [no] squelch-ingress-levels [md-level [md-level...]]
  --- tunnel-fault [accept | ignore]
  --- [no] flowspec
  --- [no] flowspec-ipv6
  --- host-lockout-policy policy-name
  --- no host-lockout-policy
  --- [no] host-shutdown
  --- ingress
    --- filter ip ip-filter-id
    --- no filter [ip ip-filter-id]
    [no] flowspec
    [no] flowspec
    [no] flowspec
    match-qinq-dot1p {top | bottom}
    --- qos policy-id [shared-queueing | multipoint-shared][fp-redirect-group queue-group-name]
    [no] qos
  --- [no] queue-override
  --- [no] queue queue-id
    --- adaptation-rule [pir adaptation-rule] [cir adaptation-rule]
    [no] adaptation-rule
    --- avg-frame-overhead percentage
    [no] avg-frame-overhead
    --- cbs size-in-kbytes
    [no] cbs
    --- high-prio-only percent
    [no] high-prio-only
    --- mbs {size-in-kbytes | default}
    [no] mbs
BGP Configuration Commands

```
config
  -- service
    -- vprn service-id [customer customer-id]
    -- no vprn service-id
    -- [no] bgp-shared-queue
    -- [no] bgp
      -- [no] advertise-inactive
      -- [no] aggregator-id-zero
      -- [no] always-compare-med
      -- auth-keychain name
      -- authentication-key [authentication-key | hash-key] [hash | hash2]
      -- no authentication-key
      -- backup-path [ipv4]
      -- best-path-selection
        -- always-compare-med [zero|infinity]
        -- always-compare-med strict-as {zero|infinity}
        -- no always-compare-med
        -- as-path-ignore [ipv4] [ipv6]
        -- no as-path-ignore
        -- [no] deterministic-med
      -- [no] bfd-enable
      -- cluster cluster-id
      -- no cluster
      -- [no] connect-retry seconds
      -- [no] damp-peer-oscillations [idle-hold-time initial-wait second-wait max-wait] [error-interval minutes]
      -- [no] damping
      -- description description-string
      -- no description
      -- [no] disable-4byte-asn
      -- [no] disable-client-reflect
      -- disable-communities [standard] [extended]
      -- no disable-communities
      -- [no] disable-fast-external-failover
      -- [no] eibgp-loadbalance
      -- enable-bgp-vpn-backup [ipv4] [ipv6]
      -- no enable-bgp-vpn-backup
      -- [no] enable-peer-tracking
      -- error-handling
        -- [no] update-fault-tolerance
      -- export policy-name [policy-name...(upto 5 max)]
      -- no export
      -- family [ipv4][ipv6] [mcast-ipv4] [flow-ipv4]
      -- no family
      -- flowspec-validate
      -- [no] flowspec-validate
      -- family
      -- [no] graceful-restart
        -- enable-notification
        -- restart-time seconds
        -- [no] stale-routes-time time
      -- hold-time seconds [min seconds2]
```
— no hold-time
— [no] ibgp-multipath
— import policy-name [policy-name...(up to 5 max)]
— no import
— keepalive seconds
— no keepalive
— local-as as-number [private]
— no local-as
— local-preference local-preference
— no local-preference
— loop-detect {drop-peer | discard-route | ignore-loop | off}
— no loop-detect
— med-out {number | igp-cost}
— no med-out
— min-route-advertisement seconds
— no min-route-advertisement
— multihop ttl-value
— no multihop
— multipath max-paths [eibgp]
— no multipath
— next-hop-resolution
   — policy policy-name
— peer-tracking-policy policy-name
— preference preference
— no preference
— [no] rapid-update {[l2-vpn] [mpv4-ipv4]}
— [no] rapid-withdrawal
— [no] remove-private
— router-id ip-address
— no router-id
— [no] shutdown
— [no] split-horizon
— [no] group name [dynamic-peer]
   — [no] advertise-inactive
   — [no] aggregator-id-zero
   — [no] as-override
   — auth-keychain name
   — authentication-key [authentication-key | hash-key] [hash | hash2]
— no authentication-key
— [no] bfd-enable
— cluster cluster-id
— no cluster
— connect-retry seconds
— no connect-retry
— [no] damp-peer-oscillations [idle-hold-time initial-wait second-wait max-wait] [error-interval minutes]
— [no] damping
— description description-string
— no description
— [no] disable-4byte-asn
— [no] disable-client-reflect
— disable-communities [standard] [extended]
— no disable-communities
— [no] disable-fast-external-failover
— [no] enable-peer-tracking
— error-handling
   — [no] update-fault-tolerance
— export policy-name [policy-name...(upto 5 max)]
— no export
— family [ipv4][ipv6] [mcast-ipv4] [flow-ipv6] [flow-ipv4]
— no family
— flowspec-validate
— [no] flowspec-validate
— [no] graceful-restart
   — enable-notification
   — restart-time seconds
     — [no] stale-routes-time time
— hold-time seconds [min seconds2]
— no hold-time
— import policy-name [policy-name...(upto 5 max)]
— no import
— keepalive seconds
— no keepalive
— local-address ip-address
— no local-address
— local-as as-number [private] [no-prepend-global-as]
— no local-as
— local-preference local-preference
— no local-preference
— loop-detect {drop-peer|discard-route|ignore-loop|off}
— no loop-detect
— med-out {number | igp-cost}
— no med-out
— min-as-origination seconds
— no min-as-origination
— min-route-advertisement seconds
— no min-route-advertisement
— multihop ttl-value
— no multihop
— [no] next-hop-self
— [no] passive
— peer-as as-number
— no peer-as
— preference preference
— no preference
— prefix-limit limit [log-only] [threshold percent] [idle-timeout {minutes | forever}]
— no prefix-limit
— [no] remove-private
— [no] shutdown
— ttl-security min-ttl-value
— no ttl-security
— type {internal | external}
— no type
— [no] updated-error-handling
— [no] neighbor ip-address
   — [no] advertise-inactive
   — [no] aggregator-id-zero
— [no] as-override
— auth-keychain name
— authentication-key [authentication-key | hash-key]
  [hash | hash2]
— no authentication-key
— [no] bfd-enable
— cluster cluster-id
— no cluster
— connect-retry seconds
— no connect-retry
— [no] damp-peer-oscillations [idle-hold-time initial-wait second-wait max-wait] [error-interval minutes]
— [no] damping
— description description-string
— no description
— [no] disable-4byte-asn
— [no] disable-client-reflect
— disable-communities [standard] [extended]
— no disable-communities
— [no] disable-fast-external-failover
— [no] enable-peer-tracking
— error-handling
  — [no] update-fault-tolerance
— export policy-name [policy-name...(upto 5 max)]
— no export
  — enable-notification
  — restart-time seconds
  — [no] stale-routes-time time
— family [ipv4][ipv6] [mcast-ipv4] [flow-ipv6] [flow-ipv4]
— no family
— flowspec-validate
— [no] flowspec-validate
— hold-time seconds [min seconds2]
— no hold-time
— import policy-name [policy-name...(upto 5 max)]
— no import
— family [ipv4]
— keepalive seconds
— no keepalive
— local-address ip-address
— no local-address
— local-as as-number [private] [no-prepend-global-as]
— no local-as
— local-preference local-preference
— no local-preference
— loop-detect {drop-peer | discard-route | ignore-loop | off}
— no loop-detect
— med-out {number | igp-cost}
— no med-out
— min-as-origination seconds
— no min-as-origination
— min-route-advertisement seconds
— no min-route-advertisement
— multihop ttl-value
— no multihop
— [no] next-hop-self
— [no] passive
— peer-as as-number
— no peer-as
— preference preference
— no preference
— prefix-limit limit limit [log-only] [threshold percent]
  [idle-timeout { minutes | forever }]
— no prefix-limit
— [no] remove-private
— [no] shutdown
— ttl-security min-ttl-value
— no ttl-security
— type {internal | external}
— no type
— [no] updated-error-handling
OSPF Configuration Commands

```plaintext
config
  service
    vprn service-id [customer customer-id]
    no vprn service-id
      [no] ospf
      ospf3 [instance-id] [router-id]
      [no] ospf3 instance-id
        advertise-router-capability { link | area | as }
        no advertise-router-capability
        [no] area area-id
          area-range ip-prefix/mask [advertise | not-advertise]
          no area-range ip-prefix/mask
          [no] blackhole-aggregate
          [no] interface ip-int-name [secondary]
            [no] advertise-subnet
            authentication bidirectional sa-name
            authentication inbound sa-name outbound sa-name
            no authentication
            authentication-key [authentication-key | hash-key]
              [hash | hash2]
            no authentication-key
            authentication-type {password | message-digest}
            no authentication-type
            bfd-enable [remain-down-on-failure]
            no bfd-enable
            dead-interval seconds
            no dead-interval
            hello-interval seconds
            no hello-interval
            interface-type {broadcast | point-to-point}
            no interface-type
            lfa-policy-map route-nh-template template-name
            no lfa-policy-map
            [no] loopfree-alternate-exclude
            lsa-filter-out [all | except-own-rtrlsa | except-own-rtrlsa-and-defaults]
            [no] lsa-filter-out
            message-digest-key key-id md5 [key | hash-key]
              [hash | hash2]
            no message-digest-key key-id
            metric metric
            no metric
            mtu bytes
            no mtu
            [no] passive
            priority number
            no priority
            retransmit-interval seconds
            no retransmit-interval
            [no] shutdown
            transit-delay seconds
            no transit-delay
            key-rollover-interval key-rollover-interval
```
— [no] loopfree-alternate-exclude
— [no] nssa
  — area-range ip-prefix/mask [advertise | not-advertise]
  — no area-range ip-prefix/mask
  — originate-default-route [type-7]
  — no originate-default-route
  — [no] redistribute-external
  — [no] summaries
— [no] sham-link ip-int-name ip-address
  — authentication-key [authentication-key | hash-key]
    [hash | hash2]
  — no authentication-key
  — authentication-type {password | message-digest}
  — no authentication-type
  — dead-interval seconds
  — no dead-interval
  — hello-interval seconds
  — no hello-interval
  — message-digest-key key-id md5 [key | hash-key] [hash | hash2]
  — no message-digest-key key-id
  — metric metric
  — no metric
  — retransmit-interval seconds
  — no retransmit-interval
  — [no] shutdown
  — transit-delay seconds
  — no transit-delay
— [no] stub
  — default-metric metric
  — no default-metric
  — [no] summaries
— [no] virtual-link router-id transit-area area-id
  — authentication-key [authentication-key | hash-key]
    [hash | hash2]
  — no authentication-key
  — authentication-type {password | message-digest}
  — no authentication-type
  — dead-interval seconds
  — no dead-interval
  — hello-interval seconds
  — no hello-interval
  — message-digest-key key-id md5 [key | hash-key] [hash | hash2]
  — no message-digest-key key-id
  — retransmit-interval seconds
  — no retransmit-interval
  — [no] shutdown
  — transit-delay seconds
  — no transit-delay
— [no] compatible-rfc1583
— export policy-name [ policy-name ... (up to 5 max)]
— no export
— external-db-overflow limit seconds
— no external-db-overflow
— external-preference preference
— no external-preference
— [no] graceful-restart
    — [no] helper-disable
— [no] ignore-dn-bit
— [no] ignore-dn-bit
— [no] loopfree-alternate
— loopfree-alternate-exclude prefix-policy [prefix-policy... up to 5]
— no loopfree-alternate-exclude
— [no] multicast-import
— overload [timeout seconds]
— no overload
— [no] overload-include-ext-2
— [no] overload-include-stub
— overload-on-boot [timeout seconds]
— no overload-on-boot
— preference preference
— no preference
— reference-bandwidth bandwidth-in-kbps
— no reference-bandwidth
— router-id ip-address
— no router-id
— [no] shutdown
— [no] super-backbone
— [no] suppress-dn-bit
— timers
    — [no] lsa-arrival lsa-arrival-time
    — [no] lsa-generate max-lsa-wait [lsa-initial-wait [lsa-second-wait]]
    — [no] spf-wait max-spf-wait [spf-initial-wait [spf-second-wait]]
— [no] unicast-import-disable
— vpn-domain id {0005 | 0105 | 0205 | 8005}
— no vpn-domain
— vpn-tag vpn-tag
— no vpn-tag
PIM Configuration Commands

```
config
  — service
  — vprn [no] pim
    — apply-to {all | none}
    — import {join-policy | register-policy} [policy-name [.. policy-name]]
    — no import {join-policy | register-policy}
    — [no] interface ip-int-name
      — assert-period assert-period
      — no assert-period
      — [no] bfd-enable [ipv4 ipv6]
      — [no] bsm-check-rtr-alert
      — hello-interval hello-interval
      — no hello-interval
      — hello-multiplier deci-units
      — no hello-multiplier
      — [no] improved-assert
      — [no] instant-prune-echo
      — [no] ipv4-multicast-disable
      — [no] ipv6-multicast-disable
      — max-groups value
      — no max-groups
      — mcac
        — mc-constraints
          — level level-id bw bandwidth
          — no level
          — number-down number-lag-port-down
          — no number-down
          — [no] shutdown
          — policy policy-name
          — no policy
          — unconstrained-bw bandwidth mandatory-bw mandatory-bw
            — no unconstrained-bw
            — multicast-senders {auto | always | never}
            — no multicast-senders
            — priority dr-priority
            — no priority
            — [no] shutdown
            — sticky-dr [priority dr-priority]
            — no sticky-dr
            — three-way-hello [compatibility-mode]
            — no three-way-hello
            — [no] tracking-support
            — [no] ipv4-multicast-disable
            — [no] ipv6-multicast-disable
            — [no] mc-ecmp-balance
            — [no] mc-ecmp-balance-hold
            — [no] non-dr-attract-traffic
            — rp
              — auto-rp-discovery
```
— [no] anycast rp-ip-address
  — [no] rp-set-peer ip-address
— [no] auto-rp-discovery
— bootstrap-export policy-name [.. policy-name...up to five]
— no bootstrap-export
— bootstrap-import policy-name [.. policy-name...up to five]
— no bootstrap-import
— bsr-candidate
  — address ip-address
  — no address
  — hash-mask-len hash-mask-length
  — no hash-mask-len
  — priority bootstrap-priority
  — no priority
  — [no] shutdown
— ipv6
  — anycast ipv6-address
  — [no] rp-set-peer ipv6-address
— bsr-candidate ipv6-address
  — address ipv6-address
  — [no] address
  — hash-mask-length hash-mask-length
  — [no] hash-mask-length
  — priority bootstrap-priority
  — no priority
  — [no] shutdown
  — [no] embedded-rp
    — group-range grp-ipv6-address/prefix-length
    — [no] shutdown
— rp-candidate
  — address ipv6-address
  — no address
  — [no] group-range grp-ipv6-address/prefix-length
    — holdtime holdtime
    — no holdtime
    — priority priority
    — no priority
    — [no] shutdown
— static
  — [no] address ipv6-address
    — [no] group-prefix grp-ipv6-address/prefix-length
    — [no] override
— rp-candidate
  — address ip-address
  — no address
  — [no] group-range {grp-ip-address/mask | grp-ip-address {netmask}}
    — holdtime holdtime
    — no holdtime
    — priority priority
    — no priority
    — [no] shutdown
— static
  — [no] address ip-address
Virtual Private Routed Network Services

- \[\text{no}\] group-prefix \{grp-ip-address/mask | grp-ip-address netmask\}
- \[\text{no}\] override
- \[\text{no}\] rpf-table \{rtable-m | rtable-u | both\}
- \[\text{no}\] shutdown
- spt-switchover-threshold \{grp-ip-address/mask | grp-ip-address netmask\} spt-threshold
- \[\text{no}\] spt-switchover-threshold \{grp-ip-address/mask | grp-ip-address netmask\}
- ssm-assert-compatible-mode \{enable | disable\}
- ssm-default-range-disable ipv4
- \[\text{no}\] ssm-groups
  - \[\text{no}\] group-range \{grp-ip-address/mask | grp-ip-address netmask\}

C-Multicast Listener Discovery (MLD) Commands

```text
config
  service
    - \[\text{no}\] vprn
  \[\text{no}\] mld
    - \[\text{no}\] interface ip-int-name
      - \[\text{no}\] disable-router-alert-check
      - import policy-name
      - \[\text{no}\] import
      - max-groups value
      - \[\text{no}\] max-groups
      - query-interval seconds
      - \[\text{no}\] query-interval
      - query-last-member-interval seconds
      - \[\text{no}\] query-last-member-interval
      - query-response-interval seconds
      - \[\text{no}\] query-response-interval
      - \[\text{no}\] shutdown
      - static
        - \[\text{no}\] group grp-ipv6-address
          - source src-ipv6-address
          - \[\text{no}\] starg
        - version version
        - \[\text{no}\] version
      - query-interval seconds
      - \[\text{no}\] query-interval
      - query-last-member-interval seconds
      - \[\text{no}\] query-last-member-interval
      - query-response-interval seconds
      - \[\text{no}\] query-response-interval
      - robust-count robust-count
      - \[\text{no}\] robust-count
      - \[\text{no}\] shutdown
      - ssm-translate
        - \[\text{no}\] grp-range start end
```
— [no] source src-ipv6-address
Show Commands

show
  service
    egress-label start-label [end-label]
    ingress-label start-label [[end-label]
    id service-id
      all
      authentication
        statistics [policy name] [sap sap-id]
    arp [ip-address] [mac ieee-address] [sap port-id:encap] [interface ip-int-name]
    arp-host [wholesaler service-id] [sap sap-id] [interface interface-name] ip-address
      ip-address[/mask] [mac ieee-address] [port port-id] [no-inter-dest-id | inter-
      dest-id inter-dest-id]} [detail]
    arp-host statistics [sap sap-id] [interface interface-name]
    arp-host summary [interface interface-name]
    base
    sessions summary
    sessions [detail] wholesaler service-id
    interface [ip-address | ip-int-name] [detail]
    ptp
    retailers
    sap [sap-id [detail]]
    sdp [sdp-id | far-end ip-address] [detail]
    sap-using [sap sap-id]
    sap-using interface [ip-address | ip-int-name]
    sap-using ingress | egress atm-td-profile td-profile-id
    sap-using ingress | egress filter filter-id
    sap-using ingress | egress qos-policy qos-policy-id
    sap-using authentication-policy policy-name
    sdp-using [sdp-id | far-end ip-address] [detail | keep-alive-history]
    sdp-using [sdp-id] [vc-id]
    service-using [vprn] [sdp sdp-id] [customer customer-id]
show

- router [vprn-service-id]
  - aggregate [active]
  - arp [ip-address | ip-int-name | mac ieee-mac-address] [sdp sdp-id:vc-id] [summary]
  - bgp
    - damping [ip-prefix/mask | ip-address] [detail]
    - damping [damp-type] [detail]
    - group [name] [detail]
    - neighbor [ip-address [[family family] filter1]]
    - neighbor [as-number [[family family] filter2]]
    - paths
    - routes [family family] [prefix [detail | longer]]
    - routes [family family] [prefix [hunt | brief]]
    - routes [family family] [community comm-id]
    - routes [family family] [aspath-regex reg-ex1]
    - routes [family] [ipv6-prefix[/prefix-length] [detail | longer][hunt [brief]]]
  - summary [all]
- ecmp
- interface [{ip-address | ip-int-name} [detail] | summary | exclude-services]
- mvpn
- route-table [ip-address[/mask] [longer | best]] [protocol protocol] [summary]
- service-prefix
- static-arp [ip-address | ip-int-name | mac ieee-mac-address]
- static-route [ip-prefix /mask] [preference preference] [next-hop ip-address] [detail]
- tunnel-table [ip-address[/mask] [protocol protocol] [sdp sdp-id]
- tunnel-table [summary]
Clear Commands

**clear**

- **router**
  - **arp-host**
  - **arp-host** { mac ieee-address | sap sap-id | ip-address ip-address/[mask] }
  - **arp-host** [port port-id] [inter-dest-id intermediate-destination-id | no-inter-dest-id]
  - **arp-host statistics** { sap sap-id | interface interface-name }
- **bgp**
  - **damping** [{prefix/mask [neighbor ip-address]} | {group name}]
  - **flap-statistics** ([ip-prefix/mask] [neighbor ip-address]) | [group group-name] | [regex reg-exp] | [policy policy-name]
  - **neighbor** { ip-address | as as-number | external | all } [soft | soft-inbound | statistics]
  - **protocol**
  - **interface** { ip-int-name | ip-address } [icmp]

**clear**

- **service**
  - **id** service-id
    - **spoke-sdp** sdp-id:vc-id ingress-vc-label
  - **statistics**
    - **sap** sap-id [all | counters | stp]
    - **sdp** sdp-id keep-alive
    - **id** service-id
      - **counters**
      - **spoke-sdp** sdp-id:vc-id [all | counters | stp]
      - **spoke-sdp**
Debug Commands

debug
  — service
    — id service-id
      — [no] arp-host
      — [no] event-type {config-change | svc-oper-status-change | sap-oper-status-change | sdppbind-oper-status-change}
    — [no] host-connectivity-verify
      — [no] ip ip-address
      — [no] mac ieee-address
      — [no] sap sap-id
      — [no] sap sap-id
        — event-type {config-change | oper-status-change}
    — [no] sdp sdp-id:vc-id
        — event-type {config-change | oper-status-change}
    — stp
      — [no] all-events
      — [no] bpdu
      — [no] core-connectivity
      — [no] exception
      — [no] fsm-state-changes
      — [no] fsm-timers
      — [no] port-role
      — [no] port-state
      — [no] sap sap-id
      — [no] sdp sdp-id:vc-id

debug
  — router [router-instance]
    — igmp
      — [no] interface [ip-int-name | ip-address]
      — [no] mcs [ip-int-name]
      — [no] misc
      — [no] packet [query|v1-report|v2-report|v3-report|v2-leave] [ip-int-name|ip-address]
VPRN Service Configuration Commands

Generic Commands

shutdown

Syntax
[no] shutdown

Context
config>service>vprn

Description
This command administratively disables an entity. When disabled, an entity does not change, reset, or remove any configuration settings or statistics.

The operational state of the entity is disabled as well as the operational state of any entities contained within. Many objects must be shut down before they may be deleted.

Services are created in the administratively down (shutdown) state. When a no shutdown command is entered, the service becomes administratively up and then tries to enter the operationally up state. Default administrative states for services and service entities is described below in Special Cases.

The no form of this command places the entity into an administratively enabled state.

If the AS number was previously changed, the BGP AS number inherits the new value.

Special Cases:

Service Admin State — Bindings to an SDP within the service will be put into the out-of-service state when the service is shutdown. While the service is shutdown, all customer packets are dropped and counted as discards for billing and debugging purposes.

A service is regarded as operational providing that one IP Interface SAP and one SDP is operational.

VPRN BGP and RIP — This command disables the BGP or RIP instance on the given IP interface. Routes learned from a neighbor that is shutdown are immediately removed from the BGP or RIP database and RTM. If BGP or RIP is globally shutdown, then all RIP group and neighbor interfaces are shutdown operationally. If a BGP or RIP group is shutdown, all member neighbor interfaces are shutdown operationally. If a BGP or RIP neighbor is shutdown, just that neighbor interface is operationally shutdown.

description

Syntax
description description-string
no description

Context
config>service>vprn

Description
This command creates a text description stored in the configuration file for a configuration context.
The **description** command associates a text string with a configuration context to help identify the content in the configuration file.

The **no** form of this command removes the string from the configuration.

**Default**
No description associated with the configuration context.

**Parameters**

`string` — The description character string. Allowed values are any string up to 80 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.
Global Commands

vprn

Syntax:  
  vprn service-id [customer customer-id] [create]  
  no vprn service-id

Context:  
  config>service

Description:  
This command creates or edits a Virtual Private Routed Network (VPRN) service instance.  
If the service-id does not exist, a context for the service is created. If the service-id exists, the context for editing the service is entered.  
VPRN services allow the creation of customer-facing IP interfaces in the same routing instance used for service network core routing connectivity. VPRN services require that the IP addressing scheme used by the subscriber must be unique between it and other addressing schemes used by the provider and potentially the entire Internet.  
IP interfaces defined within the context of an VPRN service ID must have a SAP created as the access point to the subscriber network.  
When a service is created, the customer keyword and customer-id must be specified and associates the service with a customer. The customer-id must already exist having been created using the customer command in the service context. When a service is created with a customer association, it is not possible to edit the customer association. The service must be deleted and re-created with a new customer association.  
When a service is created, the use of the customer customer-id is optional to navigate into the service configuration context. If attempting to edit a service with the incorrect customer-id results in an error.  
Multiple VPRN services are created to separate customer-owned IP interfaces. More than one VPRN service can be created for a single customer ID. More than one IP interface can be created within a single VPRN service ID. All IP interfaces created within an VPRN service ID belongs to the same customer.  
The no form of the command deletes the VPRN service instance with the specified service-id. The service cannot be deleted until all the IP interfaces and all routing protocol configurations defined within the service ID have been shutdown and deleted.

Default:  
None — No VPRN service instances exist until they are explicitly created.

Parameters:  
  service-id — The unique service identification number identifying the service in the service domain. This ID must be unique to this service and may not be used for any other service of any type. The service-id must be the same number used for every 7750 SR and 7710 SR on which this service is defined.

Values:  
  service-id: 1 — 2147483648  
  svc-name: 64 characters maximum

customer customer-id — Specifies an existing customer identification number to be associated with the service. This parameter is required on service creation and optional for service editing or deleting.
aggregate

**Syntax**

```
aggregate ip-prefix/ip-prefix-length [summary-only] [as-set] [aggregator as-number: ip-address] [community comm-id] [black-hole | indirect ip-address]
```

**Context**

```
config>service>vprn
```

**Description**

This command creates an aggregate route.

Use this command to automatically install an aggregate in the routing table when there are one or more component routes. A component route is any route used for forwarding that is a more-specific match of the aggregate.

The use of aggregate routes can reduce the number of routes that need to be advertised to neighbor routers, leading to smaller routing table sizes.

Overlapping aggregate routes may be configured; in this case a route becomes a component of only the one aggregate route with the longest prefix match. For example if one aggregate is configured as 10.0.0.0/16 and another as 10.0.0.0/24, then route 10.0.128/17 would be aggregated into 10.0.0.0/16, and route 10.0.0.128/25 would be aggregated into 10.0.0.0/24. If multiple entries are made with the same prefix and the same mask the previous entry is overwritten.

A standard 4-byte BGP community may be associated with an aggregate route in order to facilitate route policy matching.

By default aggregate routes are not installed in the forwarding table, however there are configuration options that allow an aggregate route to be installed with a black-hole next hop or with an indirect IP address as next hop.

The **no** form of the command removes the aggregate.

**Default**

No aggregate routes are defined.

**Parameters**

- `ip-prefix` — The destination address of the aggregate route in dotted decimal notation.
  - **Values**
    - `ipv4-prefix`  `a.b.c.d` (host bits must be 0)
    - `ipv4-prefix-length`  `0 — 32`
    - `ipv6-prefix`  `x:x:x:x:x:x:x:x` (eight 16-bit pieces)
      - `x:x:x:x:x:d.d.d`  `x:`  `[0 — FFFF]H`
      - `d:`  `[0 — 255]D`
    - `ipv6-prefix-length`  `0 — 128`

  The mask associated with the network address expressed as a mask length.
  - **Values**
    - `0 — 32`

- `summary-only` — This optional parameter suppresses advertisement of more specific component routes for the aggregate.

  To remove the `summary-only` option, enter the same aggregate command without the `summary-only` parameter.
as-set — This optional parameter is only applicable to BGP and creates an aggregate where the path advertised for this route will be an AS_SET consisting of all elements contained in all paths that are being summarized. Use this feature carefully as it can increase the amount of route churn due to best path changes.

aggregator as-number:ip-address — This optional parameter specifies the BGP aggregator path attribute to the aggregate route. When configuring the aggregator, a two-octet AS number used to form the aggregate route must be entered, followed by the IP address of the BGP system that created the aggregate route.

community comm-id — This configuration option associates a BGP community with the aggregate route. The community can be matched in route policies and is automatically added to BGP routes exported from the aggregate route.

Values

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>comm-id</td>
<td>Associated BGP community</td>
</tr>
<tr>
<td>asn, comm-val</td>
<td>Community identifier range</td>
</tr>
<tr>
<td>well-known-comm</td>
<td>Community values</td>
</tr>
<tr>
<td>no-advertise, no-export, no-export-subconfed</td>
<td>Community action</td>
</tr>
</tbody>
</table>

black-hole — This optional parameter installs the aggregate route, when activated, in the FIB with a black-hole next-hop; where packets matching this route are discarded.

indirect ip-address — This configuration option specifies that the aggregate route should be installed in the FIB with a next-hop taken from the route used to forward packets to ip-address.

Values

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv4-prefix</td>
<td>IPv4 prefix</td>
</tr>
<tr>
<td>ipv6-prefix</td>
<td>IPv6 prefix</td>
</tr>
<tr>
<td>a.b.c.d</td>
<td>IPv4 address</td>
</tr>
<tr>
<td>x:x:x:x:x:x:x:x</td>
<td>IPv6 address</td>
</tr>
<tr>
<td>d: [0 — 255]D</td>
<td>IPv6 address</td>
</tr>
</tbody>
</table>

auto-bind

Syntax auto-bind {ldp | gre | rsvp-te | mpls}
no auto-bind

Context config>service>vprn

Description This command specifies the automatic binding type for the SDP assigned to this service.

Default None — The auto-bind type must be explicitly specified.

Parameters ldp — Specifies LDP to be the automatic binding for the SDP assigned to the service.
gre — Specifies GRE to be the automatic binding for the SDP assigned to the service.
rsvp-te — Specifies RSVP-TE to be the automatic binding for the SDP assigned to the service
mpls — Specifies that both LDP and RSVP-TE can be used to resolve the BGP nexthop for VPRN routes in an associated VPRN instance.

autonomous-system
Global Commands

**Syntax**
autonomous-system *as-number*

no autonomous-system

**Context**
config>service>vprn

**Description**
This command defines the autonomous system (AS) to be used by this VPN routing/forwarding (VRF). This command defines the autonomous system to be used by this VPN routing context.

The **no** form of the command removes the defined AS from this VPRN context.

**Default**
no autonomous-system

**Parameters**
*as-number* — Specifies the AS number for the VPRN service.

**Values**
1 — 4294967295

**backup-path**

**Syntax**
backup-path [ipv4] [ipv6]

no backup-path [ipv4] [ipv6]

**Context**
config>router

config>service>vprn

**Description**
This command enables the computation and use of a backup path for IPv4 and/or IPv6 BGP-learned prefixes belonging to the base router or a particular VPRN. Multiple paths must be received for a prefix in order to take advantage of this feature. When a prefix has a backup path and its primary path(s) fail the affected traffic is rapidly diverted to the backup path without waiting for control plane re-convergence to occur. When many prefixes share the same primary path(s), and in some cases also the same backup path, the time to failover traffic to the backup path is independent of the number of prefixes. In some cases prefix independent convergence may require use of FP2 or later IOMs/IMMs/XMAs.

By default, IPv4 and IPv6 prefixes do not have a backup path installed in the IOM.

**Default**
no backup-path

**Parameters**
ipv4 — Enables the use of a backup path for BGP-learned IPv4 prefixes

ipv6 — Enables the use of a backup path for BGP-learned IPv6 prefixes

**carrier-carrier-vpn**

**Syntax**
[no] carrier-carrier-vpn

**Context**
config>service>vprn

**Description**
This command configures a VPRN service to support a Carrier Supporting Carrier model. It should be configured on a network provider’s CSC-PE device.

This command cannot be applied to a VPRN unless it has no SAP or spoke-SDP interfaces. Once this command has been entered one or more MPLS-capable CSC interfaces can be created in the VPRN.

The **no** form of the command removes the Carrier Supporting Carrier capability from a VPRN.
confederation

Syntax

confederation confed-as-num members as-number [as-number...(up to 15 max)]
no confederation confed-as-num members as-number [as-number...(up to 15 max)]
no confederation

Context

config>service>vprn

Description

This command configures the VPRN BGP instance to participate in a BGP confederation. BGP
confederations can be used to reduce the number of IBGP sessions required within an AS.
When a VPRN BGP instance is part of a confederation, it can form confederation-EBGP sessions
with CE router peers in a different sub-autonomous systems of the same confederation as well as
regular EBGP sessions with CE router peers outside the confederation. A VPRN BGP instance that is
part of a confederation cannot import or export its routes to the base router instance (as VPN-IP
routes).
The no form of the command deletes the specified member AS from the confederation. When
members are not specified in the no statement, the entire list is removed and confederations is
disabled. When the last member of the list is removed, confederations is disabled.

Default

No confederations are defined.

Parameters

confed-as-num — The confederation AS number defined as a decimal value.

Values

1 — 4294967295

members as-number — The AS number(s) that are members of the confederation, each expressed as
a decimal integer. Configure up to 15 members per confed-as-num.

Values

1 — 4294967295

dns

Syntax

[no] dns

Context

config>service>vprn

Description

This command enables the context to configure domain name servers.
The no form of the command disables DNS for this service.

ipv4-source-address

Syntax

ipv4-source-address ipv4-address
no ipv4-source-address

Context

config>service>vprn>dns
Global Commands

### Description
This command configures the IPv4 address of the default secondary DNS server for the subscribers using this interface. Subscribers that cannot obtain an IPv4 DNS server address by other means, can use this for DNS name resolution.

The ipv4-address value can only be set to a nonzero value if the value of VPRN type is set to `subscriber-split-horizon`.

The **no** form of the command reverts to the default.

**Default**
none

**Parameters**
- `ipv4-address` — Specifies the IPv4 address of the default secondary DNS server.
  - **Values**
    - ipv4-address - a.b.c.d

### ipv6-source-address

**Syntax**
`ipv6-source-address ipv6-address`

**Context**
`config>service>vprn>dns`

**Description**
This command configures the IPv6 address of the default secondary DNS server for the subscribers using this interface. Subscribers that cannot obtain an IPv6 DNS server address by other means, can use this for DNS name resolution.

The ipv6-address value can only be set to a nonzero value if the value of VPRN type is set to `subscriber-split-horizon`.

The **no** form of the command reverts to the default.

**Default**
none

**Parameters**
- `ipv4-address` — Specifies the IPv6 address of the default secondary DNS server.
  - **Values**
    - ipv4-address - a.b.c.d

### primary-dns

**Syntax**
`primary-dns ip-address`

**Context**
`config>service>vprn>dns`

**Description**
This command configures the primary DNS server used for DNS name resolution. DNS name resolution can be used when executing ping, traceroute, and service-ping, and also when defining file URLs. DNS name resolution is not supported when DNS names are embedded in configuration files.

The **no** form of the command removes the primary DNS server from the configuration.

**Default**
no primary-dns — No primary DNS server is configured.
Parameters  
\textit{ip-address} — The IP or IPv6 address of the primary DNS server.

Values  
- \textit{ipv4-address} - a.b.c.d
- \textit{ipv6-address}: x:x:x:x:x:interface
  x:x:x:x:d.d.d.[interface]
  x: [0..FFFF]H
  d: [0..255]D

interface - 32 chars max, for link local addresses.

---

**secondary-dns**

Syntax  
\texttt{secondary-dns} \textit{ip-address}
\texttt{no secondary-dns}

Context  
config>service>vprn>dns

Description  
This command configures the secondary DNS server for DNS name resolution. The secondary DNS server is used only if the primary DNS server does not respond.

DNS name resolution can be used when executing ping, traceroute, and service-ping, and also when defining file URLs. DNS name resolution is not supported when DNS names are embedded in configuration files.

The \texttt{no} form of the command removes the secondary DNS server from the configuration.

Default  
\texttt{no secondary-dns} — No secondary DNS server is configured.

Parameters  
\textit{ip-address} — The IP or IPv6 address of the secondary DNS server.

Values  
- \textit{ipv4-address} - a.b.c.d
- \textit{ipv6-address}: x:x:x:x:x:interface
  x:x:x:x:d.d.d.[interface]
  x: [0..FFFF]H
  d: [0..255]D

interface - 32 chars max, for link local addresses.

---

**tertiary-dns**

Syntax  
\texttt{tertiary-dns} \textit{ip-address}
\texttt{no tertiary-dns}

Context  
config>service>vprn>dns

Description  
This command configures the tertiary DNS server for DNS name resolution. The tertiary DNS server is used only if the primary DNS server and the secondary DNS server do not respond.

DNS name resolution can be used when executing ping, traceroute, and service-ping, and also when defining file URLs. DNS name resolution is not supported when DNS names are embedded in configuration files.

The \texttt{no} form of the command removes the tertiary DNS server from the configuration.

Default  
\texttt{no tertiary-dns} — No tertiary DNS server is configured.
**Global Commands**

### Parameters

**ip-address** — The IP or IPv6 address of the tertiary DNS server.

### Values

- **ipv4-address** - a.b.c.d
- **ipv6-address**:
  - x:x:x:x[x[-interface]]
  - x:x:x:x:d.d.d.d[-interface]
  - x: [0..FFFF]H
  - d: [0..255]D
  - interface - 32 chars max, for link local addresses

---

**ecmp**

**Syntax**

```plaintext
ecmp max-ecmp-routes
no ecmp
```

**Context**

```
config>service>vprn
```

**Description**

This command enables equal-cost multipath (ECMP) and configures the number of routes for path sharing. For example, the value of 2 means that 2 equal cost routes will be used for cost sharing.

ECMP groups form when the system routes to the same destination with equal cost values. Routing table entries can be entered manually (as static routes), or they can be formed when neighbors are discovered and routing table information is exchanged by routing protocols. The system can balance traffic across the groups with equal costs.

ECMP can only be used for routes learned with the same preference and same protocol. See the discussion on preferences in the `static-route` command.

When more ECMP routes are available at the best preference than configured by the `max-ecmp-routes` parameter, then the lowest next-hop IP address algorithm is used to select the number of routes configured.

The `no` form of the command disables ECMP path sharing. If ECMP is disabled and multiple routes are available at the best preference and equal cost, the newly updated route is used.

**Default**

`no ecmp`

**Parameters**

- **max-ecmp-routes** — Specifies the maximum number of routes for path sharing.
  - **Values**
    - 0 — 32

---

**enable-bgp-vpn-backup**

**Syntax**

```plaintext
enable-bgp-vpn-backup [ipv4] [ipv6]
no enable-bgp-vpn-backup
```

**Context**

```
config>service>vprn>bgp
```

**Description**

This command allows BGP-VPN routes imported into the VPRN to be used as backup paths for IPv4 and/or IPv6 BGP-learned prefixes.

**Parameters**

- **ipv4** — Allows BGP-VPN routes to be used as backup paths for IPv4 prefixes.
- **ipv6** — Allows BGP-VPN routes to be used as backup paths for IPv6 prefixes.
grt-lookup

Syntax
grt-lookup

Context
config>service>vprn

Description
This command provides the context under which all Global Route Table (GRT) leaking commands are configured. If all the supporting commands in the context are removed, this command will also be removed.

enable-grt

Syntax
[no] enable-grt

Context
config>service>vprn>grt-lookup

Description
This command enables the functions required for looking up routes in the Global Route Table (GRT) when the lookup in the local VRF fails. If this command is enabled without the use of a static-route option (as subcommand to this parent), a lookup in the local VRF is preferred over the GRT. When the local VRF returns no route table lookup matches, the result from the GRT is preferred.

The no form of this command disables the lookup in the GRT when the lookup in the local VRF fails.

Default
no enable-grt

export-grt

Syntax
export-grt policy-name [policy-name ...(up to 5 max)]
no export-grt

Context
config>service>vprn>grt-lookup

Description
This command uses route policy to determine which routes are exported from the VRF to the GRT along with all the forwarding information. These entries will be marked as BGP-VPN routes in the GRT. Routes must be in the GRT in order for proper routing to occur from the GRT to the VRF.

Default
no export-grt

export-limit

Syntax
export-limit num-routes
no export-limit

Context
config>service>vprn>grt-lookup
cfg>service>vprn>ospf
cfg>service>vprn>ospf3

Description
This command provides the ability to limit the total number of routes exported from the VRF to the GRT. The value zero (0) provides an override that disables the maximum limit. Setting this value to
Global Commands

zero (0) will not limit the number of routes exported from the VRF to the GRT. Configuring a range of one (1) to 1000 will limit the number of routes to the specified value.

The no form of the command sets the export-limit to a default of five (5).

Default export-limit 5

Parameters num-routes — Specifies maximum number of routes that can be exported.

Values 0 — 1000

export-v6-limit

Syntax export-v6-limit num-routes
no export-v6-limit

Context config>service>vprn>grt-lookup

Description The export-limit range provides the ability to limit the total number of IPv6 routes exported from the VPRN to the GRT. The value “0” provides an override that disables the maximum limit. Setting this value to “0” will not limit the number of routes exported from the VPRN to the GRT. Configuring a range of 1-1000 will limit the number of routes to the specified value.

The no form of the command sets the export-limit to a default of 5.

Default export-v6-limit 5

Parameters num-routes — Specifies maximum number of routes that can be exported.

Values 0 — 1000

allow-local-management

Syntax [no] allow-local-management

Context config>service>vprn>grt-lookup>enable-grt

Description When enabled, both IPv4 and IPv6 base interfaces shall respond to leaked traffic from the VPRN.

static-route

Syntax static-route \{ip-prefix/prefix-length | ip-prefix netmask\} [preference preference] [metric metric] [enable|disable] grt
no static-route

Context config>service>vprn>grt-lookup>enable-grt

Description This command is a simplified version of the traditional static-route command pointing to the base routing instance. This instructs the route lookup function to look only in the GRT for a route matching destination static route and not look up the route in the local VPRN. The GRT keyword is a required parameter.
The no form causes the feature into the default mode of primary lookup for all routes in the local VPRN and failing a match in the local VPRN, the lookup result in the GRT will be used.

**Parameters**

*ip-prefix/prefix-length* — Specifies the IPv4 prefix and prefix length.

**Values**

- **ip-prefix**: a.b.c.d (host bits must be 0)
- **ipv4-prefix-length**: [0..32]
- **ipv6-prefix x:x:x:x:x:x:x (eight 16-bit pieces)**
- **x:x:x:x:d.d.d**
- **x**: [0 — FFFF]H
- **d**: [0 — 255]D
- **ipv6-prefix-length**: 0 — 128

*netmask* — Specifies the netmask.

**Values**

- **a.b.c.d (network bits all 1 and host bits all 0)**

*preference* — Specifies the preference.

**Values**

- **1..255**

*metric* — Specifies the metric.

**Values**

- **0..65535**

*enable|disable* — Keyword; specifies the state of the static-route.

*grt* — Keyword; Global Route Table lookup.
IGMP Commands

igmp

Syntax       [no] igmp
Context      config>service>vprn
Description  This command enables the context to configure IGMP parameters.
             The no form of the command disables IGMP.
Default      disabled

group-interface

Syntax       [no] group-interface ip-int-name
             [no] group-interface fwd-service service-id ip-int-name
Context      config>service>vprn>igmp
Description  This command configures IGMP group interfaces.
             The no form of the command reverts to the default.
Default      none
Parameters   ip-int-name — Specifies the name of the IP interface. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.
             fwd-service service-id — Specifies the service ID. This is only configured in the retailer VRF. This construct references the wholesaler service under which the group-interface (and the subscriber) is actually defined.
             Values  1 — 2147483650, svc-name up to 64 char maximum
Default      none

disable-router-alert-check

Syntax       [no] disable-router-alert-check
Context      config>service>vprn>igmp>gr-if
             config>service>vprn>igmp>if
Description  This command enables the IGMP router alert check option.
             The no form of the command disables the router alert check.
import

Syntax

import policy-name
no import

Context

config>service>vprn>igmp>gr-if
config>service>vprn>igmp>if

Description

This command specifies the policy that is to be applied on this interface.

Parameters

policy-name — Specify the policy to filter IGMP packets.

max-groups

Syntax

max-groups value
no max-groups

Context

config>service>vprn>igmp>gr-if
config>service>vprn>igmp>if

Description

This command configures the maximum number of groups for which IGMP can have local receiver information based on received IGMP reports on this interface. When this configuration is changed dynamically to a value lower than currently accepted number of groups, the groups that are already accepted are not deleted. Only new groups will not be allowed.

The no form of the command removes the value.

Parameters

value — Specifies the maximum number of groups for this interface.

Values

1 — 16000

max-sources

Syntax

max-sources [1..1000]
no max-sources

Context

config>service>vprn>igmp>gr-if
config>service>vprn>igmp>if

Description

This command specifies the maximum number of sources for which IGMP can have local receiver information based on received IGMP reports on this interface. When this configuration is changed dynamically to a value lower than currently accepted number of sources, the sources that are already accepted are not deleted. Only new sources will not be allowed.

Parameters

sources — Specifies the maximum number of sources for this interface.

Values

1 — 1000
Global Commands

max-grp-sources

Syntax max-grp-sources [1..32000]
no max-grp-sources

Context config>service>vprn>igmp>gr-if
       config>service>vprn>igmp>if

Description This command configures the maximum number of group sources for which IGMP can have local
receiver information based on received IGMP reports on this interface. When this configuration is
changed dynamically to a value lower than currently accepted number of group sources, the group
sources that are already accepted are not deleted. Only new group sources will not be allowed.
The no form of the command reverts to the default.

Default 0

Parameters 1 — 32000 — Specifies the maximum number of group source.

Values 1 — 32000

mcac

Syntax mcac

Context config>service>vprn>igmp>gr-if

Description This command enables the context to configure multicast CAC parameters.

mc-constraints

Syntax mc-constraints

Context config>service>vprn>igmp>gr-if

Description This command configures multicast CAC constraints.

policy

Syntax policy policy-name
no policy

Context config>service>vprn>igmp>gr-if

Description This command references the global channel bandwidth definition policy that is used for (H)mcac
and HQoS Adjust.
HQoS Adjustment is supported only with redirection enabled. In other words, the policy from the
redirected interface is used for HQoS Adjustment.
Hierarchical mcac (Hmcac) is supported only with redirection enabled. In Hmcac, the subscriber is checked first against its bandwidth limits followed by the check on the redirected interface against the bandwidth limits defined under the redirected interface. In the Hmcac case the channel definition policy must be referenced under the redirected interface level.

Parameters

policy-name — Specifies the name of the global mcac channel definition policy defined under the hierarchy configure>router>mcac>policy.

Default
No policy is referenced.

**unconstrained-bw**

Syntax

unconstrained-bw bandwidth mandatory-bw mandatory-bw
no unconstrained-bw

Context
config>service>vprn>igmp>gr-if

Description
This command configures unconstrained-bw for multicast cac policy on this interface.

The **no** form of the command

Parameters

bandwidth — Specifies the bandwidth assigned for interface's multicast cac policy traffic in kilo-bits per second (kbps).

mandatory-bw mandatory-bw —

**query-src-ip**

Syntax

query-src-ip ip-address
no query-src-ip

Context
config>service>vprn>igmp>gr-if

Description
This command configures the query source IP address for the group interface. This IP address overrides the source IP address configured at the router level.

The **no** form of the command removes the IP address.

Default
none

Parameters

ip-address — Sets the source IPv4 address for all subscriber’s IGMP queries.

**sub-hosts-only**

Syntax

[no] sub-hosts-only

Context
config>service>vprn>igmp>gr-if

Description
This command enables the IGMP traffic from known hosts only.

The **no** form of the command disable the IGMP traffic from known hosts only
subnet-check

Syntax  [no] subnet-check
Context  config>service>vprn>igmp>gr-if
Description  This command enables local subnet checking for IGMP.
The no form of the command disables local subnet checking for IGMP.

version

Syntax  version version
        no version
Context  config>service>vprn>igmp>gr-if
Description  This command configures the version of IGMP.
The no form of the command

Parameters  version — Specifies the IGMP version.
Values  1, 2 or 3

grp-if-query-src-ip

Syntax  grp-if-query-src-ip ip-address
        no grp-if-query-src-ip
Context  config>service>vprn>igmp
Description  This command configures the query source IP address for all group interfaces.
The no form of the command removes the IP address.
Default  none

interface

Syntax  interface ip-int-name
        no interface
Context  config>service>vprn>igmp
Description  This command enables the context to configure IGMP interface parameters.
Parameters  ip-int-name — Specifies the name of the IP interface. Interface names can be from 1 to 32
            alphanumeric characters. If the string contains special characters (#, $, spaces, etc.), the entire
            string must be enclosed within double quotes.
import

Syntax
import policy-name
no import

Context
config>service>vprn>igmp>if

Description
This command imports a policy to filter IGMP packets. The no form of the command removes the policy association from the IGMP instance.

Default
no import — No import policy specified.

Parameters
policy-name — The import route policy name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

The specified name(s) must already be defined.

max-groups

Syntax
max-groups value
no max-groups

Context
config>service>vprn>igmp>if

Description
This command specifies the maximum number of groups for which IGMP can have local receiver information based on received IGMP reports on this interface. When this configuration is changed dynamically to a value lower than the currently accepted number of groups, the groups that are already accepted are not deleted. Only new groups will not be allowed.

Default
0, no limit to the number of groups.

Parameters
value — Specifies the maximum number of groups for this interface.

Values
1 — 16000

mcac

Syntax
mcac

Context
config>service>vprn>if
cfg>service>vprn>pim>if

Description
This command configures multicast CAC policy and constraints for this interface.

Default
none
mc-constraints

Syntax  mc-constraints

Context  config>service>vprn>igmp>if>mcac
         config>service>vprn>pim>if>mcac

Description  This command enables the context to configure multicast CAC constraints.

Default  none

level

Syntax  level level-id bw bandwidth
       no level level-id

Context  config>service>vprn>igmp>if>mcac
         config>service>vprn>pim>if>mcac

Description  This command configures interface levels and associated bandwidth for multicast CAC policy.

Parameters  level-id — Specifies an entry for the multicast CAC policy constraint level configured on this system.

   Values  1 — 8

bandwidth — Specifies the bandwidth in kilobits per second (kbps) for the level.

   Values  1 — 2147483647

number-down

Syntax  number-down number-lag-port-down
       no number-down

Context  config>service>vprn>igmp>if>mcac>mc-constraints
         config>service>vprn>pim>if>mcac>mc-constraints

Description  This command configures the number of ports down and level for interface’s multicast CAC policy.

Default  not enabled

Parameters  number-lag-port-down — If the number of ports available in the LAG is reduced by the number of ports configured in this command here then bandwidth allowed for bundle and/or interface will be as per the levels configured in this context.

   Values  1 — 64 (for 64-link LAG)
          1 — 32 (for other LAGs)

policy
**Syntax**  
`policy policy-name`  
`no policy`

**Context**  
`config>service>vprn>igmp>if>mcac`  
`config>service>vprn>pim>if>mcac`

**Description**  
This command configures the multicast CAC policy name.

**Parameters**  
`policy-name` — The multicast CAC policy name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

---

**unconstrained-bw**

**Syntax**  
`unconstrained-bw bandwidth mandatory-bw mandatory-bw`  
`no unconstrained-bw`

**Context**  
`config>service>vprn>igmp>if>mcac`  
`config>service>vprn>pim>if>mcac`

**Description**  
This command configures the bandwidth for the interface's multicast CAC policy traffic. When disabled (`no unconstrained-bw`) there will be no checking of bandwidth constraints on the interface level. When enabled and a policy is defined, enforcement is performed. The allocated bandwidth for optional channels should not exceed the `unconstrained-bw` minus the `mandatory-bw` and the mandatory channels have to stay below the specified value for the `mandatory-bw`. After this interface check, the bundle checks are performed.

**Parameters**  
`bandwidth` — The bandwidth assigned for interface's MCAC policy traffic, in kilo-bits per second (kbps).

**Values**  
0 — 2147483647

`mandatory-bw` — Specifies the bandwidth pre-reserved for all the mandatory channels on a given interface in kilo-bits per second (kbps).

If the `bandwidth` value is 0, no mandatory channels are allowed. If `bandwidth` is not configured, then all mandatory and optional channels are allowed.

If the value of `mandatory-bw` is equal to the value of `bandwidth`, then all the unconstrained bandwidth on a given interface is allocated to mandatory channels configured through multicast CAC policy on that interface and no optional groups (channels) are allowed.

The value of `mandatory-bw` should always be less than or equal to that of `bandwidth`. An attempt to set the value of `mandatory-bw` greater than that of `bandwidth`, will result in inconsistent value error.

**Values**  
0 — 2147483647

---

**static**

**Syntax**  
`static`
Global Commands

Context  config>service>vprn>igmp>if
Description  This command tests forwarding on an interface without a receiver host. When enabled, data is forwarded to an interface without receiving membership reports from host members.
Default  none

group

Syntax  [no] group grp-ip-address
Context  config>service>vprn>igmp>if>static
Description  This command adds a static multicast group either as a (*,G) or one or more (S,G) records. Use IGMP static group memberships to test multicast forwarding without a receiver host. When IGMP static groups are enabled, data is forwarded to an interface without receiving membership reports from host members.
When static IGMP group entries on point-to-point links that connect routers to a rendezvous point (RP) are configured, the static IGMP group entries do not generate join messages toward the RP.
Default  none
Parameters  grp-ip-address — Specifies an IGMP multicast group address that receives data on an interface. The IP address must be unique for each static group. The address must be in dotted decimal notation

source

Syntax  source
Context  config>service>vprn>igmp>if>static>group
Description  This command specifies a IPv4 unicast address that sends data on an interface. This enables a multicast receiver host to signal a router the group is to receive multicast traffic from, and from the source(s) that the traffic is expected.
The source command is mutually exclusive with the specification of individual sources for the same group.
The source command in combination with the group is used to create a specific (S,G) static group entry.
Use the no form of the command to remove the source from the configuration.
Default  none
Parameters  ip-address — Specifies the IPv4 unicast address.

starg

Syntax  starg
### Context
config>service>vprn>igmp>if>static>group

### Description
This command adds a static (*,G) entry. This command can only be enabled if no existing source addresses for this group are specified.

Use the `no` form of the command to remove the starg entry from the configuration.

**Default**
none

### subnet-check

**Syntax**

```
[no] subnet-check
```

**Context**
config>service>vprn>igmp>if

**Description**
This command enables subnet checking for IGMP messages received on this interface. All IGMP packets with a source address that is not in the local subnet are dropped.

**Default**
enabled

### version

**Syntax**

```
version version
no version
```

**Context**
config>service>vprn>igmp>if

**Description**
This command specifies the IGMP version. If routers run different versions of IGMP, they will negotiate the lowest common version of IGMP that is supported by hosts on their subnet and operate in that version. For IGMP to function correctly, all routers on a LAN should be configured to run the same version of IGMP on that LAN.

For IGMPv3, note that a multicast router that is also a group member performs both parts of IGMPv3, receiving and responding to its own IGMP message transmissions as well as those of its neighbors.

**Default**
3

**Parameters**

- `version` — Specifies the IGMP version number.
  - **Values**
    - 1, 2, 3

### query-interval

**Syntax**

```
query-interval seconds
no query-interval
```

**Context**
config>service>vprn>igmp

**Description**
This command specifies the frequency that the querier router transmits general host-query messages. The host-query messages solicit group membership information and are sent to the all-systems multicast group address, 224.0.0.1.
Global Commands

**Default**

125

**Parameters**

- **seconds** — The time frequency, in seconds, that the router transmits general host-query messages.
  
  **Values**
  
  2 — 1024

**query-last-member-interval**

**Syntax**

`query-last-member-interval seconds`

**Context**

`config>service>vprn>igmp`

**Description**

This command configures the frequency at which the querier sends group-specific query messages including messages sent in response to leave-group messages. The lower the interval, the faster the detection of the loss of the last member of a group.

**Default**

1

**Parameters**

- **seconds** — Specifies the frequency, in seconds, at which query messages are sent.
  
  **Values**
  
  1 — 1024

**query-response-interval**

**Syntax**

`query-response-interval seconds`

**Context**

`config>service>vprn>igmp`

**Description**

This command specifies how long the querier router waits to receive a response to a host-query message from a host.

**Default**

10

**Parameters**

- **seconds** — Specifies the time length of time to wait to receive a response to the host-query message from the host.
  
  **Values**
  
  1 — 1023

**robust-count**

**Syntax**

`robust-count robust-count`

`no robust-count`

**Context**

`config>service>vprn>igmp`

**Description**

This command configures the robust count. The robust-count variable allows tuning for the expected packet loss on a subnet. If a subnet anticipates losses, the robust-count variable can be increased.

**Default**

2
Parameters

**robust-count** — Specifies the robust count value.

**Values**

2 — 10

### ssm-translate

**Syntax**

```plaintext
igmp
```

**Context**

`config>service>vprn>igmp`

`config>service>vprn>igmp>if`

**Description**

This command enables the context to configure group ranges which are translated to SSM (S,G) entries. If the static entry needs to be created, it has to be translated from an IGMPv1 IGMPv2 request to a Source Specific Multicast (SSM) join. An SSM translate source can only be added if the starg command is not enabled. An error message is generated if you try to configure the `source` command with `starg` command enabled.

### grp-range

**Syntax**

```plaintext
[no] grp-range start end
```

**Context**

`config>service>vprn>igmp>ssm-translate`

**Description**

This command is used to configure group ranges which are translated to SSM (S,G) entries.

**Parameters**

- **start** — An IP address that specifies the start of the group range.
- **end** — An IP address that specifies the end of the group range. This value should always be greater than or equal to the value of the `start` value.

### source

**Syntax**

```plaintext
[no] source ip-address
```

**Context**

`config>service>vprn>igmp>ssm-translate>grp-range`

**Description**

This command specifies the source IP address for the group range. Whenever a (*,G) report is received in the range specified by `grp-range start` and `end` parameters, it is translated to an (S,G) report with the value of this object as the source address.

**Parameters**

- **ip-address** — Specifies the IP address that will be sending data.

### igmp-host-tracking

**Syntax**

```plaintext
igmp-host-tracking
```

**Context**

`config>service>vprn`

`config>service>vprn>sap`
Global Commands

**Description**
This command enables the context to configure IGMP host tracking parameters.

### expiry-time

**Syntax**
expiry-time expiry-time
go expiry-time

**Context**
config>service>vprn>igmp-trk
config>service>vprn>sap>igmp-trk

**Description**
This command configures the time that the system continues to track inactive hosts. The no form of the command removes the values from the configuration.

**Default**
no expiry-time

**Parameters**
expiry-time — Specifies the time, in seconds, that this system continues to track an inactive host.

- **Values**
  - 1 — 65535

### import

**Syntax**
import policy-name
no import

**Context**
config>service>vprn>sap>igmp-trk

**Description**
This command associates an import policy to filter IGMP packets. The no form of the command removes the values from the configuration.

**Default**
no import

**Parameters**
policy-name — Specifies the import policy name.

### max-num-groups

**Syntax**
max-num-groups max-num-groups
no max-num-groups

**Context**
config>service>vprn>sap>igmp-trk

**Description**
This command configures the maximum number of multicast groups allowed to be tracked. The no form of the command removes the values from the configuration.

**Default**
no max-num-groups

**Parameters**
max-num-groups — Specifies the maximum number of multicast groups allowed to be tracked.

- **Values**
  - 1 — 196607
maximum-routes

Syntax   maximum-routes number [log-only] [threshold percentage]  
         no maximum-routes  

Context   config>service>vprn  

Description   This command specifies the maximum number of remote routes that can be held within a VPN routing/forwarding (VRF) context. Note that local, host, static and aggregate routes are not counted.  

Note that the VPRN service ID must be in a shutdown state in order to modify maximum-routes command parameters.  

If the log-only parameter is not specified and the maximum-routes value is set below the existing number of routes in a VRF, then the offending RIP peer (if applicable) is brought down (but the VPRN instance remains up). BGP peering will remain up but the exceeding BGP routes will not be added to the VRF.  

The maximum route threshold can dynamically change to increase the number of supported routes even when the maximum has already been reached. Protocols will resubmit their routes which were initially rejected.  

The no form of the command disables any limit on the number of routes within a VRF context. Issue the no form of the command only when the VPRN instance is shutdown.  

Default   0 or disabled — The threshold will not be raised.  

Parameters   number — An integer that specifies the maximum number of routes to be held in a VRF context.  

   Values   1 — 2147483647  
   log-only — This parameter specifies that if the maximum limit is reached, only log the event. log-only does not disable the learning of new routes.  
   threshold percentage — The percentage at which a warning log message and SNMP trap should be set. There are two warnings, the first is a mid-level warning at the threshold value set and the second is a high-level warning at level between the maximum number of routes and the mid-level rate ( [mid+max] / 2 ).  

   Values   0 — 100  

multicast-info-policy

Syntax   multicast-info-policy policy-name  
         no multicast-info-policy  

Context   config>service>vprn  

Description   This command configures multicast information policy.  

Parameters   policy-name — Specifies the policy name.  

   Values   32 chars max
Global Commands

mc-maximum-routes

Syntax  
\texttt{mc-maximum-routes number [log-only] [threshold threshold]}  

Context  
\texttt{config>service>vprn}  

Description  
This command specifies the maximum number of multicast routes that can be held within a VPN routing/forwarding (VRF) context. When this limit is reached, a log and SNMP trap are sent. If the \texttt{log-only} parameter is not specified and the maximum-routes value is set below the existing number of routes in a VRF, then no new joins will be processed. The \texttt{no} form of the command disables the limit of multicast routes within a VRF context. Issue the \texttt{no} form of the command only when the VPRN instance is shutdown.

Default  
no mc-maximum-routes

Parameters  
\texttt{number} — Specifies the maximum number of routes to be held in a VRF context.

Values  
1 — 2147483647

\texttt{log-only} — Specifies that if the maximum limit is reached, only log the event. \texttt{log-only} does not disable the learning of new routes.

\texttt{threshold threshold} — The percentage at which a warning log message and SNMP trap should be sent.

Values  
0 — 100

Default  
10

ptp

Syntax  
\texttt{[no] ptp}  

Context  
\texttt{config>service>vprn}  

Description  
This command enables the context to configure PTP parameters for the VPRN service.

peer-limit

Syntax  
\texttt{peer-limit limit}  
\texttt{no peer-limit}  

Context  
\texttt{config>service>vprn>ptp}  

Description  
This command specifies an upper limit to the number of discovered peers permitted within the routing instance. This can be used to ensure that a routing instance does not consume all the possible discovered peers and blocking discovered peers in other routing instances.

If it is desired to reserve a fixed number of discovered peers per router instance, then all router instances supporting PTP should have values specified with this command and the sum of all the peer-limit values must not exceed the maximum number of discovered peers supported by the system.
If the user attempts to specify a peer-limit, and there are already more discovered peers in the routing instance than the new limit being specified, the configuration will not be accepted.

**Default**
no limit

**Parameters**

- **limit** — Specifies the maximum number of discovered peers allowed in the routing instance.
  - **Values**
    - 0 — 50
  - **Default**
    - 0 (The maximum number of discovered peers supported by the system.)

---

**peer**

**Syntax**

```
peer a.b.c.d [create]
```

**Context**

```
config>system>ptp
configure>service>vprn>ptp
```

**Description**
This command configures a remote PTP peer. It provides the context to configure parameters for the remote PTP peer.

Up to 20 remote PTP peers may be configured.

The **no** form of the command deletes the specified peer.

If the clock-type is ordinary slave or boundary, and PTP is no shutdown, the last peer cannot be deleted. This prevents the user from having PTP enabled without any peer configured and enabled.

Peers are created within the routing instance associated with the context of this command. All configured PTP peers must use the same routing instance.

**Default**
none

**Parameters**

- **a.b.c.d** — The IP address of the remote peer.
  - **Values**
    - ipv4-address a.b.c.d

---

**priority**

**Syntax**

```
priority local-priority
no priority
```

**Context**

```
configure>service>vprn>ptp>peer
```

**Description**
This command configures the local priority used to choose between PTP masters in the best master clock algorithm (BMCA). This setting is only relevant when the g.8265.1-2010 profile is selected.

The parameter is ignored when the ieee1588-2008 profile is selected. The value 1 is the highest priority and 255 is the lowest priority.

The priority of a peer cannot be configured if the PTP profile is ieee1588-2008.

**Default**
128

**Parameters**

- **local-priority** — Specifies the PTP peer local priority.
Values

### reassembly-group

**Syntax**
```
reassembly-group nat-group-id
no reassembly-group
```

**Context**
```
configure>router
cfg>service>vprn
```

**Description**
This command associates a reassembly-group consisting of multiple ISAs with the routing context in which the application requiring reassembly service resides.

**Default**
```
no route-distinguisher
```

**Parameters**
- `nat-group-id` — Nat-group id. The nat-group contains up to 10 active ISAs.
- `asn:number` — The ASN is a 2-byte value less than or equal to 65535. The assigned number can be any 32-bit unsigned integer value.

### route-distinguisher

**Syntax**
```
route-distinguisher [ip-address:number | asn:number]
no route-distinguisher
```

**Context**
```
config>service>vprn
```

**Description**
This command sets the identifier attached to routes the VPN belongs to. Each routing instance must have a unique (within the carrier’s domain) route distinguisher associated with it. A route distinguisher must be defined for a VPRN to be operationally active.

**Default**
```
no route-distinguisher
```

**Parameters**
The route distinguisher is a 6-byte value that can be specified in one of the following formats:
- `ip-address:number` — Specifies the IP address in dotted decimal notation. The assigned number must not be greater than 65535.
- `asn:number` — The ASN is a 2-byte value less than or equal to 65535. The assigned number can be any 32-bit unsigned integer value.

### router-id

**Syntax**
```
router-id ip-address
no router-id
```

**Context**
```
config>service>vprn
cfg>service>vprn>ospf
cfg>service>vprn>bgp
```


Description
This command sets the router ID for a specific VPRN context. If neither the router ID nor system interface are defined, the router ID from the base router context is inherited. The no form of the command removes the router ID definition from the given VPRN context.

Default
no router-id

Parameters
ip-address — The IP address must be given in dotted decimal notation.

service-name

Syntax
service-name service-name
no service-name

Context
config>service>vprn

Description
This command configures an optional service name, up to 64 characters in length, which adds a name identifier to a given service to then use that service name in configuration references as well as display and use service names in show commands throughout the system. This helps the service provider/administrator to identify and manage services within the 7750 SR, 7450 ESS and 7710 SR platforms.

All services are required to assign a service ID to initially create a service. However, either the service ID or the service name can be used to identify and reference a given service once it is initially created.

Parameters
service-name — Specifies a unique service name to identify the service. Service names may not begin with an integer (0-9).

sgt-qos

Syntax
sgt-qos

Context
config>service>vprn

Description
This command enables the context to configure DSCP/Dot1p re-marking for self-generated traffic.

application

Syntax
application dscp-app-name dscp {dscp-value | dscp-name}
application dot1p-app-name dot1p dot1p-priority
no application {dscp-app-name | dot1p-app-name}

Context
config>service>vprn>sgt-qos

Description
This command configures DSCP/Dot1p re-marking for self-generated traffic. When an application is configured using this command, then the specified DSCP name/value is used for all packets generated by this application within the router instance it is configured.

Using the value configured in this command:
Global Commands

- Sets the DSCP bits in the IP packet.
- Maps to the FC. This value will be signaled from the CPM to the egress forwarding complex.
- Based on this signaled FC the egress forwarding complex QoS policy sets the IEEE802.1 dot1P and LSP EXP bits.
- The Dot1P and the LSP EXP bits are set by the egress complex for all packets based on the signaled FC. This includes ARP and IS-IS packets that, due to their nature, do not carry DSCP bits.
- The DSCP value in the egress IP header will be as configured in this command. The egress QoS policy will not overwrite this value.

Only one DSCP name/value can be configured per application, if multiple entries are configured then the subsequent entry overrides the previous configured entry.

The no form of this command reverts back to the default value.

**Parameters**

- **dscp-app-name** — Specifies the DSCP application name.
  - **Values** — ldp, rsvp, bgp, rip, mspdp, pim, ptp, ospf, igmp, mld, telnet, tftp, ftp, ssh, snmp, snmp-notification, syslog, icmp, traceroute, tacplus, dns, ntp, radius, cflowd, dhcp, bootp, ndis, vrrp, srp

- **dscp-value** — Specifies a value when this packet egresses the respective egress policy should provide the mapping for the DSCP value to either LSP-EXP bits or IEEE 802.1p (Dot1P) bits as appropriate otherwise the default mapping applies.
  - **Values** — 0 — 63

- **dscp-name** — Specifies the DSCP name.
  - **Values** — none, be, ef, cp1, cp2, cp3, cp4, cp5, cp6, cp7, cp9, cs1, cs2, cs3, cs4, cs5, nc1, nc2, af11, af12, af13, af21, af22, af23, af31, af32, af41, af42, af43, cp11, cp13, cp15, cp17, cp19, cp21, cp23, cp25, cp27, cp29, cp31, cp33, cp35, cp37, cp39, cp41, cp42, cp43, cp44, cp45, cp47, cp49, cp50, cp51, cp52, cp53, cp54, cp55, cp57, cp58, cp59, cp60, cp61, cp62, cp63

- **dot1p-priority** — Specifies the Dot1P priority.
  - **Values** — 0 — 7

- **dot1p-app-name** — Specifies the Dot1P application name.
  - **Values** — arp, isis

**dscp**

**Syntax**

```
   dscp  dscp-name  fc  fc-name
   no dscp  dscp-name
```

**Context**

config>service>vprn>sgt-qos

**Description**

This command creates a mapping between the DiffServ Code Point (DSCP) of the self generated traffic and the forwarding class.

Self generated traffic that matches the specified DSCP will be assigned to the corresponding forwarding class. Multiple commands can be entered to define the association of some or all sixty-
four DiffServ code points to the forwarding class. For undefined code points, packets are assigned to the forwarding class specified under the default-action command.

All DSCP names that define a DSCP value must be explicitly defined.

The **no** form of this command removes the DiffServ code point to forwarding class association. The default-action then applies to that code point value.

### Parameters

**dscp-name** — The name of the DiffServ code point to be associated with the forwarding class. DiffServ code point can only be specified by its name and only an existing DiffServ code point can be specified. The software provides names for the well known code points.

**Values**

be, ef, cp1, cp2, cp3, cp4, cp5, cp6, cp7, cp9, cs1, cs2, cs3, cs4, cs5, nc1, nc2, af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, cp11, cp13, cp15, cp17, cp19, cp21, cp23, cp25, cp27, cp29, cp31, cp33, cp35, cp37, cp39, cp41, cp42, cp43, cp44, cp45, cp47, cp49, cp50, cp51, cp52, cp53, cp54, cp55, cp57, cp58, cp59, cp60, cp61, cp62, cp63

**fc fc-name** — Specifies the forwarding class name. All packets with DSCP value or MPLS EXP bits that is not defined will be placed in this forwarding class.

**Default** None, the fc name must be specified

**Values** be, l2, af, l1, h2, ef, h1, nc

### snmp-community

**Syntax**

```
snmp-community community-name [version SNMP-version]
no snmp-community [community-name]
```

**Context**

`config>service>vprn`

**Description**

This command sets the SNMP community name to be used with the associated VPRN instance. If an SNMP community name is not specified, then SNMP access is not allowed.

The **no** form of the command removes the SNMP community name from the given VPRN context.

**Default** None — The SNMP community must be explicitly specified.

**Parameters**

**community-name** — Specifies one or more SNMP community names.

**version SNMP-version** — Specifies the SNMP version.

**Values** v1, v2c, both

### source-address

**Syntax**

```
source-address
```

**Context**

`config>service>vprn`
Global Commands

Description
This command enables the context to specify the source address and application that should be used in all unsolicited packets.

application

Syntax
application app [ip-int-name|ip-address]
no application app

Context
config>service>vprn>source-address

Description
This command specifies the source address and application.

Parameters
app — Specify the application name.

Values
ping, ptp, ssh, telnet, traceroute

ip-int-name | ip-address — Specifies the name of the IP interface or IP address. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

static-route

Syntax
[no] static-route {ip-prefix/prefix-length | ip-prefix netmask} [preference preference] [metric metric] [tag tag] [community comm-id] [enable | disable] {next-hop ip-int-name | ip-address [mcast-family] | ipsec-tunnel ipsec-tunnel-name} [bfd-enable] | {cpe-check cpe-ip-address [interval seconds] [drop-count count] [log]}]
[no] static-route {ip-prefix/prefix-length | ip-prefix netmask} [preference preference] [metric metric] [tag tag] [community comm-id] [enable | disable] indirect ip-address [cpe-check cpe-ip-address [interval seconds][drop-count count] [log]]
[no] static-route {ip-prefix/prefix-length | ip-prefix netmask} [preference preference] [metric metric] [tag tag] [community comm-id] [enable | disable] black-hole [mcast-family]

Context
config>service>vprn

Description
This command creates a static route. A static route can have a directly-connected interface as a next-hop (specified using the IP interface name or an IP address of the interface), or an indirect IP address as a next-hop or a black-hole next-hop (specifying a discard action).

The no form of the command deletes the static route entry. If a static route needs to be removed when multiple static routes exist to the same destination, then as many parameters to uniquely identify the static route must be entered.

If a CPE connectivity check target address is already being used as the target address in a different static route, then cpe-check parameters must match. If they do not, the new configuration command will be rejected.

If a static-route command is issued with no cpe-check target but the destination prefix/netmask and next-hop matches a static route that did have an associated cpe-check, the cpe-check test will be removed from the associated static route.

Default
No static routes are defined.
Parameters

- **ip-prefix** — The destination address of the aggregate route in dotted decimal notation.
  - **Values**
    - ipv4-prefix: a.b.c.d (host bits must be 0)
    - ipv4-prefix-length: 0 — 32

- **netmask** — The subnet mask in dotted decimal notation.
  - **Values**
    - 0.0.0.0 — 255.255.255.255 (network bits all 1 and host bits all 0)

- **ip-int-name** — The name of the IP interface. Interface names must be unique within the group of defined IP interfaces for `config router interface` and `config services interface` commands. An interface name cannot be in the form of an IP address. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed with

- **ip-address** — The IP address of the IP interface. The `ip-addr` portion of the `address` command specifies the IP host address that will be used by the IP interface within the subnet. This address must be unique within the subnet and specified in dotted decimal notation.
  - **Values**
    - ipv4-address: a.b.c.d (host bits must be 0)

- **community comm-id** — This configuration option associates a BGP community with the static route. The community can be matched in route policies and is automatically added to BGP routes exported from the static route.
  - **Values**
    - comm-id: asn:comm-val | well-known-comm
      - asn: 0 — 65535
      - comm-val: 0 — 65535
      - well-known-comm: no-advertise, no-export, no-export-subconfed

- **enable** — Static routes can be administratively enabled or disabled. Use the `enable` parameter to re-enable a disabled static route. In order to enable a static route, it must be uniquely identified by the IP address, mask, and any other parameter that is required to identify the exact static route.
  - Default: enable

- **disable** — Static routes can be administratively enabled or disabled. Use the `disable` parameter to disable a static route while maintaining the static route in the configuration. In order to enable a static route, it must be uniquely identified by the IP address, mask, and any other parameter that is required to identify the exact static route.
  - Default: enable

- **interval seconds** — This optional parameter specifies the interval between ICMP pings to the target IP address.
  - **Values**
    - 1 — 255 seconds
  - Default: 1 seconds

- **drop-count count** — This optional parameter specifies the number of consecutive ping-replies that must be missed to declare the CPE down and to de-active the associated static route.
  - **Values**
    - Value range: 1 — 255
  - Default: 3
log — This optional parameter enables the ability to log transitions between active and in-active based on the CPE connectivity check. Events should be sent to the system log, syslog and SNMP traps.

next-hop [ip-address | ip-int-name] — Specifies the directly connected next hop IP address used to reach the destination. If the next hop is over an unnumbered interface, the ip-int-name of the unnumbered interface (on this node) can be configured.

The next-hop keyword and the indirect or black-hole keywords are mutually exclusive. If an identical command is entered (with the exception of either the indirect or black-hole parameters), then this static route will be replaced with the newly entered command, and unless specified, the respective defaults for preference and metric will be applied.

The ip-addr configured here can be either on the network side or the access side on this node. This address must be associated with a network directly connected to a network configured on this node.

ipsec-tunnel ipsec-tunnel-name — specifies an IPSec tunnel name up to 32 characters in length.

indirect ip-address — Specifies that the route is indirect and specifies the next hop IP address used to reach the destination.

The configured ip-addr is not directly connected to a network configured on this node. The destination can be reachable via multiple paths. The static route remains valid as long as the address configured as the indirect address remains a valid entry in the routing table. Indirect static routes cannot use an ip-prefix/mask to another indirect static route.

The indirect keyword and the next-hop or black-hole keywords are mutually exclusive. If an identical command is entered (with the exception of either the next-hop or black-hole parameters), then this static route will be replaced with the newly entered command and unless specified the respective defaults for preference and metric will be applied.

The ip-addr configured can be either on the network or the access side and is normally at least one hop away from this node.

black-hole — Specifies a black hole route meaning that if the destination address on a packet matches this static route it will be silently discarded.

The black-hole keyword is mutually exclusive with either the next-hop or indirect keywords. If an identical command is entered, with exception of either the next-hop or indirect parameters, then the static route is replaced with the new command, and unless specified, the respective defaults for preference and metric are applied.

preference preference — The preference of this static route (as opposed to the routes from different sources such as BGP or OSPF), expressed as a decimal integer. When modifying the preference value of an existing static route, unless specified, the metric will not change.

If multiple routes are learned with an identical preference using the same protocol, the lowest cost route is used. If multiple routes are learned with an identical preference using the same protocol and the costs (metrics) are equal, then the decision of which route to use is determined by the configuration of the ECMP command.

Default 5

Values 1 — 255

metric metric — The cost metric for the static route, expressed as a decimal integer. This value is used when importing this static route into other protocols such as OSPF. This value is also used
Virtual Private Routed Network Services

to determine the static route to install in the forwarding table: When modifying the metrics of an existing static route, unless specified, the preference will not change.

If there are multiple static routes with the same preference but unequal metrics, the lower cost (metric) route is installed. If there are multiple static routes with equal preference and metrics then ECMP rules apply. If there are multiple routes with unequal preferences, then the lower preference route is installed.

**Default**

```
1
```

**Values**

```
0 — 65535
```

tag — Adds a 32-bit integer tag to the static route. The tag is used in route policies to control distribution of the route into other protocols.

**Values**

```
1..4294967295
```

**bfd-enable** — Associates the state of the static route to a BFD session between the local system and the configured nexthop. This keyword cannot be configured if the nexthop is **indirect** or a **blackhole** keywords are specified.

cpe-check target-ip-address — This parameter specifies the IP address of the target CPE device. ICMP pings will be sent to this target IP address. This parameter must be configured to enable the CPE connectivity feature for the associated static route. The target-ip-address cannot be in the same subnet as the static route subnet itself to avoid possible circular references. This option is mutually exclusive with BFD support on a given static route.

**Default**

```
no cpe-check enabled
```

**mcast-family** — Enables submission of the IPv4 static route into IPv4 multicast RTM.

**Values**

```
mcast-ipv4
```

**type**

| Syntax            | type [hub | spoke | subscriber-split-horizon] no type |
|-------------------|-----------------------------------|
| **Context**       | config>service>vprn>             |
| **Description**   | This command designates the type of VPRN instance being configured for hub and spoke topologies. Use the **no** form to reset to the default of a fully meshed VPRN. |
| **Default**       | no type                           |
| **Parameters**    | hub — Specifies a hub VPRN which allows all traffic from the hub SAPs to be routed to the destination directly, while all traffic from spoke VPRNs or network interfaces can only be routed to a hub SAP. |
|                   | spoke — Specifies a spoke VPRN which allows traffic from associated SAPs or spoke terminations to only be forwarded through routes learned from separate VPRN, which should be configured as a type Hub VPRN. |
|                   | subscriber-split-horizon — Controls the flow of traffic for wholesale subscriber applications. |
Global Commands

vrf-export

Syntax
vrf-export policy [policy...]
no vrf-export

Context config>service>vprn

Description This command specifies the export policies to control routes exported from the local VPN routing/forwarding (VRF) to other VRFs on the same or remote PE routers (via MP-BGP).

You can specify up to fifteen (15) policy names.

The **no** form of the command removes all route policy names from the export list.

Default None — No routes are exported from the VRF by default.

Parameters
- **policy** — The route policy statement name.

vrf-import

Syntax
vrf-import policy [policy...]
no vrf-import

Context config>service>vprn

Description This command sets the import policies to control routes imported to the local VPN routing/forwarding (VRF) from other VRFs on the same or remote PE routers (via MP-BGP). Up to fifteen (15) names may be specified.

BGP-VPN routes imported with a vrf-import policy will use the BGP preference value of 170 when imported from remote PE routers, or retain the protocol preference value of the exported route when imported from other VRFs on the same router, unless the preference is changed by the policy.

The **no** form of the command removes all route policy names from the import list

Default None — No routes are accepted into the VRF by default.

Parameters
- **policy** — The route policy statement name.

vrf-target

Syntax
vrf-target {ext-community | export ext-community | import ext-community}
no vrf-target

Context config>service>vprn

Description This command facilitates a simplified method to configure the route target to be added to advertised routes or compared against received routes from other VRFs on the same or remote PE routers (via MP-BGP).

BGP-VPN routes imported with a vrf-target statement will use the BGP preference value of 170 when imported from remote PE routers, or retain the protocol preference value of the exported route when imported from other VRFs in the same router.
Specified **vrf-import** or **vrf-export** policies override the **vrf-target** policy.

The no form of the command removes the vrf-target

**Default**

```text
no vrf-target
```

**Parameters**

`ext-comm` — An extended BGP community in the `type:x:y` format. The value `x` can be an integer or IP address. The `type` can be the target or origin. `x` and `y` are 16-bit integers.

**Values**

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;2byte-asnumber:ext-comm-val&gt;</td>
<td>&lt;4byte-asnumber:comm-val&gt;}</td>
<td>comm-val</td>
<td>0..65535</td>
</tr>
<tr>
<td>&lt;2byte-asnumber:ext-comm-val&gt;</td>
<td>&lt;4byte-asnumber:comm-val&gt;}</td>
<td>2byte-asnumber</td>
<td>0..65535</td>
</tr>
<tr>
<td>&lt;2byte-asnumber:ext-comm-val&gt;</td>
<td>&lt;4byte-asnumber:comm-val&gt;}</td>
<td>ext-comm-val</td>
<td>0..4294967295</td>
</tr>
<tr>
<td>&lt;2byte-asnumber:ext-comm-val&gt;</td>
<td>&lt;4byte-asnumber:comm-val&gt;}</td>
<td>4byte-asnumber</td>
<td>0..4294967295</td>
</tr>
</tbody>
</table>

**import ext-community** — Specify communities allowed to be accepted from remote PE neighbors.

**export ext-community** — Specify communities allowed to be sent to remote PE neighbors.

**Default**

```text
Failover local.
```

**server**

**Syntax**

```text
server server-name
no server
```

**Context**

```text
configure>service>ies>sub-if>grp-if>local-address-assignment
```

**Description**

This command designates a local 7x50 DHCPv4 server for local pools management where IPv4 addresses for PPPoXv4 clients will be allocated without the need for the internal 7x50 DHCP relay-agent. Those addresses will be tied to PPPoX sessions and they will be de-allocated when the PPPoX session is terminated.

**Default**

```text
none
```

**Parameters**

`server-name` — Specifies the name of the local 7x50 DHCP server.

**client-application**

**Syntax**

```text
client-application [ppp-v4]
no client-application
```

**Context**

```text
configure>service>ies>sub-if>grp-if>local-address-assignment
```
Global Commands

configure>service>ies>sub-if>local-address-assignment
configure>service>vprn>sub-if>grp-if>local-address-assignment
configure>service>vprn>sub-if>local-address-assignment

Description
This command enables local 7x50 DHCP Server pool management for PPPoXv4 clients. A pool of IP addresses can be shared between IPoE clients that rely on DHCP protocol (lease renewal process) and PPPoX clients where address allocation is not dependent on DHCP messaging but instead an IP address allocation within the pool is tied to the PPPoX session.

Default
none

Parameters
ppp-v4 —

default-pool

Syntax
default-pool pool-name
do default-pool

Description
This command references a default DHCP address pool for local PPPoX pool management in case that the pool-name is not returned via Radius or LUDB.

Default
none

Parameters
pool-name — Specifies the name of the local 7x50 DHCP server pool.

delayed-enable

Syntax
delayed-enable seconds [init-only]
do delayed-enable

Context
configure>service>ies>sub-if>local-address-assignment
configure>service>vprn>sub-if>local-address-assignment

Description
This command will render the subscriber-interface non operational for the given amount of time once the node is rebooted or once the interface is enabled (no-shutdown). The purpose of this timer is to stall the operation of the subscriber-interface until the MCS database is synchronized.

A typical use case for this timer would be to prevent IP lease duplication for PPPoE clients using local PPPoXv4/v6 pools in redundant DHCPv4/v6 server configuration. Since there is no classical DHCP lease state maintained for local PPPoXv4/v6 pools, the IP addresses will not be synchronized via DHCP Server. Instead they will be synchronized via PPPoX clients whose state is maintained in 7x50. Once the PPPoX subscriber host is synchronized between the two 7x50 nodes, the respective IP address lease will be updated in the respective local pool.

One artifact of this behavior (IP address assignment in local DHCP pools is synchronized via PPPoX clients and not via DHCP server synchronization mechanism) is that during the node boot, the DHCP server must wait for the completion of PPPoX subscriber synchronization via MCS so that it learns
which addresses/prefixes are already allocated on the peering node. Since the DHCP server can theoretically start assigning IP addresses before the PPPoX sync is completed, a duplicate address assignment may occur. For example an IP address lease can be granted via DHCP local pools while PPPoX sync is still in progress. Once the PPPoX sync is completed, the DHCP server may discover that the granted IP lease has already been allocated by the peering node. The most recent lease will be kept and the other will be removed from both systems. To prevent this scenario, a configurable timer is set to an arbitrary value that will render sub-if non-operational until the timer expires. The purpose of this timer is to allow the PPPoX sync to complete before subscribers under the sub-intf can be served.

| Default  | none                  |
| Parameters | second — Specifies in seconds. |
| Values    | 1..1200                |
Multicast VPN Commands

mvpn

Syntax
mvpn

Context
config>service>vprn

Description
This command enables the context to configure MVPN-related parameters for the IP VPN.

auto-discovery

Syntax
[no] auto-discovery [default | mdt-safi] [source-address ip-address]

Context
config>service>vprn>mvpn

Description
This command enables MVPN membership auto-discovery through BGP. When auto-discovery is enabled, PIM peering on the inclusive provider tunnel is disabled. Changing auto-discovery configuration requires shutdown of this VPRN instance.

The no form of the command disables MVPN membership auto-discovery through BGP.

Default
enabled

default — Enable Enable AD route exchange based on format defined in ng-MVPN (RFC6514).

mdt-safi — Enable AD route exchange based on mdt-safi format defined in draft-rosen-vpn-mcast.

This command allows optionally to specify a source-address - an IP address to be used by Rosen MVPN for core diversity non-default IGP instances (not using system IP). Two unique IP addresses for all MVPNs are supported. For instances using default System IP, source address configuration should not be specified to avoid consuming one of the addresses.

Explicitly defined source-address allows GRE-encapsulated Rosen MVPN multicast traffic (Default and Data MDT) to originate from a configured IP address, so the source IP address of the GRE packets won't be the default system IP address.

Value:

ip-address — an IPv4 address. To achieve the desired functionality the address should be a pre-configured non-default ISIS or OSPF loopback address for an IGP instance using loopback address different from the system IP loopback.

c-mcast-signaling

Syntax
c-mcast-signaling {bgp | pim}

no c-mcast-signaling

Context
config>service>vprn>mvpn
**Description**
This command specifies BGP or PIM, for PE-to-PE signaling of CE multicast states. When this command is set to PIM and neighbor discovery by BGP is disabled, PIM peering will be enabled on the inclusive tree.

Changes may only be made to this command when the mvnp node is shutdown.

The **no** form of the command reverts it back to the default.

**Default**
mcast-signaling bgp

**Parameters**
- **bgp** — Specifies to use BGP for PE-to-PE signaling of CE multicast states. Auto-discovery must be enabled.
- **pim** — Specifies to use PIM for PE-to-PE signaling of CE multicast states.

---

**intersite-shared**

**Syntax**
intersite-shared [persistend-type5-adv]

**no** intersite-shared

**Context**
config>service>vprn>mvnp

**Description**
This command specifies whether to use inter-site shared C-trees or not.

**Default**
intersite-shared

**Parameters**
- **persistend-type5-adv** — when specified for intersite-shared tress enabled, this parameter ensures that Type 5 SA routes are generated for the multicast source even if no joins are present for that source. When the parameter is not specified, the Type 5 SA routes are withdrawn where the prune from the last receiver is received for the multicast source.

---

**mdt-type**

**Syntax**
mdt-type {sender-receiver | sender-only | receiver-only}

**Context**
config>service>vprn>mvnp

**Description**
This command allows restricting MVPN instance per PE node to a specific role. By default, MVPN instance on a given PE node assumes the role of being a sender as well as receiver. This creates a mesh of MDT/PMSI across all PE nodes from this PE.

This command provides an option to configure either a sender-only or receiver only mode per PE node. Restricting the role of a PE node avoids creating full mesh of MDT/PMSI across all PE nodes that are participating in MVPN instance.

The **no** version of this command restores the default (sender-receiver).

**Default**
mdt-type sender-receiver

**Parameters**
- **sender-receiver** — MVPN has both sender and receivers connected to PE node
- **sender-only** — MVPN has only senders connected to PE node
- **receiver-only** — MVPN has only receivers connected to PE node
Global Commands

red-source-list

Syntax  red-source-list
Context  config>service>vprn>mvpn>
Description  This command enables context to configure list of redundant source prefixes for preferred source selection.

src-prefix

Syntax  src-prefix  ip-address/mask  [ip-address/mask  ..up to 8 maximum]
no  src-prefix  ip-address/mask
Context  config>service>vprn>mvpn>red-source-list
Description  This command configures up to 8 multicast source IPv4 prefixes for preferred source selection. Single or multi-line inputs are allowed. The no form of the command deletes specified prefix from the list
Default  no prefixes are specified
Parameters  ip-address/mask — IPv4 address prefix with mask.

provider-tunnel

Syntax  provider-tunnel
Context  config>service>vprn>mvpn
Description  This command enables context to configure tunnel parameters for the MVPN.

inclusive

Syntax  inclusive
Context  config>service>vprn>mvpn>pt
Description  This command enables the context for specifying inclusive provider tunnels

mldp

Syntax  mldp
no  mldp
Context  config>service>vprn>mvpn>provider-tunnel>inclusive
**Description**
This command enables use of mLDP LSP for the provider tunnel.

**Default**
no mldp

### shutdown

**Syntax**
```plaintext
shutdown
no shutdown
```

**Context**
config>service>vprn>mvpn>provider-tunnel>inclusive>mldp

**Description**
This command administratively disables and enables use of mLDP LSP for the provider tunnel.

**Default**
no shutdown

### pim

**Syntax**
```plaintext
pim {asm | ssm} grp-ip-address
no pim
```

**Context**
config>service>vprn>mvpn>provider-tunnel>inclusive

**Description**
This command specifies the PIM mode to use, ASM or SSM, for PIM-based inclusive provider tunnels and the multicast group address to use. Also enables the context for specifying parameters for PIM peering on the inclusive provider tunnel.

Note that auto-discovery must be enabled in order for SSM to operate.

The **no** form of the command removes the pim context including the statements under the context.

**Default**
no pim

**Parameters**
- **asm** — Specifies to use PIM ASM for inclusive provider tunnels.
- **ssm** — Specifies to use PIM SSM for inclusive provider tunnels.
- **group-address** — Specifies the multicast group address to use.

### hello-interval

**Syntax**
```plaintext
hello-interval hello-interval
no hello-interval
```

**Context**
config>service>vprn>mvpn>provider-tunnel>inclusive>pim

**Description**
This command specifies the interval at which PIM hello messages are transmitted on the PIM inclusive provider tunnel.

The **no** form of this command reverts to the default value.

**Default**
30 seconds
Parameters

**hello-interval** — Specifies the hello interval, in seconds. A 0 (zero) value disables the sending of hello messages.

**Values**  
0 — 255

### hello-multiplier

**Syntax**  
hello-multiplier deci-units

no hello-multiplier

**Context**  
config>service>vprn>mvpn>provider-tunnel>inclusive>pim

**Description**  
This command specifies the hello multiplier. The hello-multiplier in conjunction with the hello-interval determines the hold time for a PIM neighbor.

Hold time = (hello-interval * hello-multiplier) / 10.

The no form of the command reverts the value to the default.

**Default**  
35

**Parameters**  
decci-units — Specifies the value, in multiples of 0.1, for the formula used to calculate the hold time

**Values**  
20 — 100

### improved-assert

**Syntax**  
[no] improved-assert

**Context**  
config>service>vprn>mvpn>provider-tunnel>inclusive>pim

**Description**  
This command enables improved assert procedure on the PIM inclusive provider tunnel.

The no form of the command disables improved assert procedure.

**Default**  
enabled

### three-way-hello

**Syntax**  
[no] three-way-hello

**Context**  
config>service>vprn>mvpn>provider-tunnel>inclusive>pim

**Description**  
This command enables PIM three-way hello on the inclusive provider tunnel.

The no form of the command disables the PIM three-way hello.

**Default**  
disabled

### tracking-support
Syntax  
[no] tracking-support

Context  
config>service>vprn>mvpn>provider-tunnel>inclusive>pim

Description  
This command enables the setting of the T bit in the LAN Prune Delay option of the hello message. This indicates the router's capability to disable Join message suppression. The no form of the command disables the setting.

Default  
disabled

selective

Syntax  
selective

Context  
config>service>vprn>mvpn>provider-tunnel

Description  
This command enables the context to specify selective provider tunnel parameters.

Default  
one

auto-discovery-disable

Syntax  
[no] auto-discovery-disable

Context  
config>service>vprn>mvpn>provider-tunnel>selective

Description  
This command disables C-trees to P-tunnel binding auto-discovery through BGP so it is signaled using PIM join TLVs.

This command requires the c-mcast-signaling parameter to be set to PIM.

The no form of the command enables multicast VPN membership auto-discovery through BGP.

Default  
no auto-discovery-disable

data-delay-interval

Syntax  
data-delay-interval  value

no data-delay-interval

Context  
config>service>vprn>mvpn>provider-tunnel>selective

Description  
This command specifies the interval, in seconds, before a PE router connected to the source switches traffic from the inclusive provider tunnel to the selective provider tunnel.

The no form of the command reverts the value to the default.

Default  
3 seconds

Parameters  
value  — Specifies the data delay interval, in seconds.
data-threshold

Syntax

data-threshold {c-grp-ip-addr/mask | c-grp-ip-addr netmask} s-pmsi-threshold

data-threshold c-grp-ipv6-addr/prefix-length s-pmsi-threshold

no data-threshold {c-grp-ip-addr/mask | c-grp-ip-addr netmask}

no data-threshold c-grp-ipv6-addr/prefix-length

Context

config>service>vprn>mvpn>provider-tunnel>selective

Description

This command specifies the data rate threshold that triggers the switch from the inclusive provider tunnel to the selective provider tunnel for C-(S,G) within the group range. Multiple statements are allowed in the configuration.

The no form of the command removes the values from the configuration.

Default

none

Parameters

group-address/mask — Specifies a multicast group address and netmask length.

c-grp-ip-addr/mask | c-grp-ip-addr netmask — Specifies an IPv4 multicast group address and netmask length or network mask.

c-grp-ipv6-addr/prefix-length — Specifies an IPv6 multicast group address and prefix length.

s-pmsi-threshold — Specifies the rate, in kilobits per second (kbps). If the rate for a C-(S,G) within the specified group range exceeds the threshold, traffic for the C-(S,G) will be switched to the selective provider tunnel.

Values

c-grp-ip-addr : multicast group address a.b.c.d

mask [4..32]

netmask : a.b.c.d (network bits all 1 and host bits all 0)

s-pmsi-threshold : [1..4294967294](threshold in kbps)

c-grp-ipv6-addr : multicast ipv6-address x:x:x:x:x:x:x (eight 16-bit pieces)

x:x:x:x:x:x:d.d.d.d

x [0..FFFF]H

d [0..255]D

prefix-length [1..128]

join-tlv-packing-disable

Syntax

[no] join-tlv-packing-disable

Context

config>service>vprn>mvpn>provider-tunnel>selective>pim

Description

This command enables packing of MDT join TLVs into a single PDU to improve efficiency, if multiple Join TLVs are available at the time of transmission.

The no form of the command disables packing of MDT join TLVs into a single PDU.

Default

no join-tlv-packing-disable
pim-asm

**Syntax**

```
[no] pim-asm {grp-ip-address/mask | grp-ip-address netmask}
```

**Context**

```
config>service>vprn>mvpn>provider-tunnel>selective
```

**Description**

This command specifies the range of PIM-ASM groups to use on the sender PE to setup ASM multicast tree for draft Rosen based Data MDT.

enable-asm-mdt

**Syntax**

```
[no] enable-asm-mdt
```

**Context**

```
config>service>vprn>mvpn>provider-tunnel>selective
```

**Description**

This command enables Data MDT with PIM-ASM mode on the receiver PE node. PIM-ASM or PIM-SSM operation mode is derived based on the locally configured SSM range on the node.

If asm-mode is disabled using this command, then PIM-SSM mode is enabled for all groups, independent of the configured SSM range on the node.

pim-ssm

**Syntax**

```
pim-ssm {grp-ip-address/mask | grp-ip-address netmask}
no pim-ssm
```

**Context**

```
config>service>vprn>mvpn>provider-tunnel>selective
```

**Description**

This command specifies the PIM SSM groups to use for the selective provider tunnel.

**Parameters**

```
group-address/mask — Specifies a multicast group address and netmask length.
```

umh-pe-backup

**Syntax**

```
umh-pe-backup
```

**Context**

```
config>service>vprn>mvpn
```

**Description**

This command enables context to configure primary and standby upstream PE association for the MVPN.

umh-pe

**Syntax**

```
umh-pe ip-address standby ip-address
no umh-pe ip-address
```

**Context**

```
config>service>vprn>mvpn>umh-pe-backup
```
Global Commands

Description  This command assigns a standby PE to each primary PE that must be selected as an alternative PE in case the UFD session on tunnel from primary PE is detected down. Standby for a PE cannot be modified without shutting down the MVPN instance.

If a primary PE is not assigned a standby PE then the UMH selection would fall back to the default method.
**umh-selection**

**Syntax**
```
umh-selection {highest-ip|hash-based|tunnel-status|unicast-rt-pref}
no umh-selection
```

**Context**
```
config>service>vprn>mvpn
```

**Description**
This command specifies which UMH selection mechanism to use, highest IP address, hash based or provider tunnel status.

The **no** form of the command resets it back to default.

**Default**
```
umh-selection highest-ip
```

**Parameters**
- **highest-ip** — Specifies that the highest IP address is selected as UMH.
- **hash-based** — Specifies that the UMH selection is based on the hash based procedures.
- **tunnel-status** — Specifies that UMH selection is based on the state of the tunnel as well as the available unicast routes through the tunnel.
- **unicast-rt-pref** — When selected, best unicast route will decide which UMH is chosen. Note that, all PE routers shall prefer the same route to the UMH for the UMH selection criterion (for example BGP path selection criteria must not influence one PE to choose different UMH from another PE).

**vrf-export**

**Syntax**
```
vrf-export {unicast | policy-name [policy-name...(up to 16 max)]}
no vrf-export
```

**Context**
```
config>service>vprn>mvpn
```

**Description**
This command specifies the export policy (up to 16) to control MVPN routes exported from the local VRF to other VRFs on the same or remote PE routers.

**Default**
```
vrf-export unicast
```

**Parameters**
- **unicast** — Specifies to use unicast VRF export policy for the MVPN.
- **policy** — Specifies a route policy name.

**vrf-import**

**Syntax**
```
vrf-import {unicast | policy-name [policy-name...(up to 16 max)]}
no vrf-import
```

**Context**
```
config>service>vprn>mvpn
```

**Description**
This command specifies the import policy (up to 16) to control MVPN routes imported to the local VRF from other VRFs on the same or remote PE routers.

**Default**
```
vrf-import unicast
```
Parameters  
  **unicast** — Specifies to use a unicast VRF import policy for the MVPN.

  **policy** — Specifies a route policy name.

---

**vrf-target**

**Syntax**

```
vrp-target {unicast | ext-community | export unicast | ext-community | import unicast | ext-community}
```

**no vrf-target**

**Context**

```
config>service>vprn>mvpn
```

**Description**

This command specifies the route target to be added to the advertised routes or compared against the received routes from other VRFs on the same or remote PE routers. vrf-import or vrf-export policies override the vrf-target policy.

The `no` form of the command removes the vrf-target.

**Default**

no vrf-target

**Parameters**

**unicast** — Specifies to use unicast vrf-target ext-community for the multicast VPN.

**ext-comm** — An extended BGP community in the `type:x:y` format. The value `x` can be an integer or IP address. The `type` can be the target or origin. `x` and `y` are 16-bit integers.

**Values**

```
target: [ip-address:comm-val | 2byte-asnumber:ext-comm-val | 4byte-asnumber:comm-val]
  ip-address: a.b.c.d
  comm-val: 0 — 65535
  2byte-asnumber: 1 — 65535
  4byte-asnumber: 0 — 4294967295
```

**import ext-community** — Specify communities allowed to be accepted from remote PE neighbors.

**export ext-community** — Specify communities allowed to be sent to remote PE neighbors.

---

**export**

**Syntax**

```
export {unicast | ext-community}
```

**Context**

```
config>service>vprn>mvpn>vrf-target
```

**Description**

This command specifies communities to be sent to peers.

**Parameters**

**unicast** — Specifies to use unicast vrf-target ext-community for the multicast VPN.

**ext-comm** — An extended BGP community in the `type:x:y` format. The value `x` can be an integer or IP address. The `type` can be the target or origin. `x` and `y` are 16-bit integers.

**Values**

```
target: [ip-address:comm-val | 2byte-asnumber:ext-comm-val | 4byte-asnumber:comm-val]
  ip-address: a.b.c.d
  comm-val: 0 — 65535
```
import

Syntax    import \( \text{unicast} \mid \text{ext-community} \)  
Context   config>service>vprn>mvpn>vrf-target  
Description This command specifies communities to be accepted from peers.  
Parameters  
unicast — Specifies to use unicast vrf-target ext-community for the multicast VPN. 

ext-comm — An extended BGP community in the \text{type}:x:y format. The value \( x \) can be an integer or IP address. The \text{type} can be the target or origin. \( x \) and \( y \) are 16-bit integers. 

Values  
\( \text{target:} \{ \text{ip-address:comm-val} \mid 2\text{byte-asnumber:ext-comm-val} \mid 4\text{byte-asnumber:comm-val} \} \)  
\( \text{ip-address:} \) a.b.c.d  
\( \text{comm-val:} \) 0 — 65535  
\( 2\text{byte-asnumber:} \) 1 — 65535  
\( 4\text{byte-asnumber} \) 0 — 4294967295
Redundant Interface Commands

redundant-interface

Syntax  [no] redundant-interface ip-int-name

Context  config>service>vprn

Description  This command configures a redundant interface.

Parameters  ip-int-name — Specifies the name of the IP interface. Interface names can be from 1 to 32 alphanumeric characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

address

Syntax  address {ip-address/mask | ip-address netmask} [remote-ip ip-address]
        no address

Context  config>service>vprn>redundant-interface

Description  This command assigns an IP address mask or netmask and a remote IP address to the interface.

Parameters  ip-address/mask — Assigns an IP address/IP subnet format to the interface.

ip-address netmask — Specifies a string of 0s and 1s that mask or screen out the network part of an IP address so that only the host computer part of the address remains.

Assigns an IP address netmask to the interface.

remote-ip ip-address — Assigns a remote IP to the interface.
SDP Commands

**spoke-sdp**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>[no] spoke-sdp sdp-id</th>
</tr>
</thead>
<tbody>
<tr>
<td>Context</td>
<td>config&gt;service&gt;vprn</td>
</tr>
<tr>
<td>Description</td>
<td>This command binds a service to an existing Service Distribution Point (SDP). A spoke SDP is treated like the equivalent of a traditional bridge “port” where flooded traffic received on the spoke SDP is replicated on all other “ports” (other spoke and mesh SDPs or SAPs) and not transmitted on the port it was received. The SDP has an operational state which determines the operational state of the SDP within the service. For example, if the SDP is administratively or operationally down, the SDP for the service will be down. The SDP must already be defined in the config&gt;service&gt;sdp context in order to associate an SDP with a VPRN service. If the sdp sdp-id is not already configured, an error message is generated. If the sdp-id does exist, a binding between that sdp-id and the service is created. SDPs must be explicitly associated and bound to a service. If an SDP is not bound to a service, no far-end devices can participate in the service. The no form of this command removes the SDP binding from the service. The SDP configuration is not affected; only the binding of the SDP to a service. Once removed, no packets are forwarded to the far-end router.</td>
</tr>
<tr>
<td>Default</td>
<td>No sdp-id is bound to a service.</td>
</tr>
<tr>
<td>Special Cases</td>
<td>VPRN — Several SDPs can be bound to a VPRN service. Each SDP must be destined to a different router. If two sdp-id bindings terminate on the same, an error occurs and the second SDP binding is rejected.</td>
</tr>
<tr>
<td>Parameters</td>
<td>sdp-id — The SDP identifier. Allowed values are integers in the range of 1 and 17407 for existing SDPs. vc-id — The virtual circuit identifier.</td>
</tr>
<tr>
<td>Values</td>
<td>1 — 4294967295</td>
</tr>
</tbody>
</table>

**spoke-sdp**

| Syntax          | spoke-sdp sdp-id [:vc-id] vc-type {ether|pipe} [create] |
|-----------------|---------------------------------------------------------|
| Context         | config>service>vprn>if                                   |
| Description     | This command binds a service to an existing Service Distribution Point (SDP). |
A spoke SDP is treated like the equivalent of a traditional bridge “port” where flooded traffic received on the spoke SDP is replicated on all other “ports” (other spoke and mesh SDPs or SAPs) and not transmitted on the port it was received.

The SDP has an operational state which determines the operational state of the SDP within the service. For example, if the SDP is administratively or operationally down, the SDP for the service will be down.

The SDP must already be defined in the `config>service>sdp` context in order to associate an SDP with a service. If the `sdp sdp-id` is not already configured, an error message is generated. If the `sdp-id` does exist, a binding between that `sdp-id` and the service is created.

SDPs must be explicitly associated and bound to a service. If an SDP is not bound to a service, no far-end devices can participate in the service.

Class-based forwarding is not supported on a spoke SDP used for termination on an IES or VPRN services. All packets are forwarded over the default LSP.

The `no` form of this command removes the SDP binding from the service. The SDP configuration is not affected; only the binding of the SDP to a service. Once removed, no packets are forwarded to the far-end router.

**Default** none

**Special Cases** VPRN — Several SDPs can be bound to a VPRN service. Each SDP must be destined to a different router. If two `sdp-id` bindings terminate on the same , an error occurs and the second SDP is binding is rejected.

`sdp-id` — The SDP identifier.

**Values** 1 — 17407

`vc-id` — The virtual circuit identifier.

**Values** 1 — 4294967295

`vc-type` — The encapsulation and pseudowire type for the spoke SDP.

**Values** ether—Ethernet pseudowire.

ipipe—IP pseudowire.

**Default** ether

### egress

**Syntax** `egress`

**Context** `config>service>vprn>if>spoke-sdp`

**config>service>vprn>red-if>spoke-sdp`

**Description** This command configures an SDP context.

### hash-label

**Syntax** `[no] hash-label`
Virtual Private Routed Network Services

**Context**

config>service>vprn
config>service>vprn>spoke-sdp
config>service>vprn>if>spoke-sdp

**Description**

This command enables the use of the hash label on a VLL, VPLS, or VPRN service bound to LDP or RSVP SDP as well as to a VPRN service using the autobind mode with the with the ldp, rsvp-te, or mpls options. This feature is not supported on a service bound to a GRE SDP or for a VPRN service using the autobind mode with the gre option.

When this feature is enabled, the ingress data path is modified such that the result of the hash on the packet header is communicated to the egress data path for use as the value of the label field of the hash label. The egress data path appends the hash label at the bottom of the stack (BoS) and sets the S-bit to 1 to indicate that.

In order to allow for applications whereby the egress LER infers the presence of the Hash Label implicitly from the value of the label, the Most Significant Bit (MSB) of the result of the hash is set before copying into the Hash Label. This means that the value of the hash label will always be in the range [524,288 - 1,048,575] and will not overlap with the signaled/static LSP and signaled/static service label ranges. This also guarantees that the hash label will not match a value in the reserved label range.

The (unmodified) result of the hash continues to be used for the purpose of ECMP and LAG spraying of packets locally on the ingress LER. Note however that for VLL services, the result of the hash is overwritten and the ECMP and LAG spraying will be based on service-id when ingress SAP shared queuing is not enabled. However, the hash label will still reflect the result of the hash such that an LSR can use it to perform fine grained load balancing of VLL pseudowire packets.

Packets that are generated in CPM and forwarded labeled within the context of a service (for example, OAM packets) must also include a Hash Label at the BoS and set the S-bit accordingly.

The TTL of the hash label is set to a value of 0.

The **no** form of this command disables the use of the hash label.

**Default**

no hash-label

**ingress**

**Syntax**

ingress

**Context**

config>service>vprn>if>spoke-sdp
config>service>vprn>red-if>spoke-sdp

**Description**

This command configures the SDP context.
### qos

**Syntax**

```plaintext
qos network-policy-id fp-redirect-group queue-group-name instance instance-id
no qos
```

**Context**

```plaintext
configure>service>apipe>spoke-sdp>ingress
configure>service>cpipe>spoke-sdp>ingress
configure>service>epipe>spoke-sdp>ingress
configure>service>fpipe>spoke-sdp>ingress
configure>service>ipipe>spoke-sdp>ingress
config>service>vpls>spoke-sdp>ingress
config>service>vpls>mesh-sdp>ingress
config>service>pw-template>ingress
config>service>vprn>interface>spoke-sdp>ingress
config>service>ies>interface>spoke-sdp>ingress
```

**Description**

This command is used to redirect pseudowire packets to an ingress forwarding plane queue-group for the purpose of rate-limiting.

The ingress pseudowire rate-limiting feature uses a policer in queue-group provisioning model. This model allows the mapping of one or more pseudowires to the same instance of policers, which are defined in a queue-group template.

Operationally, the provisioning model in the case of the ingress pseudowire shaping feature consists of the following steps:

1. Create an ingress queue-group template and configure policers for each FC that needs to be redirected and optionally, for each traffic type (unicast or multicast).
2. Apply the queue-group template to the network ingress forwarding plane where there exists a network IP interface to which the pseudowire packets can be received. This creates one instance of the template on the ingress of the FP. One or more instances of the same template can be created.
3. Configure FC-to-policer mappings together with the policer redirect to a queue-group in the ingress context of a network QoS policy. No queue-group name is specified in this step, which means the same network QoS policy can redirect different pseudowires to different queue-group templates.
4. Apply this network QoS policy to the ingress context of a spoke-SDP inside a service, or to the ingress context of a pseudowire template, and specify the redirect queue-group name.
5. One or more spoke-SDPs can have their FCs redirected to use policers in the same policer queue-group instance.

The following are the constraints and rules of this provisioning model when used in the ingress pseudowire rate-limiting feature:

1. When a pseudowire FC is redirected to use a policer in a named policer queue-group and the queue-group name does not exist, the association is failed at the time the user associates the ingress context of a spoke-SDP to the named queue-group. In such a case, the pseudowire packet will feed directly the ingress network shared queue for that FC defined in the network-queue policy applied to the ingress of the MDA/FP.
2. When a pseudowire FC is redirected to use a policer in a named policer queue-group and the queue-group name exists but the policer-id is not defined in the queue-group template,
association is failed at the time the user associates the ingress context of a spoke-SPD to the named queue-group. In such a case, the pseudowire packet will feed directly the ingress network shared queue for that FC defined in the network-queue policy applied to the ingress of the MDA/FP.

3. When a pseudowire FC is redirected to use a policer in a named policer queue-group and the queue-group name exists and the policer-id is defined in the queue-group template, it is not required to check that an instance of that queue-group exists in all ingress FPs which have network IP interfaces. The handling of this is dealt with in the data path as follows:
   a When a pseudowire packet for that FC is received and an instance of the referenced queue-group name exists on that FP, the packet is processed by the policer and will then feed the per-FP ingress shared queues referred to as policer-output-queues.
   b When a pseudowire packet for that FC is received and an instance of the referenced queue-group name does not exist on that FP, the pseudowire packets will be fed directly into the corresponding ingress network shared queue for that FC defined in the network-queue policy applied to the ingress of the MDA/FP.

4. If a network QoS policy is applied to the ingress context of a pseudowire, any pseudowire FC which is not explicitly redirected in the network QoS policy will have the corresponding packets feed directly the ingress network shared queue for that FC defined in the network-queue policy applied to the ingress of the MDA/FP.

5. If no network QoS policy is applied to the ingress context of the pseudowire, then all packets of the pseudowire will feed:
   a the ingress network shared queue for the packet FC defined in the network-queue policy applied to the ingress of the MDA/FP. This is the default behavior.
   b a queue-group policer followed by the per-FP ingress shared queues referred to as policer-output-queues if the ingress context of the network IP interface from which the packet is received is redirected to a queue-group (csc-policing). The only exceptions to this behavior are for packets received from a IES/VPRN spoke interface and from an R-VPLS spoke-SPD, which is forwarded to the R-VPLS IP interface. In these two cases, the ingress network shared queue for the packet FC defined in the network-queue policy applied to the ingress of the MDA/FP is used.

When a pseudowire is redirected to use a policer queue-group, the classification of the packet for the purpose of FC and profile determination is performed according to default classification rule or the QoS filters defined in the ingress context of the network QoS policy applied to the pseudowire. This is true regardless of whether an instance of the named policer queue-group exists on the ingress FP on which the pseudowire packet is received. The user can apply a QoS filter matching the dot1.p in the VLAN tag corresponding to the Ethernet port encapsulation, the EXP in the outer label when the tunnel is an LSP, the DSCP in the IP header if the tunnel encapsulation is GRE, and the DSCP in the payload IP header if the user enabled the ler-use-dscp option and the pseudowire terminates in IES or VPRN service (spoke-interface).

When the policer queue-group name the pseudowire is redirected does not exist, the redirection command is failed. In this case, the packet classification is performed according to default classification rule or the QoS filters defined in the ingress context of the network QoS policy applied to the network IP interface on which the pseudowire packet is received.

The no version of this command removes the redirection of the pseudowire to the queue-group.
SDP Commands

Parameters

- **network-policy-id** — Specifies the network policy identification. The value uniquely identifies the policy on the system.
  - **Values** 1 — 65535

- **fp-redirect-group queue-group-name** — Specifies the name of the queue group template up to 32 characters in length.

- **ingress-instance instance-id** — Specifies the identification of a specific instance of the queue-group.
  - **Values** 1 — 16384

vc-label

**Syntax**

vc-label egress-vc-label
no vc-label [egress-vc-label]

**Context**

config>service>vprn>if>spoke-sdp>egress
config>service>vprn>red-if>spoke-sdp>egress

**Description**

This command configures the egress VC label.

**Parameters**

- **vc-label** — A VC egress value that indicates a specific connection.
  - **Values** 16 — 1048575

vc-label

**Syntax**

vc-label ingress-vc-label
no vc-label [ingress-vc-label]

**Context**

config>service>vprn>if>spoke-sdp>ingress
config>service>vprn>red-if>spoke-sdp>ingress

**Description**

This command configures the ingress VC label.

**Parameters**

- **vc-label** — A VC ingress value that indicates a specific connection.
  - **Values** 2048 — 18431

egress

**Syntax**

egress

**Context**

config>service>vprn>network-interface

**Description**

This command enables the context to configure egress network filter policies for the interface.

filter
Syntax  
```
filter ip ip-filter-id
no filter [ip ip-filter-id] [ipv6 ipv6-filter-id]
```

Context  
```
config>service>vprn>network-interface>egress
config>service>vprn>if>spoke-sdp>egress
config>service>vprn>if>spoke-sdp>ingress
config>service>vprn>red-if>spoke-sdp>ingress
config>service>vprn>red-if>spoke-sdp>egress
config>service>vprn>nw-if>egress
```

Description  
This command associates an IP filter policy with an ingress or egress Service Access Point (SAP) or IP interface. An IP filter policy can be associated with spoke SDPs. Filter policies control the forwarding and dropping of packets based on IP or MAC matching criteria.

The filter command is used to associate a filter policy with a specified ip-filter-id with an ingress or egress SAP. The ip-filter-id must already be defined before the filter command is executed. If the filter policy does not exist, the operation will fail and an error message returned.

In general, filters applied to SAPs (ingress or egress) apply to all packets on the SAP. One exception is non-IP packets are not applied to IP match criteria, so the default action in the filter policy applies to these packets.

The `no` form of this command removes any configured filter ID association with the SAP or IP interface. The filter ID itself is not removed from the system unless the scope of the created filter is set to local. To avoid deletion of the filter ID and only break the association with the service object, use scope command within the filter definition to change the scope to local or global. The default scope of a filter is local.

Parameters  
ip ip-filter-id — Specifies IP filter policy. The filter ID must already exist within the created IP filters.

Values  
```
1 — 65535
```

QOS  
```
Syntax  
```
qos network-policy-id port-redirect-group queue-group-name [instance instance-id]
no qos [network-policy-id]
```

Context  
```
configure>service>apipe>spoke-sdp>egress
configure>service>cpipe>spoke-sdp>egress
configure>service>epipe>spoke-sdp>egress
configure>service>fpipe>spoke-sdp>egress
configure>service>ipipe>spoke-sdp>egress
configure>service>vpl>spoke-sdp>egress
configure>service>vpls>mesh-sdp>egress
configure>service>pw-template>egress
configure>service>vprn>interface>spoke-sdp>egress
configure>service>ies>interface>spoke-sdp>egress
```

Description  
This command is used to redirect pseudowire packets to an egress port queue-group for the purpose of shaping.
The egress pseudowire shaping provisioning model allows the mapping of one or more pseudowires to the same instance of queues, or policers and queues, which are defined in the queue-group template.

Operationally, the provisioning model consists of the following steps:

1. Create an egress queue-group template and configure queues only or policers and queues for each FC that needs to be redirected.

2. Apply the queue-group template to the network egress context of all ports where there exists a network IP interface on which the pseudowire packets can be forwarded. This creates one instance of the template on the egress of the port. One or more instances of the same template can be created.

3. Configure FC-to-policer or FC-to-queue mappings together with the redirect to a queue-group in the egress context of a network QoS policy. No queue-group name is specified in this step, which means the same network QoS policy can redirect different pseudowires to different queue-group templates.

4. Apply this network QoS policy to the egress context of a spoke-SPD inside a service or to the egress context of a pseudowire template and specify the redirect queue-group name.

One or more spoke-SPDs can have their FCs redirected to use queues only or queues and policers in the same queue-group instance.

The following are the constraints and rules of this provisioning model:

1. When a pseudowire FC is redirected to use a queue or a policer and a queue in a queue-group and the queue-group name does not exist, the association is failed at the time the user associates the egress context of a spoke-SPD to the named queue-group. In such a case, the pseudowire packet will be fed directly to the corresponding egress queue for that FC used by the IP network interface on which the pseudowire packet is forwarded. This queue can be a queue-group queue, or the egress shared queue for that FC defined in the network-queue policy applied to the egress of this port. This is the existing implementation and default behavior for a pseudowire packet.

2. When a pseudowire FC is redirected to use a queue or a policer, and a queue in a queue-group and the queue-group name exists, but the policer-id and/or the queue-id is not defined in the queue-group template, the association is failed at the time the user associates the egress context of a spoke-SPD to the named queue-group. In such a case, the pseudowire packet will be fed directly to the corresponding egress queue for that FC used by the IP network interface the pseudowire packet is forwarded on.

3. When a pseudowire FC is redirected to use a queue, or a policer and a queue in a queue-group, and the queue-group name exists and the policer-id or policer-id plus queue-id exist, it is not required to check that an instance of that queue-group exists in all egress network ports which have network IP interfaces. The handling of this is dealt with in the data path as follows:
   a When a pseudowire packet for that FC is forwarded and an instance of the referenced queue-group name exists on that egress port, the packet is processed by the queue-group policer and will then be fed to the queue-group queue.
   b When a pseudowire packet for that FC is forwarded and an instance of the referenced queue-group name does not exist on that egress port, the pseudowire packet will be fed directly to the corresponding egress shared queue for that FC defined in the network-queue policy applied to the egress of this port.
4. If a network QoS policy is applied to the egress context of a pseudowire, any pseudowire FC, which is not explicitly redirected in the network QoS policy, will have the corresponding packets feed directly the corresponding the egress shared queue for that FC defined in the network-queue policy applied to the egress of this port.

When the queue-group name the pseudowire is redirected to exists and the redirection succeeds, the marking of the packet DEI/dot1.p/DSCP and the tunnel DEI/dot1.p/DSCP/EXP is performed; according to the relevant mappings of the (FC, profile) in the egress context of the network QoS policy applied to the pseudowire. This is true regardless, wether an instance of the queue-group exists or not on the egress port to which the pseudowire packet is forwarded. If the packet profile value changed due to egress child policer CIR profiling, the new profile value is used to mark the packet DEI/dot1.p and the tunnel DEI/dot1.p/EXP, but the DSCP is not modified by the policer operation.

When the queue-group name the pseudowire is redirected does not exist, the redirection command is failed. In this case, the marking of the packet DEI/dot1.p/DSCP and the tunnel DEI/dot1.p/DSCP/EXP fields is performed according to the relevant commands in the egress context of the network QoS policy applied to the network IP interface to which the pseudowire packet is forwarded.

The no version of this command removes the redirection of the pseudowire to the queue-group.

**Parameters**

- **network-policy-id** — Specifies the network policy identification. The value uniquely identifies the policy on the system.
  - **Values** 1 — 65535

- **port-redirect-group queue-group-name** — This optional parameter specifies that the queue-group-name will be used for all egress forwarding class redirections within the network QoS policy ID. The specified queue-group-name must exist as a port egress queue group on the port associated with the IP interface.

- **egress-instance instance-id** — Specifies the identification of a specific instance of the queue-group.
  - **Values** 1 — 16384
Interface Commands

interface

Syntax

interface ip-int-name
no interface ip-int-name

Context
config>service>vprn

Description
This command creates a logical IP routing interface for a Virtual Private Routed Network (VPRN). Once created, attributes like an IP address and service access point (SAP) can be associated with the IP interface.

The interface command, under the context of services, is used to create and maintain IP routing interfaces within VPRN service IDs. The interface command can be executed in the context of an VPRN service ID. The IP interface created is associated with the service core network routing instance and default routing table. The typical use for IP interfaces created in this manner is for internet access.

Interface names are case sensitive and must be unique within the group of defined IP interfaces defined for config router interface and config service vprn interface. Interface names must not be in the dotted decimal notation of an IP address. For example, the name “1.1.1.1” is not allowed, but “int-1.1.1.1” is allowed. Show commands for router interfaces use either interface names or the IP addresses. Use unique IP address values and IP address names to maintain clarity. It could be unclear to the user if the same IP address and IP address name values are used. Although not recommended, duplicate interface names can exist in different router instances.

The available IP address space for local subnets and routes is controlled with the config router service-prefix command. The service-prefix command administers the allowed subnets that can be defined on service IP interfaces. It also controls the prefixes that may be learned or statically defined with the service IP interface as the egress interface. This allows segmenting the IP address space into config router and config service domains.

When a new name is entered, a new logical router interface is created. When an existing interface name is entered, the user enters the router interface context for editing and configuration.

By default, there are no default IP interface names defined within the system. All VPRN IP interfaces must be explicitly defined. Interfaces are created in an enabled state.

The no form of this command removes IP the interface and all the associated configuration. The interface must be administratively shutdown before issuing the no interface command.

For VPRN services, the IP interface must be shutdown before the SAP on that interface may be removed. VPRN services do not have the shutdown command in the SAP CLI context. VPRN service SAPs rely on the interface status to enable and disable them.

Parameters

ip-int-name — Specifies the name of the IP interface. Interface names must be unique within the group of defined IP interfaces for config router interface and config service vprn interface commands. An interface name cannot be in the form of an IP address. Interface names can be from 1 to 32 alphanumeric characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.
active-cpm-protocols

**Syntax**  
[no] active-cpm-protocols

**Context**  
config>service>vprn>if

**Description**  
This command enables CPM protocols on this interface.

address

**Syntax**  
address ip-address/mask | ip-address netmask | broadcast [all-ones | host-ones]  
no address

**Context**  
config>service>vprn>if  
config>service>vprn>nw-if

**Description**  
Assigns an IP address, IP subnet, and broadcast address format to a VPRN IP router interface. Only one IP address can be associated with an IP interface.

An IP address must be assigned to each VPRN IP interface. An IP address and a mask are used together to create a local IP prefix. The defined IP prefix must be unique within the context of the routing instance. It cannot overlap with other existing IP prefixes defined as local subnets on other IP interfaces in the same routing context within the .

The local subnet that the address command defines must be part of the services address space within the routing context using the config router service-prefix command. The default is to disallow the complete address space to services. Once a portion of the address space is allocated as a service prefix, that portion can be made unavailable for IP interfaces defined within the config router interface CLI context for network core connectivity with the exclude option in the config router service-prefix command.

The IP address for the interface can be entered in either CIDR (Classless Inter-Domain Routing) or traditional dotted decimal notation. The show commands display CIDR notation and is stored in configuration files.

By default, no IP address or subnet association exists on an IP interface until it is explicitly created. Use the no form of this command to remove the IP address assignment from the IP interface. When the no address command is entered, the interface becomes operationally down.
The operational state is a read-only variable and the only controlling variables are the address and admin states. The address and admin states are independent and can be set independently. If an interface is in an administratively up state and an address is assigned, it becomes operationally up and the protocol interfaces and the MPLS LSPs associated with that IP interface will be reinitialized.

*ip-address* — The IP address of the IP interface. The *ip-address* portion of the `address` command specifies the IP host address that will be used by the IP interface within the subnet. This address must be unique within the subnet and specified in dotted decimal notation. Allowed values are IP addresses in the range 1.0.0.0 – 223.255.255.255 (with support of /31 subnets).

* / * — The forward slash is a parameter delimiter and separates the *ip-address* portion of the IP address from the mask that defines the scope of the local subnet. No spaces are allowed between the *ip-address*, the “/” and the *mask-length* parameter. If a forward slash is not immediately following the *ip-address*, a dotted decimal mask must follow the prefix.

*mask-length* — The subnet mask length when the IP prefix is specified in CIDR notation. When the IP prefix is specified in CIDR notation, a forward slash (/) separates the *ip-address* from the *mask-length* parameter. The mask length parameter indicates the number of bits used for the network portion of the IP address; the remainder of the IP address is used to determine the host portion of the IP address. Allowed values are integers in the range 0 – 30. Note that a mask length of 32 is reserved for system IP addresses.

*mask* — The subnet mask in dotted decimal notation. When the IP prefix is not specified in CIDR notation, a space separates the *ip-address* from a traditional dotted decimal mask. The *mask* parameter indicates the complete mask that will be used in a logical ‘AND’ function to derive the local subnet of the IP address. Allowed values are dotted decimal addresses in the range 128.0.0.0 – 255.255.255.252. Note that a mask of 255.255.255.255 is reserved for system IP addresses.

*broadcast* — The optional *broadcast* parameter overrides the default broadcast address used by the IP interface when sourcing IP broadcasts on the IP interface. If no broadcast format is specified for the IP address, the default value is *host-ones* which indicates a subnet broadcast address. Use this parameter to change the broadcast address to *all-ones* or revert back to a broadcast address of *host-ones*.

The broadcast format on an IP interface can be specified when the IP address is assigned or changed.

This parameter does not affect the type of broadcasts that can be received by the IP interface. A host sending either the local broadcast (*all-ones*) or the valid subnet broadcast address (*host-ones*) will be received by the IP interface.

**Default** host-ones
**all-ones** — The **all-ones** keyword following the **broadcast** parameter specifies the broadcast address used by the IP interface for this IP address will be 255.255.255.255, also known as the local broadcast.

**host-ones** — The **host-ones** keyword following the **broadcast** parameter specifies that the broadcast address used by the IP interface for this IP address will be the subnet broadcast address. This is an IP address that corresponds to the local subnet described by the **ip-address** and the **mask-length** or **mask** with all the host bits set to binary one. This is the default broadcast address used by an IP interface.

The **broadcast** parameter within the **address** command does not have a negate feature, which is usually used to revert a parameter to the default value. To change the **broadcast** type to **host-ones** after being changed to **all-ones**, the **address** command must be executed with the **broadcast** parameter defined.

---

**allow-directed-broadcasts**

**Syntax**  
[no] allow-directed-broadcasts

**Context**  
config>service>vprn>if  
config>service>vprn>if>ipv6  
config>service>vprn>nw-if

**Description**  
This command controls the forwarding of directed broadcasts out of the IP interface.

A directed broadcast is a packet received on a local router interface destined for the subnet broadcast address on another IP interface. The **allow-directed-broadcasts** command on an IP interface enables or disables the transmission of packets destined to the subnet broadcast address of the egress IP interface.

When enabled, a frame destined to the local subnet on this IP interface will be sent as a subnet broadcast out this interface. Care should be exercised when allowing directed broadcasts as it is a well-known mechanism used for denial-of-service attacks.

When disabled, directed broadcast packets discarded at this egress IP interface will be counted in the normal discard counters for the egress SAP.

By default, directed broadcasts are not allowed and will be discarded at this egress IP interface.

The **no** form of this command disables the forwarding of directed broadcasts out of the IP interface.

**Default**  
no allow-directed-broadcasts — Directed broadcasts are dropped.

---

**bfd**

**Syntax**  
bfd transmit-interval [receive receive-interval] [multiplier multiplier] [echo-receive echo-interval]  
no bfd

**Context**  
config>service>vprn>if  
config>service>vprn>if>ipv6  
config>service>vprn>nw-if
Description

This command specifies the BFD parameters for the associated IP interface. If no parameters are defined the default value are used.

The multiplier specifies the number of consecutive BFD messages that must be missed from the peer before the BFD session state is changed to down and the upper level protocols (OSPF, IS-IS, BGP or PIM) is notified of the fault.

The no form of the command removes BFD from the associated IGP protocol adjacency.

Important notes: On the SR-OS, the transmit-interval, receive receive-interval, and echo-receive echo-interval values can only be modified to a value less than 100 when:

1. The type cpm-np option is explicitly configured.
2. The service is shut down (shutdown)
3. The interval is specified 10 — 100000.
4. The service is re-enabled (no shutdown)

To remove the type cpm-np option, re-issue the bfd command without specifying the type parameter.

Default

no bfd

Parameters

transmit-interval — Sets the transmit interval for the BFD session.

Values 10 — 100000
Default 100

receive receive-interval — Sets the receive interval for the BFD session.

Values 10 — 100000
Default 100

multiplier multiplier — Set the multiplier for the BFD session.

Values 3 — 20
Default 3

echo-receive echo-interval — Sets the minimum echo receive interval, in milliseconds, for the BFD session.

Values 100 — 100000
Default 100

cflowd

Syntax cflowd {acl | interface} [direction]
no cflowd

Context config>service>vprn>if
config>service>vprn>nw-if

Description This command enables cflowd to collect traffic flow samples through a router for analysis.
cflowd is used for network planning and traffic engineering, capacity planning, security, application and user profiling, performance monitoring, usage-based billing, and SLA measurement. When cflowd is enabled at the interface level, all packets forwarded by the interface are subjected to analysis according to the cflowd configuration.

If cflowd is enabled without either egress-only or both specified or with the ingress-only keyword specified, then only ingress sampling will be enabled on the associated IP interface.

**Default**
no cflowd  

**Parameters**
- **acl** — cflowd configuration associated with a filter.  
- **interface** — cflowd configuration associated with an IP interface.  
- **direction** — Specifies the direction to collect traffic flow samples.
  
  **Values**
  - **ingress-only** — Enables ingress sampling only on the associated interface.  
  - **egress-only** — Enables egress sampling only on the associated interface.  
  - **both** — Enables both ingress and egress cflowd sampling.

### dist-cpu-protection

**Syntax**
dist-cpu-protection policy-name  
no dist-cpu-protection  

**Context**
config>service>vprn>if>nw-if  

**Description**
This command assigns a Distributed CPU Protection (DCP) policy to the network interface. Only a valid created DCP policy can be assigned to a SAP or a network interface (note that this rule does not apply to templates such as an msap-policy).

**Default**
no dist-cpu-protection

### delayed-enable

**Syntax**
delayed-enable seconds  
no delayed-enable  

**Context**
config>service>vprn>if  

**Description**
This command creates a delay to make the interface operational by the specified number of seconds. The value is used whenever the system attempts to bring the interface operationally up.

**Parameters**
- **seconds** — Specifies a delay, in seconds, to make the interface operational.

  **Values**
  - 1 — 1200

### ip-mtu

**Syntax**
ip-mtu octets
no ip-mtu

Context config>service>vprn>if
Description This command configures the IP maximum transmit unit (packet) for this interface. The no form of the command returns the default value.
Default no ip-mtu

ipcp

Syntax ipcp
Context config>service>vprn>if
Description This command creates allows access to the IPCP context within the interface configuration. Within this context, IPCP extensions can be configured to define such things as the remote IP address and DNS IP address to be signaled via IPCP on the associated PPP interface.
This command is only applicable if the associated SAP/port is a PPP/MLPPP interface.
Default none

dns

Syntax dns ip-address [secondary ip-address]
dns secondary ip-address
no dns [ip-address] [secondary ip-address]
Context config>service>vprn>if/ipcp
Description This command defines the dns address(es) to be assigned to the far-end of the associated PPP/MLPPP link via IPCP extensions.
This command is only applicable if the associated SAP/port is a PPP/MLPPP interface with an IPCP encapsulation.
The no form of the command deletes either the specified primary DNS address, secondary DNS address or both addresses from the IPCP extension peer-ip-address configuration.
Default no dns
Parameters

Parameters

Parameters

Parameters

Parameters

Parameters

Parameters

Parameters

Parameters

Parameters

Parameters

Parameters

Parameters
Virtual Private Routed Network Services

Syntax  peer-ip-address ip-address
        no peer-ip-address

Context  config>service>vprn>if>ipcp

Description  This command defines the remote IP address to be assigned to the far-end of the associated PPP/MLPPP link via IPCP extensions.

This command is only applicable if the associated SAP/port is a PPP/MLPPP interface with an IPCP encapsulation.

The interface must be shut down to modify the IPCP configuration.

The no form of the command deletes the IPCP extension peer-ip-address configuration.

Default  no peer-ip-address (0.0.0.0)

Parameters  ip-address — Specifies a unicast IPv4 address to be signaled to the far-end of the associated PPP/MLPPP link by IPCP extensions.

ipv6

Syntax  [no] ipv6

Context  config>service>vprn>if

Description  This command configures an IPv6 interface.

address

Syntax  address ipv6-address/mask [eui-64] [preferred]
        no address ipv6-address/prefix-length

Context  config>service>vprn>if>ipv6

Description  This command assigns an IPv6 address to the VPRN interface.

Parameters  ipv6-address/prefix-length — Specifies the IPv6 address on the interface.

Values  ipv6-address/prefix: ipv6-address x:x:x:x:x:x:x (eight 16-bit pieces)
        x:x:x:x:x:d.d.d
        x [0 — FFFF]H
        d [0 — 255]D

        prefix-length 1 — 128

eui-64 — When the eui-64 keyword is specified, a complete IPv6 address from the supplied prefix and 64-bit interface identifier is formed. The 64-bit interface identifier is derived from MAC address on Ethernet interfaces. For interfaces without a MAC address, for example ATM interfaces, the Base MAC address of the chassis is used.

preferred — specifies that the IPv6 address is the preferred IPv6 address for this interface. Preferred address is an address assigned to an interface whose use by upper layer protocols is unrestricted.
Preferred addresses maybe used as the source (or destination) address of packets sent from (or to) the interface. Preferred address doesn’t go through the DAD process.

**dhcp6-relay**

**Syntax**

[no] dhcp6-relay

**Context**

config>service>vprn>if>ipv6

**Description**

This command configures DHCPv6 relay parameters for the VPRN interface.

**dhcp6-server**

**Syntax**

[no] dhcp6-server

**Context**

config>service>vprn>if>ipv6

**Description**

This command configures DHCPv6 server parameters for the VPRN interface.

**icmp6**

**Syntax**

icmp6

**Context**

config>service>vprn>if>ipv6

**Description**

This command configures ICMPv6 for the interface.

**local-proxy-nd**

**Syntax**

[no] local-proxy-nd

**Context**

config>service>vprn>if>ipv6

**Description**

This command enables or disables neighbor discovery on the interface.

**neighbor**

**Syntax**

neighbor ipv6-address mac-address

no neighbor ipv6-address

**Context**

config>service>vprn>if>ipv6

**Description**

This command configures IPv6-to-MAC address mapping on the interface.

**Parameters**

ipv6-address — Specifies the IPv6 address on the interface.
**Values**

- ipv6-address  
  - x:x:x:x:x:x:x (eight 16-bit pieces)
  - x:x:x:x:d.d.d
  - x [0 — FFFF]H
  - d [0 — 255]D

**mac-address** — Specifies the 48-bit MAC address for the static ARP in the form aa:bb:cc:dd:ee:ff or aa-bb-cc-dd-ee-ff where aa, bb, cc, dd, ee and ff are hexadecimal numbers. Allowed values are any non-broadcast, non-multicast MAC and non-IEEE reserved MAC addresses.

**proxy-nd-policy**

**Syntax**

```plaintext
proxy-nd-policy policy-name [policy-name...(up to 5 max)]
no proxy-nd-policy
```

**Context**

```
config>service>vprn>if>ipv6
```

**Description**

This command configures a proxy neighbor discovery policy for the interface.

**Parameters**

- `policy-name` — Specifies the existing policy name(s).

**local-proxy-arp**

**Syntax**

```plaintext
[no] local-proxy-arp
```

**Context**

```
config>service>vprn>if
config>service>vprn>nw-if
```

**Description**

This command enables local proxy ARP. When local proxy ARP is enabled on an IP interface, the system responds to all ARP requests for IP addresses belonging to the subnet with its own MAC address, and thus will become the forwarding point for all traffic between hosts in that subnet. When local-proxy-arp is enabled, ICMP redirects on the ports associated with the service are automatically blocked.

**Default**

no local-proxy-arp

**loopback**

**Syntax**

```plaintext
[no] loopback
```

**Context**

```
config>service>vprn>if
config>service>vprn>nw-if
```

**Description**

This command specifies that the associated interface is a loopback interface that has no associated physical interface. As a result, the associated interface cannot be bound to a SAP.

When using mtrace/mstat in a Layer 3 VPN context then the configuration for the VPRN should have a loopback address configured which has the same address as the core instance's system address (BGP next-hop).
Interface Commands

Default  None

mac

Syntax  [no] mac ieee-mac-address

Context  config>service>vprn>if  
         config>service>vprn>if>vrrp  
         config>service>vprn>nw-if

Description  This command assigns a specific MAC address to a VPRN IP interface.

The no form of this command returns the MAC address of the IP interface to the default value.

Default  The physical MAC address associated with the Ethernet interface that the SAP is configured on.

Parameters  ieee-mac-address — Specifies the 48-bit MAC address for the static ARP in the form
             aa:bb:cc:dd:ee:ff or aa-bb-cc-dd-ee-ff where aa, bb, cc, dd, ee and ff are hexadecimal numbers.
             Allowed values are any non-broadcast, non-multicast MAC and non-IEEE reserved MAC addresses.

ntp-broadcast

Syntax  [no] ntp-broadcast

Context  config>service>vprn>nw-if

Description  This command enables receiving of NTP/SNTP broadcasts on the interface.

monitor-oper-group

Syntax  monitor-oper-group name
        no monitor-oper-group

Context  config>service>vprn>if

Description  This command specifies the operational group to be monitored by the object under which it is configured. The oper-group name must be already configured under the config>service context before its name is referenced in this command.

The no form of the command removes the association from the configuration.

Default  no monitor-oper-group

Parameters  name — Specifies a character string of maximum 32 ASCII characters identifying the group instance.

proxy-arp
Virtual Private Routed Network Services

Syntax   [no] proxy-arp
Context   config>service>vprn>nw-if
Description This command enables proxy ARP on the interface.
Default   no proxy-arp

proxy-arp-policy

Syntax   [no] proxy-arp-policy policy-name [policy-name...(up to 5 max)]
Context   config>service>vprn>if
cfg>service>vprn>nw-if
Description This command enables a proxy ARP policy for the interface.
The no form of this command disables the proxy ARP capability.
Default   no proxy-arp
Parameters policy-name — The export route policy name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.
The specified name(s) must already be defined.

ptp-hw-assist

Syntax   [no] ptp-hw-assist
Context   config>service>vprn>if
Description This command configures the 1588 port based timestamping assist function for the interface. This capability is supported on a specific set of hardware. The command may be blocked if not all hardware has the required level of support.
If the SAP configuration of the interface is removed, the ptp-hw-assist configuration will be removed.
If the IPv4 address configuration of the interface is removed, the ptp-hw-assist configuration will be removed.
Only one interface per physical port can have ptp-hw-assist enabled.
Default   no ptp-hw-assist

qos-route-lookup

Syntax   qos-route-lookup [source | destination]
no qos-route-lookup
Context   config>service>vprn>if
Description
This command enables QoS classification of the ingress IP packets on an interface based on the QoS information associated with routes in the forwarding table.

If the optional destination parameter is specified and the destination address of an incoming IP packet matches a route with QoS information the packet is classified to the fc and priority associated with that route, overriding the fc and priority/profile determined from the sap-ingress or network qos policy associated with the IP interface. If the destination address of the incoming packet matches a route with no QoS information the fc and priority of the packet remain as determined by the sap-ingress or network QoS policy.

If the optional source parameter is specified and the source address of an incoming IP packet matches a route with QoS information the packet is classified to the fc and priority associated with that route, overriding the fc and priority/profile determined from the sap-ingress or network qos policy associated with the IP interface. If the source address of the incoming packet matches a route with no QoS information the fc and priority of the packet remain as determined by the sap-ingress or network QoS policy.

If neither the optional source or destination parameter is present, then the default is destination address matching.

The functionality enabled by the qos-route-lookup command can be applied to IPv4 packets or IPv6 packets on an interface, depending on whether it is present at the interface context (applies to IPv4) or the interface>ipv6 context (applies to IPv6). The ability to specify source address based QoS lookup is not supported for IPv6.

The no form of the command reverts to the default.

Default
destination

Parameters
source — Enables QoS classification of incoming IP packets based on the source address matching a route with QoS information.

destination — Enables QoS classification of incoming IP packets based on the destination address matching a route with QoS information.

redundant-interface

Syntax redundant-interface red-ip-int-name
no redundant-interface

Context config>service>vprn

Description This command configures a redundant interface used for dual homing.

Parameters red-ip-int-name — Specifies the redundant IP interface name.

remote-proxy-arp

Syntax [no] remote-proxy-arp

Context config>service>vprn>if
Virtual Private Routed Network Services

config>service>vprn>nw-if

**Description**
This command enables remote proxy ARP on the interface.

Remote proxy ARP is similar to proxy ARP. It allows the router to answer an ARP request on an interface for a subnet that is not provisioned on that interface. This allows the router to forward to the other subnet on behalf of the requester. To distinguish remote proxy ARP from local proxy ARP, local proxy ARP performs a similar function but only when the requested IP is on the receiving interface.

**Default**
no remote-proxy-arp

**secondary**

**Syntax**
secondary {ip-address/mask | ip-address netmask} [broadcast all-ones | host-ones] [igp-inhibit]
no secondary {ip-address/mask | ip-address netmask}

**Context**
cfg>service>vprn>if
cfg>service>vprn>nw-if

**Description**
This command assigns ansecondary IP address/IP subnet/broadcast address format to the interface.

**Default**
none

**Parameters**
- `ip-address` — The IP address of the IP interface. The `ip-address` portion of the `address` command specifies the IP host address that will be used by the IP interface within the subnet. This address must be unique within the subnet and specified in dotted decimal notation. Allowed values are IP addresses in the range 1.0.0.0 – 223.255.255.255 (with support of /31 subnets).

- `mask` — The subnet mask in dotted decimal notation. When the IP prefix is not specified in CIDR notation, a space separates the `ip-address` from a traditional dotted decimal mask. The `mask` parameter indicates the complete mask that will be used in a logical ‘AND’ function to derive the local subnet of the IP address. Allowed values are dotted decimal addresses in the range 128.0.0.0 – 255.255.255.252. Note that a mask of 255.255.255.255 is reserved for system IP addresses.

- `netmask` — Specifies a string of 0s and 1s that mask or screen out the network part of an IP address so that only the host computer part of the address remains.

- `broadcast` — The optional `broadcast` parameter overrides the default broadcast address used by the IP interface when sourcing IP broadcasts on the IP interface. If no broadcast format is specified for the IP address, the default value is `host-ones` which indicates a subnet broadcast address. Use this parameter to change the broadcast address to `all-ones` or revert back to a broadcast address of `host-ones`.

The broadcast format on an IP interface can be specified when the IP address is assigned or changed. This parameter does not affect the type of broadcasts that can be received by the IP interface. A host sending either the local broadcast (`all-ones`) or the valid subnet broadcast address (`host-ones`) will be received by the IP interface. *(Default: host-ones)*

- `all-ones` — The `all-ones` keyword following the `broadcast` parameter specifies the broadcast address used by the IP interface for this IP address will be 255.255.255.255, also known as the local broadcast.
**host-ones** — The **host-ones** keyword following the **broadcast** parameter specifies that the broadcast address used by the IP interface for this IP address will be the subnet broadcast address. This is an IP address that corresponds to the local subnet described by the *ip-address* and the *mask-length* or *mask* with all the host bits set to binary one. This is the default used by an IP interface. The **broadcast** parameter within the **address** command does not have a negate feature, which is usually used to revert a parameter to the default value. To change the **broadcast** type to **host-ones** after being changed to **all-ones**, the **address** command must be executed with the **broadcast** parameter defined.

**igp-inhibit** — The optional **igp-inhibit** parameter signals that the given secondary IP interface should not be recognized as a local interface by the running IGP. For OSPF and IS-IS, this means that the specified secondary IP interfaces will not be injected and used as passive interfaces and will not be advertised as internal IP interfaces into the IGP’s link state database. For RIP, this means that these secondary IP interfaces will not source RIP updates.

---

### static-arp

**Syntax**

```
static-arp ieee-mac-address unnumbered
no static-arp unnumbered
```

**Context**

```
config>service>vprn>if
config>service>vprn>nw-if
```

**Description**

This command configures a static address resolution protocol (ARP) entry associating a subscriber IP address with a MAC address for the core router instance. This static ARP will appear in the core routing ARP table. A static ARP can only be configured if it exists on the network attached to the IP interface. If an entry for a particular IP address already exists and a new MAC address is configured for the IP address, the existing MAC address will be replaced with the new MAC address.

The **no** form of this command removes a static ARP entry.

**Default**

none

**Parameters**

- **ip-address** — Specifies the IP address for the static ARP in IP address dotted decimal notation.
- **ieee-mac-address** — Specifies the 48-bit MAC address for the static ARP in the form
  
  `aa:bb:cc:dd:ee:ff` or `aa-bb-cc-dd-ee-ff` where `aa`, `bb`, `cc`, `dd`, `ee` and `ff` are hexadecimal numbers. Allowed values are any non-broadcast, non-multicast MAC and non-IEEE reserved MAC addresses.

  **unnumbered** — Specifies the static ARP MAC for an unnumbered interface. Unnumbered interfaces support dynamic ARP. Once this command is configured, it overrides any dynamic ARP.

---

### static-tunnel-redundant-next-hop

**Syntax**

```
static-tunnel-redundant-next-hop ip-address
no static-tunnel-redundant-next-hop
```

**Context**

```
config>service>vprn>if
```

**Description**

This command specifies redundant next-hop address on public or private IPsec interface (with public...
or private tunnel-sap) for static IPsec tunnel. The specified next-hop address will be used by standby node to shunt traffic to master in case of it receives them.

The next-hop address will be resolved in routing table of corresponding service.

The no form of the command removes the address from the interface configuration.

**Default** none

**Parameters**
- `ip-address` — Specifies the static ISA tunnel redundant next-hop address.

---

**strip-label**

**Syntax**

```text
[no] strip-label
```

**Context**

```
config>service>vprn>nw-if
```

**Description**

This command forces packets to be stripped of all (max 5) MPLS labels before the packets are handed over for possible filter (PBR) processing.

If the packets do not have an IP header ediantely following the MPLS label stack after the strip, they are discarded. Only MPLS encapsulated IP, IGP shortcuts and VPRN over MPLS packets will be processed.

This command is only supported on:

- Optical ports
- IOM3-XP cards
- Null/Dot1q encap
- Network ports
- IPv4

The **no** form removes the strip-label command.

In order to associate an interface that is configured with the strip-label parameter with a port, the port must be configured as single-fiber for the command to be valid.

**Default** no strip-label

---

**teid-load-balancing**

**Syntax**

```text
[no] teid-load-balancing
```

**Context**

```
config>service>vprn>interface
config>service>vprn>nw-if
```

**Description**

This command enables inclusion of TEID in hashing for GTP-U/C encapsulates traffic for GTPv1/GTPv2. The **no** form of this command ignores TEID in hashing.

**Default** disabled
Interface Commands

tos-marking-state

**Syntax**
```
tos-marking-state {trusted | untrusted}
nos tos-marking-state
```

**Context**
```
config>service>vprn>nw-if
```

**Description**
This command is used to alter the default trusted state to a non-trusted state. When unset or reverted to the trusted default, the ToS field will not be remarked by egress network IP interfaces unless the egress network IP interface has the remark-trusted state set, in which case the egress network interface treats all VPRN and network IP interface as untrusted.

When the ingress interface is set to untrusted, all egress network IP interfaces will remark IP packets received on the network interface according to the egress marking definitions on each network interface. The egress network remarking rules also apply to the ToS field of IP packets routed using IGP shortcuts (tunneled to a remote next-hop). However, the tunnel QoS markings are always derived from the egress network QoS definitions.

Egress marking and remarking is based on the internal forwarding class and profile state of the packet once it reaches the egress interface. The forwarding class is derived from ingress classification functions. The profile of a packet is either derived from ingress classification or ingress policing.

The default marking state for network IP interfaces is trusted. This is equivalent to declaring no tos-marking-state on the network IP interface. When undefined or set to tos-marking-state trusted, the trusted state of the interface will not be displayed when using show config or show info unless the detail parameter is given. The `save config` command will not store the default tos-marking-state trusted state for network IP interfaces unless the detail parameter is also specified.

The `no tos-marking-state` command is used to restore the trusted state to a network IP interface. This is equivalent to executing the tos-marking-state trusted command.

**Default**
trusted

**Parameters**
- `trusted` — The default prevents the ToS field to not be remarked by egress network IP interfaces unless the egress network IP interface has the remark-trusted state set.
- `untrusted` — Specifies that all egress network IP interfaces will remark IP packets received on the network interface according to the egress marking definitions on each network interface.

unnumbered

**Syntax**
```
unnumbered [ip-int-name | ip-address]
nos unnumbered
```

**Context**
```
config>service>vprn>if
config>service>vprn>nw-if
```

**Description**
This command configures the interface as an unnumbered interface. Unnumbered IP interface is supported on a Sonet/SDH access port with the PPP, ATM, or Frame Relay encapsulation. It is not supported on a TDM port or channel.
Parameters  

- **ip-int-name** — Specifies the name of an IP interface. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.
- **ip-address** — Specifies an IP address.

QoS

Syntax  

```
qos network-policy-id port-redirect-group queue-group-name egress-instance instance-id fp-redirect-group queue-group-name ingress-instance instance-id
```

Context  

```
config>service>vprn>nw-if
```

Description  

This command associates a network Quality of Service (QoS) policy with a network IP interface. Only one network QoS policy can be associated with an IP interface at one time. Attempts to associate a second QoS policy return an error.

Associating a network QoS policy with a network interface is useful for the following purposes:

- To apply classification rules for determining the forwarding-class and profile of ingress packets on the interface.
- To associate ingress packets on the interface with a queue-group instance applied to the ingress context of the interface’s forwarding plane (FP). (This is only applicable to interfaces on IOM3 and later cards.) The referenced ingress queue-group instance may have policers defined in order to rate limit ingress traffic on a per-forwarding class (and forwarding type: unicast vs. multicast) basis.
- To perform 802.1p, DSCP, IP precedence and/or MPLS EXP re-marking of egress packets on the interface.
- To associate egress packets on the interface with a queue-group instance applied to the egress context of the interface’s port. The referenced egress queue-group instance may have policers and/or queues defined in order to rate limit egress traffic on a per-forwarding class basis.

The no form of the command removes the network QoS policy association from the network IP interface, and the QoS policy reverts to the default.

Default  

```
oqos
```

Parameters  

- **network-policy-id** — An existing network policy ID to associate with the IP interface.
  - **Values**  
    - 1 — 65535
- **port-redirect-group queue-group-name** — This optional parameter specifies the egress queue-group used for all egress forwarding-class redirections specified within the network QoS policy ID. The specified queue-group-name must exist as an egress queue group applied to the egress context of the port associated with the IP interface.
- **egress-instance instance-id** — Since multiple instances of the same egress queue-group can be applied to the same port this optional parameter is used to specify which particular instance to associate with this particular network IP interface.
  - **Values**  
    - 1 — 16384
Interface Commands

**fp-redirect-group queue-group-name** — This optional parameter specifies the ingress queue-group used for all ingress forwarding-class redirections specified within the network QoS policy ID. The specified queue-group-name must exist as an ingress queue group applied to the ingress context of the forwarding plane associated with the IP interface.

**ingress-instance instance-id** — Since multiple instances of the same ingress queue-group can be applied to the same forwarding plane this parameter is required to specify which particular instance to associate with this particular network IP interface.

Values 1 — 16384

**urpf-check**

**Syntax**

```
[no] urpf-check
```

**Context**

```
config>service>vprn>if
config>service>vprn>nw-if
config>service>vprn>interface>ipv6
```

**Description**

This command enables unicast RPF (uRPF) check on this interface.

The **no** form of the command disables unicast RPF (uRPF) Check on this interface.

**Default** disabled

**mode**

**Syntax**

```
mode {strict | loose | strict-no-ecmp}
no mode
```

**Context**

```
config>service>vprn>if>urfp-check
config>service>vprn>nw-if>urfp-check
```

**Description**

This command specifies the mode of unicast RPF check.

The **no** form of the command reverts to the default (strict) mode.

**Default** strict

**Parameters**

**strict** — When specified, uRPF checks whether incoming packet has a source address that matches a prefix in the routing table, and whether the interface expects to receive a packet with this source address prefix.

**loose** — In **loose** mode, uRPF checks whether incoming packet has source address with a corresponding prefix in the routing table. However, the loose mode does not check whether the interface expects to receive a packet with a specific source address prefix. This object is valid only when **urpf-check** is enabled.

**strict-no-ecmp** — When a packet is received on an interface in this mode and the SA matches an ECMP route the packet is dropped by uRPF.
egress

Syntax  egress
Context  config>service>vprn>nw-if
Description  This command enables the context to configure egress network filter policies for the interface.

dynamic-tunnel-redundant-next-hop

Syntax  dynamic-tunnel-redundant-next-hop ip-address
         no dynamic-tunnel-redundant-next-hop
Context  config>service>vprn>if
Description  This command specifies redundant next-hop address on public or private IPsec interface (with public or private tunnel-sap) for dynamic IPsec tunnel. The specified next-hop address will be used by standby node to shunt traffic to master in case of it receives them.
            The next-hop address will be resolved in routing table of corresponding service.
Default  none
Description  ip-address — Specifies the dynamic ISA tunnel redundant next-hop address.

egr-ip-load-balancing

Syntax  egr-ip-load-balancing {src-ip | dst-ip}
         no egr-ip-load-balancing
Context  config>service>vprn>if
         config>service>vprn>if>nw-if
Description  This command specifies whether to include source address or destination address or both in LAG/ECMP hash on IP interfaces. Additionally, when l4-load-balancing is enabled the command applies also to inclusion of source/destination port in the hash inputs.
            The no form of this command includes both source and destination parameters.
Default  no egr-ip-load-balancing

use-arp

Syntax  [no] use-arp
Context  config>service>vprn>if>dhcp
Description  This command enables the use of ARP to determine the destination hardware address.
            The no form of the command disables the use of ARP to determine the destination hardware address.
Parameters

**src-ip** — Specifies using source address and (if l4-load balancing is enabled) source port in the hash, ignore destination address/port.

**dst-ip** — Specifies using destination address and (if l4-load balancing is enabled) destination port in the hash, ignore source address/port.

enable-ingress-stats

**Syntax**

```
[no] enable-ingress-stats
```

**Context**

```
config>router>interface
config>service>ies >interface
config>service>vprn>interface
config>service>ies>sub-if>grp-if
config>service>vprn>sub-if>grp-if
```

**Description**

This command enables the collection of ingress interface IP stats. This command is only applicable to IP statistics, and not to uRPF statistics.

If enabled, the following statistics are collected:

- IPv4 offered packets
- IPv4 offered octets
- IPv6 offered packets
- IPv6 offered octets

Note that octet statistics for IPv4 and IPv6 bytes at IP interfaces include the layer 2 frame overhead.

**Default**

no enable-ingress-stats

enable-mac-accounting

**Syntax**

```
[no] enable-mac-accounting
```

**Context**

```
config>service>vprn>if
```

**Description**

This command enables MAC accounting functionality on this interface.

The **no** form of the command disables MAC accounting functionality on this interface.

host-connectivity-verify

**Syntax**

```
host-connectivity-verify [interval interval] [action {remove | alarm}]
```

**Context**

```
config>service>vprn>if>sap
```

**Description**

This command enables subscriber host connectivity verification on a given SAP within a service.
This tool will periodically scan all known hosts (from dhcp-state) and perform a UC ARP request. The subscriber host connectivity verification will maintain state (connected vs. not-connected) for all hosts.

**Default**

no host-connectivity-verify

**Parameters**

- **interval interval** — The interval, expressed in minutes, which specifies the time interval which all known sources should be verified. The actual rate is then dependent on number of known hosts and interval.

  **Values**

  1— 6000 ) Note that a zero value can be used by the SNMP agent to disable host-connectivity-verify.)

- **action** {remove | alarm} — Defines the action taken on a subscriber host connectivity verification failure for a given host. The **remove** keyword raises an alarm and removes dhcp-state and releases all allocated resources (queues, table entries, etc.). DHCP-RELEASE will be signaled to corresponding DHCP server. Static hosts will never be removed. The **alarm** keyword raises an alarm indicating that the host is disconnected.
Interface Commands

Interface ICMP Commands

**icmp**

```
Syntax  icmp
Context  config>service>vprn>if
        config>service>vprn>nw-if
Description  This command configures Internet Control Message Protocol (ICMP) parameters on a VPRN service.
```

**mask-reply**

```
Syntax  [no] mask-reply
Context  config>service>vprn>if>icmp
        config>service>vprn>nw-if>icmp
Description  This command enables responses to Internet Control Message Protocol (ICMP) mask requests on the router interface.

If a local node sends an ICMP mask request to the router interface, the mask-reply command configures the router interface to reply to the request.

By default, the router instance will reply to mask requests.

The no form of this command disables replies to ICMP mask requests on the router interface.

Default  mask-reply — Reply to ICMP mask requests.
```

**redirects**

```
Syntax  redirects [number seconds]
        no redirects
Context  config>service>vprn>if>icmp
        config>service>vprn>nw-if>icmp
Description  This command configures the rate for Internet Control Message Protocol (ICMP) redirect messages issued on the router interface.

When routes are not optimal on this router and another router on the same subnetwork has a better route, the router can issue an ICMP redirect to alert the sending node that a better route is available.

The redirects command enables the generation of ICMP redirects on the router interface. The rate at which ICMP redirects is issued can be controlled with the optional number and seconds parameters by indicating the maximum number of redirect messages that can be issued on the interface for a given time interval.
```
By default, generation of ICMP redirect messages is enabled at a maximum rate of 100 per 10 second time interval.

The no form of this command disables the generation of icmp redirects on the router interface.

**Default**

```
redirects 100 10 — Maximum of 100 redirect messages in 10 seconds.
```

**Parameters**

number — The maximum number of ICMP redirect messages to send. This parameter must be specified with the seconds parameter.

```
Values

10 — 1000
```

seconds — The time frame in seconds used to limit the seconds of ICMP redirect messages that can be issued.

```
Values

1 — 60
```

ttl-expired

**Syntax**

```
ttl-expired number seconds
no ttl-expired
```

**Context**

```
config>service>vprn>if>icmp
config>service>vprn>nw-if>icmp
```

**Description**

Configures the rate Internet Control Message Protocol (ICMP) TTL expired messages are issued by the IP interface.

By default, generation of ICMP TTL expired messages is enabled at a maximum rate of 100 per 10 second time interval.

The no form of this command disables the limiting the rate of TTL expired messages on the router interface.

**Default**

```
ttl-expired 100 10
```

**Parameters**

number — The maximum number of ICMP TTL expired messages to send, expressed as a decimal integer. This parameter must be specified with the seconds parameter.

```
Values

10 — 1000
```

seconds — The time frame in seconds used to limit the number of ICMP TTL expired messages that can be issued, expressed as a decimal integer.

```
Values

1 — 60
```

unreachables

**Syntax**

```
unreachables [number seconds]
no unreachable
```

**Context**

```
config>service>vprn>if>icmp
config>service>vprn>nw-if>icmp
```
**Description**  
This command enables and configures the rate for ICMP host and network destination unreachable messages issued on the router interface.

The **unreachables** command enables the generation of ICMP destination unreachables on the router interface. The rate at which ICMP unreachables is issued can be controlled with the optional `number` and `seconds` parameters by indicating the maximum number of destination unreachable messages which can be issued on the interface for a given time interval.

By default, generation of ICMP destination unreachable messages is enabled at a maximum rate of 10 per 10 second time interval.

The **no** form of this command disables the generation of icmp destination unreachable messages on the router interface.

**Default**  
`unreachables 100 10`

**Parameters**  
`number` — The maximum number of ICMP unreachable messages to send. This parameter must be specified with the `seconds` parameter.

**Values**  
10 — 1000

`seconds` — The time frame in seconds used to limit the `number` of ICMP unreachable messages that can be issued.

**Values**  
1 — 60
Interface ICMP Commands

icmp

Syntax          icmp
Context         config>service>vprn>if
               config>service>vprn>nw-if
Description     This command configures Internet Control Message Protocol (ICMP) parameters on a VPRN service.

mask-reply

Syntax          [no] mask-reply
Context         config>service>vprn>if>icmp
               config>service>vprn>nw-if>icmp
Description     This command enables responses to Internet Control Message Protocol (ICMP) mask requests on the router interface.

If a local node sends an ICMP mask request to the router interface, the mask-reply command configures the router interface to reply to the request.

By default, the router instance will reply to mask requests.

The no form of this command disables replies to ICMP mask requests on the router interface.

Default         mask-reply — Reply to ICMP mask requests.

redirects

Syntax          redirects [number seconds]
                no redirects
Context         config>service>vprn>if>icmp
               config>service>vprn>nw-if>icmp
Description     This command configures the rate for Internet Control Message Protocol (ICMP) redirect messages issued on the router interface.

When routes are not optimal on this router and another router on the same subnetwork has a better route, the router can issue an ICMP redirect to alert the sending node that a better route is available.

The redirects command enables the generation of ICMP redirects on the router interface. The rate at which ICMP redirects is issued can be controlled with the optional number and seconds parameters by indicating the maximum number of redirect messages that can be issued on the interface for a given time interval.
By default, generation of ICMP redirect messages is enabled at a maximum rate of 100 per 10 second time interval.

The no form of this command disables the generation of icmp redirects on the router interface.

**Default**

```
redirects 100 10 — Maximum of 100 redirect messages in 10 seconds.
```

**Parameters**

- `number` — The maximum number of ICMP redirect messages to send. This parameter must be specified with the `seconds` parameter.
  
  - **Values**
  
    10 — 1000
  
- `seconds` — The time frame in seconds used to limit the `seconds` of ICMP redirect messages that can be issued.
  
  - **Values**
  
    1 — 60

### ttl-expired

**Syntax**

```
ttl-expired number seconds
no ttl-expired
```

**Context**

- config>service>vprn>if>icmp
- config>service>vprn>nw-if>icmp

**Description**

Configures the rate Internet Control Message Protocol (ICMP) TTL expired messages are issued by the IP interface.

By default, generation of ICMP TTL expired messages is enabled at a maximum rate of 100 per 10 second time interval.

The no form of this command disables the limiting the rate of TTL expired messages on the router interface.

**Default**

```
ttl-expired 100 10
```

**Parameters**

- `number` — The maximum number of ICMP TTL expired messages to send, expressed as a decimal integer. This parameter must be specified with the `seconds` parameter.
  
  - **Values**
  
    10 — 1000
  
- `seconds` — The time frame in seconds used to limit the `number` of ICMP TTL expired messages that can be issued, expressed as a decimal integer.

  - **Values**
  
    1 — 60

### unreachables

**Syntax**

```
unreachables [number seconds]
no unreachables
```

**Context**

- config>service>vprn>if>icmp
- config>service>vprn>nw-if>icmp
**Description**

This command enables and configures the rate for ICMP host and network destination unreachable messages issued on the router interface.

The `unreachables` command enables the generation of ICMP destination unreachables on the router interface. The rate at which ICMP unreachables is issued can be controlled with the optional `number` and `seconds` parameters by indicating the maximum number of destination unreachable messages which can be issued on the interface for a given time interval.

By default, generation of ICMP destination unreachable messages is enabled at a maximum rate of 10 per 10 second time interval.

The `no` form of this command disables the generation of icmp destination unreachable messages on the router interface.

**Default**

```
unreachables 100 10
```

**Parameters**

- `number` — The maximum number of ICMP unreachable messages to send. This parameter must be specified with the `seconds` parameter.
  
  **Values**
  
  10 — 1000

- `seconds` — The time frame in seconds used to limit the `number` of ICMP unreachable messages that can be issued.
  
  **Values**
  
  1 — 60

- `populate-host-routes` — Specifies to populate subscriber-host routes in local FIB. Storing them in FIB benefits topologies only where the external router advertises more specific routes than the one corresponding to locally configured subscriber-interface subnets.
Interface ICMP Commands

icmp

Syntax  icmp
Context  config>service>vprn>if
cfgi>service>vprn>nw-if
Description  This command configures Internet Control Message Protocol (ICMP) parameters on a VPRN service.

mask-reply

Syntax  [no] mask-reply
Context  config>service>vprn>if>icmp
cfgi>service>vprn>nw-if>icmp
Description  This command enables responses to Internet Control Message Protocol (ICMP) mask requests on the router interface.
If a local node sends an ICMP mask request to the router interface, the mask-reply command configures the router interface to reply to the request.
By default, the router instance will reply to mask requests.
The no form of this command disables replies to ICMP mask requests on the router interface.
Default  mask-reply — Reply to ICMP mask requests.

redirects

Syntax  redirects [number seconds]
no redirects
Context  config>service>vprn>if>icmp
cfgi>service>vprn>nw-if>icmp
Description  This command configures the rate for Internet Control Message Protocol (ICMP) redirect messages issued on the router interface.
When routes are not optimal on this router and another router on the same subnetwork has a better route, the router can issue an ICMP redirect to alert the sending node that a better route is available.
The redirects command enables the generation of ICMP redirects on the router interface. The rate at which ICMP redirects is issued can be controlled with the optional number and seconds parameters by indicating the maximum number of redirect messages that can be issued on the interface for a given time interval.
By default, generation of ICMP redirect messages is enabled at a maximum rate of 100 per 10 second time interval.

The no form of this command disables the generation of icmp redirects on the router interface.

**Default**

`redirects 100 10` — Maximum of 100 redirect messages in 10 seconds.

**Parameters**

`number` — The maximum number of ICMP redirect messages to send. This parameter must be specified with the `seconds` parameter.

- **Values**
  - 10 — 1000

`seconds` — The time frame in seconds used to limit the `seconds` of ICMP redirect messages that can be issued.

- **Values**
  - 1 — 60

**ttl-expired**

**Syntax**

```
ttl-expired number seconds
no ttl-expired
```

**Context**

```
config>service>vprn>if>icmp
cfg>service>vprn>nw-if>icmp
```

**Description**

Configures the rate Internet Control Message Protocol (ICMP) TTL expired messages are issued by the IP interface.

By default, generation of ICMP TTL expired messages is enabled at a maximum rate of 100 per 10 second time interval.

The no form of this command disables the limiting the rate of TTL expired messages on the router interface.

**Default**

`ttl-expired 100 10`

**Parameters**

`number` — The maximum number of ICMP TTL expired messages to send, expressed as a decimal integer. This parameter must be specified with the `seconds` parameter.

- **Values**
  - 10 — 1000

`seconds` — The time frame in seconds used to limit the `number` of ICMP TTL expired messages that can be issued, expressed as a decimal integer.

- **Values**
  - 1 — 60

**unreachables**

**Syntax**

```
unreachables [number seconds]
no unreachables
```

**Context**

```
config>service>vprn>if>icmp
cfg>service>vprn>nw-if>icmp
```
Interface Commands

**Description**
This command enables and configures the rate for ICMP host and network destination unreachable messages issued on the router interface.

The `unreachables` command enables the generation of ICMP destination unreachables on the router interface. The rate at which ICMP unreachables is issued can be controlled with the optional `number` and `seconds` parameters by indicating the maximum number of destination unreachable messages which can be issued on the interface for a given time interval.

By default, generation of ICMP destination unreachable messages is enabled at a maximum rate of 10 per 10 second time interval.

The `no` form of this command disables the generation of icmp destination unreachable messages on the router interface.

**Default**
```
unreachables 100 10
```

**Parameters**

- **number** — The maximum number of ICMP unreachable messages to send. This parameter must be specified with the `seconds` parameter.
  - **Values**
    - 10 — 1000

- **seconds** — The time frame in seconds used to limit the `number` of ICMP unreachable messages that can be issued.
  - **Values**
    - 1 — 60

**lag**

**Syntax**
```
lag [lag-id[:encap-val]]
no lag
```

**Context**
```
config>service>vprn>nw-if
```

**Description**
This command binds the interface to a Link Aggregation Group (LAG)

The `no` form of the command removes the LAG id from the configuration.

**Parameters**

- **lag-id[encap-val]** — Specifies the LAG ID.
  - **Values**
    - lag-id 1 — 200
    - encap-val 0 for null
    - 0 — 4094 for dot1q

**Ilsr-load-balancing**

**Syntax**
```
lsr-load-balancing [hashing-algorithm]
no lsr-load-balancing
```

**Context**
```
config>service>vprn>nw-if
```

**Description**
This command specifies whether the IP header is used in the LAG and ECMP LSR hashing algorithm. This is the per interface setting.

**Default**
```
no lsr-load-balancing
```
<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>lbl-only</em></td>
<td>Only the label is used in the hashing algorithm.</td>
</tr>
<tr>
<td><em>lbl-ip</em></td>
<td>The IP header is included in the hashing algorithm.</td>
</tr>
<tr>
<td><em>ip-only</em></td>
<td>The IP header is used exclusively in the hashing algorithm.</td>
</tr>
<tr>
<td><em>eth-encap-ip</em></td>
<td>The hash algorithm parses down the label stack (up to 3 labels supported) and once it hits the bottom, the stack assumes Ethernet II non-tagged header follows. At the expected Ethertype offset location, algorithm checks whether the value present is IPv4/IPv6 (0x0800 or 0x0866D). If the check passes, the hash algorithm checks the first nibble at the expected IP header location for IPv4/IPv6 (0x0100/0x0110). If the secondary check passes, the hash is performed using IP SA/DA fields in the expected IP header; otherwise (any of the check failed) label-stack hash is performed.</td>
</tr>
</tbody>
</table>
Interface SAP Commands

**sap**

**Syntax**  
sap sap-id [create]
no sap sap-id

**Context**  
cfg>service>vprn>if

**Description**  
This command creates a Service Access Point (SAP) within a service. A SAP is a combination of port and encapsulation parameters which identifies the service access point on the interface and within the router. Each SAP must be unique.

All SAPs must be explicitly created. If no SAPs are created within a service or on an IP interface, a SAP will not exist on that object.

Enter an existing SAP without the create keyword to edit SAP parameters. The SAP is owned by the service in which it was created.

A SAP can only be associated with a single service. A SAP can only be defined on a port that has been configured as an access port using the config interface port-type port-id mode access command. Channelized TDM ports are always access ports.

If a port is shutdown, all SAPs on that port become operationally down. When a service is shutdown, SAPs for the service are not displayed as operationally down although all traffic traversing the service will be discarded. The operational state of a SAP is relative to the operational state of the port on which the SAP is defined.

The no form of this command deletes the SAP with the specified port. When a SAP is deleted, all configuration parameters for the SAP will also be deleted. The no form of the command causes the ptp-h-assist to be disabled.

**Default**  
No SAPs are defined.

**Special Cases**  
VPRN — A VPRN SAP must be defined on an Ethernet interface.

sap ipsec-id.private | public:tag — This parameter associates an IPSec group SAP with this interface. This is the public side for an IPSec tunnel. Tunnels referencing this IPSec group in the private side may be created if their local IP is in the subnet of the interface subnet and the routing context specified matches with the one of the interface.

This context will provide a SAP to the tunnel. The operator may associate an ingress and egress QoS policies as well as filters and virtual scheduling contexts. Internally this creates an Ethernet SAP that will be used to send and receive encrypted traffic to and from the MDA. Multiple tunnels can be associated with this SAP. The “tag” will be a dot1q value. The operator may see it as an identifier. The range is limited to 1 — 4094.

**Parameters**  
sap-id — Specifies the physical port identifier portion of the SAP definition. See Common CLI Command Descriptions on page 1783 for command syntax.

port-id — Specifies the physical port ID in the slot/mda/port format.

If the card in the slot has Media Dependent Adapters (MDAs) installed, the port-id must be in the slot_number/MDA_number/port_number format. For example /2/3 specifies port 3 on MDA 2 in slot.
The `port-id` must reference a valid port type. When the `port-id` parameter represents SONET/SDH and TDM channels the port ID must include the channel ID. A period “.” separates the physical port from the `channel-id`. The port must be configured as an access port.

If the SONET/SDH port is configured as clear-channel then only the port is specified.

`create` — Keyword used to create a SAP instance.

`split-horizon-group group-name` — Specifies the name of the split horizon group to which the SAP belongs.

### aarp

**Syntax**

```
aarp  aarpId  type  type
no aarp
```

**Context**

```
cfg>service>vprn>if>sap
cfg>service>vprn>if>spoke-sdp
```

**Description**

This command associates an aarp instance to a multi-homed SAP or spoke-sdp. This instance is paired with the same aarp-id in the same node or in a peer node as part of a configuration to provide flow and packet asymmetry removal for traffic for a multi-homed SAP or spoke-sdp.

The type specifies the role of this service point in the AARP: primary (dual-homed), secondary (dual-homed-secondary). The AA service attributes (app-profile, transit-policy) of the primary are inherited by the secondary endpoints. All endpoints within an aarp must be of the same type (sap or spoke), and all endpoints with an aarp must be within the same service.

The `no` form of the command removes the association.

**Default**

`no aarp`

**Parameters**

- `aarpId` — Specifies the AARP instance associated with this SAP. If not configured, no AARP instance is associated with this SAP.
  
  **Values**
  
  1 —

- `type` — Specifies the role of the SAP referenced by the AARP instance identified by AARP ID.
  
  **Values**
  
  - `dual-homed` — the primary dual homed aa-subscriber side service point of an aarp instance, only supported for IES and VPRN SAP and spoke-sdp
  - `dual-homed-secondary` — One of the secondary dual homed aa-subscriber side service points of an aarp instance, only supported for IES and VPRN SAP and spoke-sdp.

### tod-suite

**Syntax**

```
tod-suite  tod-suite-name
no tod-suite
```

**Context**

```
cfg>service>vprn>if>sap
```
Interface Commands

**Description**  
This command applies a time-based policy (filter or QoS policy) to the SAP. The suite name must already exist in the `config>crone` context.

**Default**  
no tod-suite

**Parameters**  
tod-suite-name — Specifies collection of policies (ACLs, QoS) including time-ranges that define the full or partial behavior of a SAP or a subscriber. The suite can be applied to more than one SAP.

**transit-policy**

**Syntax**  
transit-policy ip-aasub-policy-id  
transit-policy prefix prefix-aasub-policy-id  
no transit-ip-policy

**Context**  
config>service>vprn>if>sap  
config>service>vprn>if>spoke-sdp

**Description**  
This command associates a transit aa subscriber IP policy to the service. The transit IP policy must be defined prior to associating the policy with a SAP in the `config>application assurance>group>policy>transit-ip-policy` context.

Transit AA subscribers are managed by the system through the use of this policy assigned to services, which determines how transit subs are created and removed for that service.

The **no** form of the command removes the association of the policy to the service.

**Default**  
no transit-ip-policy

- **ip-aasub-policy-id** — An integer that identifies a transit IP profile entry.  
  **Values**  
  1 — 65535

- **prefix-aasub-policy-id** — An integer that identifies a prefix aasub-policy ID.  
  **Values**  
  1 — 65535

**accounting-policy**

**Syntax**  
accounting-policy acct-policy-id  
no accounting-policy

**Context**  
config>service>vprn>if>sap  
config>service>vprn>if>spoke-sdp

**Description**  
This command creates the accounting policy context that can be applied to an interface SAP or interface SAP spoke SDP.  
An accounting policy must be defined before it can be associated with a SAP.  
If the **policy-id** does not exist, an error message is generated.

A maximum of one accounting policy can be associated with a SAP at one time. Accounting policies are configured in the `config>log` context.
The **no** form of this command removes the accounting policy association from the SAP, and the accounting policy reverts to the default.

**Default**
Default accounting policy.

**Parameters**
acct-policy-id — Enter the accounting policy-id as configured in the `config>log>accounting-policy` context.

**Values**
1 — 99

### app-profile

**Syntax**
```text
app-profile app-profile-name
no app-profile
```

**Context**
`config>service>vprn>if>spoke-sdp`

**Description**
This command configures the application profile name.

**Parameters**
app-profile-name — Specifies the application profile name.

**Values**
32 chars max

### collect-stats

**Syntax**
```text
[no] collect-stats
```

**Context**
`config>service>vprn>if>sap`
`config>service>vprn>if>spoke-sdp`

**Description**
This command enables accounting and statistical data collection for either an interface SAP or interface SAP spoke SDP, or network port. When applying accounting policies the data, by default, is collected in the appropriate records and written to the designated billing file.

When the **no collect-stats** command is issued the statistics are still accumulated by the cards. However, the CPU will not obtain the results and write them to the billing file. If a subsequent **collect-stats** command is issued then the counters written to the billing file include all the traffic while the **no collect-stats** command was in effect.

**Default**
no collect-stats
Interface Commands

arp-timeout

**Syntax**
arp-timeout seconds  
no arp-timeout

**Context**
config>service>vprn>if

**Description**
This command configures the minimum time in seconds an ARP entry learned on the IP interface will be stored in the ARP table. ARP entries are automatically refreshed when an ARP request or gratuitous ARP is seen from an IP host, otherwise, the ARP entry is aged from the ARP table. If arp-timeout is set to a value of zero seconds, ARP aging is disabled.

The no form of this command restores arp-timeout to the default value.

**Default**
14400 seconds

**Parameters**
seconds — The minimum number of seconds a learned ARP entry will be stored in the ARP table, expressed as a decimal integer. A value of zero specifies that the timer is inoperative and learned ARP entries will not be aged.

**Values**
0 — 65535

authentication-policy

**Syntax**
authentication-policy name
no authentication-policy

**Context**
config>service>vprn>if

**Description**
This command assigns an authentication policy to the interface.

The no form of this command removes the policy name from the group interface configuration.

**Default**
no authentication-policy

**Parameters**
name — Specifies the authentication policy name. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

delayed-enable

**Syntax**
delayed-enable seconds [init-only]
no delayed-enable

**Context**
config>service>vprn>nw-if

**Description**
This command delays making interface operational by the specified number of seconds.
In environments with many subscribers, it can take time to synchronize the subscriber state between peers when the subscriber-interface is enabled (perhaps, after a reboot). To ensure that the state has time to be synchronized, the delayed-enable timer can be specified. The optional parameter init-only can be added to use this timer only after a reboot.

Default

Parameters

seconds — Specifies the number of seconds to delay before the interface is operational.

Values

1 — 1200

init-only — Delays the initialization of the subscriber-interface to give the rest of the system time to complete necessary tasks such as allowing routing protocols to converge and/or to allow MCS to sync the subscriber information. The delay only occurs immediately after a reboot.

calling-station-id

Syntax
calling-station-id calling-station-id
no calling-station-id

Context
config>service>vprn>if>sap

Description
This command enables the inclusion of the calling-station-id attribute in RADIUS authentication requests and RADIUS accounting messages. The value inserted is set at the SAP level. If no value is set at the SAP level, an empty string is included.

Default
This attribute is not sent by default.

scheduling-class

Syntax

scheduling-class class-id

Context
config>service>vprn>if>sap

Description
This command specifies the scheduling class to use for this SAP.

Parameters
class-id — Specifies the scheduling class to use for this SAP.

Values

0 — 3

Default

0

flowspec

Syntax
flowspec
no flowspec

Context
config>service>vprn>interface>sap>ingress
config>service>vprn>interface>spoke-sdp>ingress
config>service>ies>interface>sap>ingress
Interface Commands

config>service>ies>interface>spoke-sdp>ingress

**Description**  This command enables IPv4 flowspec filtering on an access IP interface associated with a VPRN or IES service. Filtering is based on all of the IPv4 flowspec routes that have been received and accepted by the corresponding BGP instance. Ingress IPv4 traffic on an interface can be filtered by both a user-defined IPv4 filter and flowspec. Evaluation proceeds in this order:

1. user-defined IPv4 filter entries
2. flowspec-derived filter entries
3. user-defined IPv4 filter default-action

The **no** form of the command removes IPv4 flowspec filtering from an IP interface.

**Default**  No access interfaces have IPv4 flowspec enabled.

flowspec-ipv6

**Syntax**  flowspec-ipv6

no flowspec-ipv6

**Context**  config>service>vprn>interface>sap>ingress
cfg=config>service>vprn>interface>spoke-sdp>ingress
cfg(config>service>ies>interface>sap>ingress
cfg(config>service>ies>interface>spoke-sdp>ingress

**Description**  This command enables IPv6 flowspec filtering on an access IP interface associated with a VPRN or IES service. Filtering is based on all of the IPv6 flowspec routes that have been received and accepted by the corresponding BGP instance. Ingress IPv6 traffic on an interface can be filtered by both a user-defined IPv6 filter and flowspec. Evaluation proceeds in this order:

1. user-defined IPv6 filter entries
2. flowspec-derived filter entries
3. user-defined IPv6 filter default-action

The **no** form of the command removes IPv6 flowspec filtering from an IP interface.

**Default**  No access interfaces have IPv6 flowspec enabled.

host-lockout-policy

**Syntax**  host-lockout-policy *policy-name*

no host-lockout-policy

**Context**  config>service>vprn>if>sap

**Description**  This command configures a host lockout policy.

The **no** form of the command removes the policy name from the configuration.
**host-shutdown**

**Syntax**

```
[no] host-shutdown
```

**Context**

```
config>service>vprn>if>sap
```

This command administratively enables host creation on this SAP.
Interface SAP Filter and QoS Policy Commands

egress

Syntax egress
Context config>service>vprn>if>sap
Description This command enables the context to configure egress SAP Quality of Service (QoS) policies and filter policies.

If no sap-egress QoS policy is defined, the system default sap-egress QoS policy is used for egress processing. If no egress filter is defined, no filtering is performed.

ingress

Syntax ingress
Context config>service>vprn>if>sap
config>service>vprn>if>sap
Description This command enables the context to configure ingress SAP Quality of Service (QoS) policies and filter policies.

If no sap-ingress QoS policy is defined, the system default sap-ingress QoS policy is used for ingress processing. If no ingress filter is defined, no filtering is performed.

agg-rate

Syntax [no] agg-rate
Context config>service>vprn>interface>sap>egress
Description This command is used to control an HQoS aggregate rate limit. It is used in conjunction with the following parameter commands: rate, limit-unused-bandwidth, and queue-frame-based-accounting.

rate

Syntax rate {max | rate}
no rate
Context config>service>vprn>interface>sap>egress>agg-rate
Description This command defines the enforced aggregate rate for all queues associated with the agg-rate context. A rate must be specified for the agg-rate context to be considered to be active on the context’s object.
Virtual Private Routed Network Services

(SAP, subscriber, VPORT etc.).

limit-unused-bandwidth

Syntax  

[no] limit-unused-bandwidth

Context  
config>service>vprn>interface>sap>egress>agg-rate

Description  
This command is used to enable (or disable) aggregate rate overrun protection on the agg-rate context.

queue-frame-based-accounting

Syntax  

[no] queue-frame-based-accounting

Context  
config>service>vprn>interface>sap>egress>agg-rate

Description  
This command is used to enabled (or disable) frame based accounting on all queues associated with the agg-rate context. Only supported on Ethernet ports. Not supported on HSMDA Ethernet ports.

agg-rate-limit

Syntax  

agg-rate-limit agg-rate [queue-frame-based-accounting]

no agg-rate-limit

Context  

Description  
This command defines a maximum total rate for all egress queues on a service SAP or multi-service site. The agg-rate-limit command is mutually exclusive with the egress scheduler policy. When an egress scheduler policy is defined, the agg-rate-limit command will fail. If the agg-rate-limit command is specified, an attempt to bind a scheduler-policy to the SAP or multi-service site will fail.

A multi-service site must have a port scope defined that ensures all queues associated with the site are on the same port or channel. If the scope is not set to a port, the agg-rate-limit command will fail.

Once an agg-rate-limit has been assigned to a multi-service site, the scope cannot be changed to card level.

A port scheduler policy must be applied on the egress port or channel the SAP or multi-service site is bound to in order for the defined agg-rate-limit to take effect. The egress port scheduler enforces the aggregate queue rate as it distributes its bandwidth at the various port priority levels. The port scheduler stops offering bandwidth to member queues once it has detected that the aggregate rate limit has been reached.

If a port scheduler is not defined on the egress port, the queues are allowed to operate based on their own bandwidth parameters.

The no form of the command removes the aggregate rate limit from the SAP or multi-service site.
Interface Commands

Parameters

*agg-rate* — Defines the rate, in kilobits-per-second, that the maximum aggregate rate that the queues on the SAP or multi-service site can operate.

**Values**  
1 — 40000000, max

*queue-frame-based-accounting* — This keyword enables frame based accounting on all queues associated with the SAP or Multi-Service Site. If frame based accounting is required when an aggregate limit is not necessary, the max keyword should precede the queue-frame-based-accounting keyword. If frame based accounting must be disabled, execute agg-rate-limit without the queue-frame-based-accounting keyword present.

**Default**  
Frame based accounting is disabled by default

filter

**Syntax**

```
filter ip ip-filter-id
no filter
```

**Context**

```
config>service>vprn>if>sap>egress
config>service>vprn>if>sap>ingress
```

**Description**

This command associates an IP filter policy with an ingress or egress Service Access Point (SAP) or IP interface. Filter policies control the forwarding and dropping of packets based on IP matching criteria.

The `filter` command is used to associate a filter policy with a specified `ip-filter-id` with an ingress or egress SAP. The `ip-filter-id` must already be defined before the `filter` command is executed. If the filter policy does not exist, the operation will fail and an error message returned.

In general, filters applied to SAPs (ingress or egress) apply to all packets on the SAP. One exception is non-IP packets are not applied to IP match criteria, so the default action in the filter policy applies to these packets.

The `no` form of this command removes any configured filter ID association with the SAP or IP interface. The filter ID itself is not removed from the system unless the scope of the created filter is set to local. To avoid deletion of the filter ID and only break the association with the service object, use `scope` command within the filter definition to change the scope to local or global. The default scope of a filter is local.

**Parameters**

*ip ip-filter-id* — Specifies IP filter policy. The filter ID must already exist within the created IP filters.

**Values**  
1 — 65535

flowspec

```
[no] flowspec
```

**Context**

```
config>service>vprn>interface>sap>ingress
config>service>vprn>interface>spoke-sdp>ingress
config>service>vprn>network-interface>ingress
```
**Virtual Private Routed Network Services**

**Description**
This command enables flowspec filtering on an IP interface of a VPRN. Filtering is based on all of the flowspec routes that have been received and accepted by the VPRN. Ingress traffic on an IP interface can be filtered by both a user-defined ip filter and flowspec. Evaluation proceeds in this order:

1. user-defined ip filter entries with entry numbers less than the configured insert-point
2. flowspec-derived filter entries
3. user-defined ip filter entries with entry numbers greater than or equal to the configured insert-point
4. ip-filter default-action

The **no** form of the command removes flowspec filtering from an IP interface.

**Default**
No interfaces have flowspec enabled.

**flowspec-ipv6**

**Syntax**

```
[no] flowspec-ipv6
```

**Context**

```
config>service>vprn>interface>sap>ingress
config>service>vprn>interface>spoke-sdp>ingress
```

**Description**
This command enables flowspec filtering on an IP interface of the base router. Filtering is based on all of the flowspec routes that have been received and accepted by the base router. Ingress traffic on an IP interface can be filtered by both a user-defined ip filter and flowspec. In this case, the user-defined ip filter entries are evaluated before the flowspec routes and the default action of the user-defined ip filter applies as the very last rule.

The **no** form of the command removes flowspec filtering from an IP interface.

**Default**
No interfaces have flowspec enabled.

**wrr-weight**

**Syntax**

```
wrr-weight value
no wrr-weight
```

**Context**

```
config>service>vprn>if>sap>egress>hsmda-queue-overider>queue
```

**Description**
This command assigns the weight value to the HSMDA queue.

The **no** form of the command returns the weight value for the queue to the default value.

**Parameters**

- `percentage` — Specifies the weight for the HSMDA queue.

**Values**

1—32

**wrr-policy**
**Interface Commands**

**wrr-policy**

**Syntax**

```
Syntax wrr-policy hsmda-wrr-policy-name
no wrr-policy
```

**Context**

```
config>service>vprn>if>sap>egress>hsmda-queue-overider
```

**Description**

This command associates an existing HSMDA weighted-round-robin (WRR) scheduling loop policy to the HSMDA queue.

**Parameters**

- `hsmda-wrr-policy-name` — Specifies the existing HSMDA WRR policy name to associate to the queue.

**secondary-shaper**

**Syntax**

```
Syntax secondary-shaper secondary-shaper-name
no secondary-shaper
```

**Context**

```
config>service>vprn>if>sap>egress>hsmda-queue-overider
```

**Description**

This command configures an HSMDA secondary shaper. Note that a shaper override can only be configured on an HSMDA SAP.

**Parameters**

- `secondary-shaper-name` — Specifies a secondary shaper name up to 32 characters in length.

**match-qinq-dot1p**

**Syntax**

```
Syntax match-qinq-dot1p {top | bottom}
no match-qinq-dot1p
```

**Context**

```
config>service>vprn>if>sap>ingress
```

**Description**

This command specifies which Dot1Q tag position Dot1P bits in a QinQ encapsulated packet should be used to evaluate Dot1P QoS classification.

The `match-qinq-dot1p` command allows the top or bottom PBits to be used when evaluating the applied sap-ingress QoS policy’s Dot1P entries. The `top` and `bottom` keywords specify which position should be evaluated for QinQ encapsulated packets.

The `no` form of the command restores the default dot1p evaluation behavior for the SAP.

By default, the bottom most service delineating Dot1Q tags Dot1P bits are used. The following table defines the default behavior for Dot1P evaluation when the `match-qinq-dot1p` command is not executed.

<table>
<thead>
<tr>
<th>Port / SAP Type</th>
<th>Existing Packet Tags</th>
<th>PBits Used for Match</th>
</tr>
</thead>
<tbody>
<tr>
<td>Null</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>Null</td>
<td>Dot1P (VLAN-ID 0)</td>
<td>Dot1P PBITS</td>
</tr>
<tr>
<td>Null</td>
<td>Dot1Q</td>
<td>Dot1Q PBITS</td>
</tr>
<tr>
<td>Null</td>
<td>TopQ BottomQ</td>
<td>TopQ PBITS</td>
</tr>
</tbody>
</table>
Virtual Private Routed Network Services

Default

no match-qinq-dot1p - No filtering based on p-bits.
top or bottom must be specified to override the default QinQ dot1p behavior.

Parameters

**top** — The top parameter is mutually exclusive to the bottom parameter. When the top parameter is specified, the top most PBits are used (if existing) to match any dot1p dot1p-value entries. The following table defines the dot1p evaluation behavior when the top parameter is specified.

<table>
<thead>
<tr>
<th>Port / SAP Type</th>
<th>Existing Packet Tags</th>
<th>PBits Used for Match</th>
</tr>
</thead>
<tbody>
<tr>
<td>Null</td>
<td>TopQ (No BottomQ)</td>
<td>TopQ PBits</td>
</tr>
<tr>
<td>Dot1Q</td>
<td>None (Default SAP)</td>
<td>None</td>
</tr>
<tr>
<td>Dot1Q</td>
<td>Dot1P (Default SAP VLAN-ID 0)</td>
<td>Dot1P PBits</td>
</tr>
<tr>
<td>Dot1Q</td>
<td>Dot1Q</td>
<td>Dot1Q PBits</td>
</tr>
<tr>
<td>QinQ / TopQ</td>
<td>TopQ</td>
<td>TopQ PBits</td>
</tr>
<tr>
<td>QinQ / TopQ</td>
<td>TopQ BottomQ</td>
<td>TopQ PBits</td>
</tr>
<tr>
<td>QinQ / QinQ</td>
<td>TopQ BottomQ</td>
<td>TopQ PBits</td>
</tr>
</tbody>
</table>

**bottom** — The bottom parameter is mutually exclusive to the top parameter. When the bottom parameter is specified, the bottom most PBits are used (if existing) to match any dot1p dot1p-value entries. The following tables define the bottom position QinQ and TopQ SAP dot1p evaluation and the default dot1p explicit marking actions.

<table>
<thead>
<tr>
<th>Port / SAP Type</th>
<th>Existing Packet Tags</th>
<th>PBits Used for Match</th>
</tr>
</thead>
<tbody>
<tr>
<td>Null</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>Null</td>
<td>Dot1P (VLAN-ID 0)</td>
<td>Dot1P PBits</td>
</tr>
<tr>
<td>Null</td>
<td>Dot1Q</td>
<td>Dot1Q PBits</td>
</tr>
<tr>
<td>Null</td>
<td>TopQ BottomQ</td>
<td>TopQ PBits</td>
</tr>
<tr>
<td>Null</td>
<td>TopQ (No BottomQ)</td>
<td>TopQ PBits</td>
</tr>
<tr>
<td>Dot1Q</td>
<td>None (Default SAP)</td>
<td>None</td>
</tr>
<tr>
<td>Dot1Q</td>
<td>Dot1P (Default SAP VLAN-ID 0)</td>
<td>Dot1P PBits</td>
</tr>
<tr>
<td>Dot1Q</td>
<td>Dot1Q</td>
<td>Dot1Q PBits</td>
</tr>
<tr>
<td>QinQ / TopQ</td>
<td>TopQ</td>
<td>TopQ PBits</td>
</tr>
<tr>
<td>QinQ / TopQ</td>
<td>TopQ BottomQ</td>
<td>TopQ PBits</td>
</tr>
<tr>
<td>QinQ / TopQ</td>
<td>TopQ BottomQ</td>
<td>TopQ PBits</td>
</tr>
</tbody>
</table>

Table 27: Bottom Position QinQ and TopQ SAP Dot1P Evaluation

<table>
<thead>
<tr>
<th>Port / SAP Type</th>
<th>Existing Packet Tags</th>
<th>PBits Used for Match</th>
</tr>
</thead>
<tbody>
<tr>
<td>Null</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>Null</td>
<td>Dot1P (VLAN-ID 0)</td>
<td>Dot1P PBits</td>
</tr>
</tbody>
</table>
The `dot1p dot1p-value` command must be configured without the `qinq-mark-top-only` parameter to remove the TopQ PBits only marking restriction.

### Table 27: Bottom Position QinQ and TopQ SAP Dot1P Evaluation (Continued)

<table>
<thead>
<tr>
<th>Port / SAP Type</th>
<th>Existing Packet Tags</th>
<th>PBits Used for Match</th>
</tr>
</thead>
<tbody>
<tr>
<td>Null</td>
<td>Dot1Q</td>
<td>Dot1Q PBits</td>
</tr>
<tr>
<td>Null</td>
<td>TopQ BottomQ</td>
<td>BottomQ PBits</td>
</tr>
<tr>
<td>Null</td>
<td>TopQ (No BottomQ)</td>
<td>TopQ PBits</td>
</tr>
<tr>
<td>Dot1Q</td>
<td>None (Default SAP)</td>
<td>None</td>
</tr>
<tr>
<td>Dot1Q</td>
<td>Dot1P (Default SAP VLAN-ID 0)</td>
<td>Dot1P PBits</td>
</tr>
<tr>
<td>Dot1Q</td>
<td>Dot1Q</td>
<td>Dot1Q PBits</td>
</tr>
<tr>
<td>QinQ / TopQ</td>
<td>TopQ</td>
<td>TopQ PBits</td>
</tr>
<tr>
<td>QinQ / TopQ</td>
<td>TopQ BottomQ</td>
<td>BottomQ PBits</td>
</tr>
<tr>
<td>QinQ / QinQ</td>
<td>TopQ BottomQ</td>
<td>BottomQ PBits</td>
</tr>
</tbody>
</table>

### Egress SAP Type

<table>
<thead>
<tr>
<th>Egress SAP Type</th>
<th>Ingress Packet Preserved Dot1P State</th>
<th>Marked (or Remarked) PBits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Null</td>
<td>No preserved Dot1P bits</td>
<td>None</td>
</tr>
<tr>
<td>Null</td>
<td>Preserved Dot1P bits</td>
<td>Preserved tag PBits remarked using dot1p-value</td>
</tr>
<tr>
<td>Dot1Q</td>
<td>No preserved Dot1P bits</td>
<td>New PBits marked using dot1p-value</td>
</tr>
<tr>
<td>Dot1Q</td>
<td>Preserved Dot1P bits</td>
<td>Preserved tag PBits remarked using dot1p-value</td>
</tr>
<tr>
<td>TopQ</td>
<td>No preserved Dot1P bits</td>
<td>TopQ PBits marked using dot1p-value</td>
</tr>
<tr>
<td>TopQ</td>
<td>Preserved Dot1P bits (used as TopQ and BottomQ PBits)</td>
<td>TopQ PBits marked using dot1p-value, BottomQ PBits preserved</td>
</tr>
<tr>
<td>QinQ</td>
<td>No preserved Dot1P bits</td>
<td>TopQ PBits and BottomQ PBits marked using dot1p-value</td>
</tr>
<tr>
<td>QinQ</td>
<td>Preserved Dot1P bits (used as TopQ and BottomQ PBits)</td>
<td>TopQ PBits and BottomQ PBits marked using dot1p-value</td>
</tr>
</tbody>
</table>
qinq-mark-top-only

Syntax: \[no\] qinq-mark-top-only

Context: config\(\text{service}\)\(\text{vprn}\)\(\text{if}\)\(\text{sap}\)\(\text{egress}\)

Description: When enabled (the encapsulation type of the access port where this SAP is defined as qinq), the qinq-mark-top-only command specifies which P-bits/DEI bit to mark during packet egress. When disabled, both set of P-bits/DEI bit are marked. When the enabled, only the P-bits/DEI bit in the top Q-tag are marked.

Default: no qinq-mark-top-only

QoS

Syntax: qos policy-id [port-redirect-group queue-group-name instance instance-id] no qos

Context: config\(\text{service}\)\(\text{vprn}\)\(\text{if}\)\(\text{sap}\)\(\text{egress}\) config\(\text{service}\)\(\text{vprn}\)\(\text{sub-if}\)\(\text{grp-if}\)\(\text{sap}\)\(\text{egress}\) config\(\text{service}\)\(\text{vprn}\)\(\text{ipsec-if}\)\(\text{sap}\)\(\text{egress}\)

Description: This command associates a Quality of Service (QoS) policy with an ingress or egress Service Access Point (SAP).

QoS ingress and egress policies are important for the enforcement of SLA agreements. The policy ID must be defined prior to associating the policy with a SAP or IP interface. If the policy-id does not exist, an error will be returned.

The qos command is used to associate both ingress and egress QoS policies. The qos command only allows ingress policies to be associated on SAP ingress and egress policies on SAP egress. Attempts to associate a QoS policy of the wrong type returns an error.

Only one ingress and one egress QoS policy can be associated with a SAP or IP interface at one time. Attempts to associate a second QoS policy of a given type will return an error.

By default, no specific QoS policy is associated with the SAP for ingress or egress, so the default QoS policy is used.

The no form of this command removes the QoS policy association from the SAP, and the QoS policy reverts to the default.

Default: none

Parameters:
- policy-id — The ingress/egress policy ID to associate with SAP or IP interface on ingress/egress. The policy ID must already exist.
  
  1 — 65535
Interface Commands

**port-redirect-group** — This keyword associates a SAP egress with an instance of a named queue group template on the egress port of a given IOM/IMM/XMA. The queue-group-name and instance instance-id are mandatory parameters when executing the command.

*queue-group-name* — Specifies the name of the egress port queue group of the IOM/IMM/XMA, up to 32 characters in length. The queue-group-name must correspond to a valid egress queue group, created under config>port>ethernet>access>egress.

*instance instance-id* — Specifies the instance of the named egress port queue group on the IOM/IMM/XMA.

| Values  | 1 — 40960 |
| Default | 1         |

**qos**

**Syntax**

```
qos policy-id [shared-queuing | multipoint-shared] fp-redirect-group queue-group-name instance instance-id
no qos
```

**Context**

```
config>service>vprn>if>sap>ingress
config>service>vprn>sub-if>grp-if>sap>ingress
config>service>vprn>ipsec-if>sap>ingress
```

**Description**

This command associates a Quality of Service (QoS) policy with an ingress Service Access Point (SAP).

QoS ingress and egress policies are important for the enforcement of SLA agreements. The policy ID must be defined prior to associating the policy with a SAP. If the policy-id does not exist, an error will be returned.

The qos command is used to associate both ingress and egress QoS policies. The qos command only allows ingress policies to be associated on SAP ingress and egress policies on SAP egress. Attempts to associate a QoS policy of the wrong type returns an error.

Only one ingress and one egress QoS policy can be associated with a SAP or IP interface at one time. Attempts to associate a second QoS policy of a given type will return an error.

By default, no specific QoS policy is associated with the SAP for ingress or egress, so the default QoS policy is used.

The no form of this command removes the QoS policy association from the SAP, and the QoS policy reverts to the default.

**Default**

```
none
```

**Parameters**

*policy-id* — The ingress/egress policy ID to associate with SAP or IP interface on ingress/egress. The policy ID must already exist.

| Values  | 1 — 65535 |
shared-queuing — Specifies the ingress shared queue policy used by this SAP. When the value of this object is null it means that the SAP will use individual ingress QoS queues instead of the shared ones.

multipoint-shared — This keyword specifies that this queue-id is for multipoint forwarded traffic only. This queue-id can only be explicitly mapped to the forwarding class multicast, broadcast, or unknown unicast ingress traffic. Attempting to map forwarding class unicast traffic to a multipoint queue generates an error; no changes are made to the current unicast traffic queue mapping.

A queue must be created as multipoint. The multipoint designator cannot be defined after the queue is created. If an attempt is made to modify the command to include the multipoint keyword, an error is generated and the command will not execute.

The multipoint keyword can be entered in the command line on a pre-existing multipoint queue to edit queue-id parameters.

Default Present (the queue is created as non-multipoint).

Values Multipoint or not present.

fp-redirect-group — This keyword creates an instance of a named queue group template on the ingress forwarding plane of a given IOM/IMM/XMA. The queue-group-name and instance instance-id are mandatory parameters when executing the command. The named queue group template can contain only policers. If it contains queues, then the command will fail.

queue-group-name — Specifies the name of the queue group template to be instantiated on the forwarding plane of the IOM/IMM/XMA, up to 32 characters in length. The queue-group-name must correspond to a valid ingress queue group template name, configured under config>qos>queue-group-templates.

instance-id — Specifies the instance of the named queue group to be created on the IOM/IMM/XMA ingress forwarding plane.

scheduler-policy

**Syntax**

```
scheduler-policy scheduler-policy-name
no scheduler-policy
```

**Context**

```
config>service>vprn>if>sap>ingress
config>service>vprn>if>sap>egress
```

**Description**

This command applies an existing scheduler policy to an ingress or egress scheduler used by SAP queues associated with this multi-service customer site. The schedulers defined in the scheduler policy can only be created once the customer site has been appropriately assigned to a chassis port, channel or slot. Scheduler policies are defined in the `config>qos>scheduler-policy scheduler-policy-name` context.

The no form of this command removes the configured ingress or egress scheduler policy from the multi-service customer site. When the policy is removed, the schedulers created due to the policy are removed also making them unavailable for the ingress SAP queues associated with the customer site. Queues that lose their parent scheduler association are deemed to be orphaned and are no longer subject to a virtual scheduler. The SAPs that have ingress queues reliant on the removed schedulers enter into an operational state depicting the orphaned status of one or more queues. When the no
Interface Commands

**scheduler-policy** command is executed, the customer site ingress or egress node will not contain an applied scheduler policy.

**scheduler-policy-name**: — The **scheduler-policy-name** parameter applies an existing scheduler policy that was created in the **config>qos>scheduler-policy scheduler-policy-name** context to create the hierarchy of ingress or egress virtual schedulers. The scheduler names defined within the policy are created and made available to any ingress or egress queues created on associated SAPs.

**Values** Any existing valid scheduler policy name.

---

**lag-link-map-profile**

**Syntax** `lag-link-map-profile link-map-profile-id`

**Context** `config>service>vprn>if>sap`

**Description** This command assigns a pre-configured lag link map profile to a SAP/network interface configured on a LAG or a PW port that exists on a LAG. Once assigned/de-assigned, the SAP/network interface egress traffic will be re-hashed over LAG as required by the new configuration.

The **no** form of this command reverts the SAP/network interface to use per-flow, service or link hash as configured for the service/LAG.

**Default** `no lag-link-map-profile`

**Parameters** `link-map-profile-id` — An integer from 1 to 64 that defines a unique lag link map profile on which the LAG the SAP/network interface exist.

---

**multi-service-site**

**Syntax** `multi-service-site customer-site-name`

**Context** `config>service>vprn>if>sap`

**Description** This command creates a new customer site or edits an existing customer site with the **customer-site-name** parameter. A customer site is an anchor point to create an ingress and egress virtual scheduler hierarchy. When scheduler policies are defined for ingress and egress, the scheduler names contained in each policy are created according to the parameters defined in the policy. Multi-service customer sites exist for the sole purpose of creating a virtual scheduler hierarchy and making it available to queues on multiple Service Access Points (SAPs).

The scheduler policy association with the customer site normally prevents the scheduler policy from being deleted until after the scheduler policy is removed from the customer site. The multi-service-site object will generate a log message indicating that the association was deleted due to scheduler policy removal.

When the multi-service customer site is created, an ingress and egress scheduler policy association does not exist. This does not prevent the site from being assigned to a chassis slot or prevent service
SAP assignment. After the site has been created, the ingress and egress scheduler policy associations can be assigned or removed at any time.

**Default**
None — Each customer site must be explicitly created.

**Parameters**
- **customer-site-name:** — Each customer site must have a unique name within the context of the customer. If `customer-site-name` already exists for the customer ID, the CLI context changes to that site name for the purpose of editing the site scheduler policies or assignment. Any modifications made to an existing site will affect all SAPs associated with the site. Changing a scheduler policy association may cause new schedulers to be created and existing queues on the SAPs to no longer be orphaned. Existing schedulers on the site may cease to exist, causing queues relying on that scheduler to be orphaned.

If the `customer-site-name` does not exist, it is assumed that an attempt is being made to create a site of that name in the customer ID context. The success of the command execution depends on the following:

- The maximum number of customer sites defined for the chassis slot has not been met.
- The `customer-site-name` is valid.
- The `create` keyword is included in the command line syntax (if the system requires it).

When the maximum number of customer sites has been exceeded a configuration error occurs; the command will not execute and the CLI context will not change.

If the `customer-site-name` is invalid, a syntax error occurs; the command will not execute and the CLI context will not change.

**Values**
Valid names consist of any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

---

**static-host**

**Syntax**

- `static-host ip ip/did-address [mac ieee-address] [create]`
- `static-host mac ieee-address [create]`
- `no static-host [ip ip-address>] mac ieee-address`
- `no static-host all [force]`
- `no static-host ip ip-address`

**Context**

`config>service>vprn>if>sap`

**Description**
This command configures a static host on this SAP.

**Syntax**

- `ip ip-address` — Specifies the IPv4 unicast address.
- `mac ieee-address` — Specify this optional parameter when defining a static host. Every static host definition must have at least one address defined, IP or MAC.
- `force` — Specifies the forced removal of the static host addresses.

This optional parameter is used to specify an existing SLA profile name to be associated with the static subscriber host. The SLA profile is configured in the `config>subscr-mgmt>sla-profile` context.
Interface Commands

ancp-string

Syntax

ancp-string ancp-string
no ancp-string

Context
config>service>vprn>if>sap>static-host

Description
This command specifies the ANCP string associated to this SAP host.

Parameters
ancp-string — Specifies the ANCP string up to 63 characters in length.

app-profile

Syntax

app-profile app-profile-name
no app-profile

Context
config>service>vprn>if>sap>static-host

Description
This command specifies an application profile name.

Parameters
app-profile-name — Specifies the application profile name up to 32 characters in length.

inter-dest-id

Syntax

inter-dest-id intermediate-destination-id
no inter-dest-id

Context
config>service>vprn>if>sap>static-host

Description
This command specifies to which intermediate destination (for example a DSLAM) this host belongs.

Parameters
intermediate-destination-id — Specifies the intermediate destination ID.

sla-profile

Syntax

sla-profile sla-profile-name
no sla-profile

Context
config>service>vprn>if>sap>static-host

Description
This command specifies an existing SLA profile name to be associated with the static subscriber host. The SLA profile is configured in the config>subscr-mgmt>sla-profile context.

Parameters
sla-profile-name — Specifies the SLA profile name.

sub-profile
Virtual Private Routed Network Services

**Syntax**

```
sub-profile sub-profile-name
no sub-profile
```

**Context**

`config>service>vprn>if>sap>static-host`

**Description**

This command specifies an existing subscriber profile name to be associated with the static subscriber host.

**Parameters**

`sub-profile-name` — Specifies the sub-profile name.

---

**subscriber**

```
subscriber sub-ident
no subscriber
```

**Context**

`config>service>vprn>if>sap>static-host`

**Description**

This command specifies an existing subscriber identification profile to be associated with the static subscriber host.

**Parameters**

`sub-ident` — Specifies the subscriber identification.

---

**subscriber-sap-id**

```
[no] subscriber-sap-id
```

**Context**

`config>service>vprn>if>sap>static-host`

**Description**

This command enables using the SAP ID as subscriber id.

**Parameters**

`subscriber-sap-id` — Specifies to use the sap-id as the subscriber-id.

---

**queue-override**

```
[no] queue-override
```

**Context**

`config>service>vprn>if>sap>egress`

`config>service>vprn>if>sap>ingress`

**Description**

This command enables the context to configure override values for the specified SAP egress or ingress QoS queue. These values override the corresponding ones specified in the associated SAP egress or ingress QoS policy.

---

**queue**

```
[no] queue queue-id
```

**Context**

`config>service>vprn>if>sap>egress>queue-override`

---
Interface Commands

config>service>vprn>if>sap>ingress>queue-override

**Description**
This command specifies the ID of the queue whose parameters are to be overridden.

**Parameters**
*queue-id* — The queue ID whose parameters are to be overridden.

**Values**
1 — 32

adaptation-rule

**Syntax**
adaptation-rule [pir adaptation-rule] [cir adaptation-rule]  
no adaptation-rule

**Context**
config>service>vprn>if>sap>egress>queue-override>queue  
config>service>vprn>if>sap>ingress>queue-override>queue

**Description**
This command can be used to override specific attributes of the specified queue’s adaptation rule parameters. The adaptation rule controls the method used by the system to derive the operational CIR and PIR settings when the queue is provisioned in hardware. For the CIR and PIR parameters individually, the system attempts to find the best operational rate depending on the defined constraint.

The **no** form of the command removes any explicitly defined constraints used to derive the operational CIR and PIR created by the application of the policy. When a specific *adaptation-rule* is removed, the default constraints for *rate* and *cir* apply.

**Default**
no adaptation-rule

**Parameters**
*pir* — The *pir* parameter defines the constraints enforced when adapting the PIR rate defined within the *queue queue-id rate* command. The *pir* parameter requires a qualifier that defines the constraint used when deriving the operational PIR for the queue. When the *rate* command is not specified, the default applies.

*cir* — The *cir* parameter defines the constraints enforced when adapting the CIR rate defined within the *queue queue-id rate* command. The *cir* parameter requires a qualifier that defines the constraint used when deriving the operational CIR for the queue. When the *cir* parameter is not specified, the default constraint applies.

*adaptation-rule* — Specifies the criteria to use to compute the operational CIR and PIR values for this queue, while maintaining a minimum offset.

**Values**
*max* — The *max* (maximum) keyword is mutually exclusive with the *min* and closest options. When *max* is defined, the operational PIR for the queue will be equal to or less than the administrative rate specified using the *rate* command.

*min* — The *min* (minimum) keyword is mutually exclusive with the *max* and closest options. When *min* is defined, the operational PIR for the queue will be equal to or greater than the administrative rate specified using the *rate* command.

*closest* — The *closest* parameter is mutually exclusive with the *min* and *max* parameter. When *closest* is defined, the operational PIR for the queue will be the rate closest to the rate specified using the *rate* command.

avg-frame-overhead
Virtual Private Routed Network Services

Syntax

```
avg-frame-overhead percent
no avg-frame-overhead
```

Context

```
config>service>vprn>if>sap>egress>queue-override>queue
```

Description

This command configures the average frame overhead to define the average percentage that the offered load to a queue will expand during the frame encapsulation process before sending traffic on-the-wire. While the avg-frame-overhead value may be defined on any queue, it is only used by the system for queues that egress a Sonet or SDH port or channel. Queues operating on egress Ethernet ports automatically calculate the frame encapsulation overhead based on a 20 byte per packet rule (8 bytes for preamble and 12 bytes for Inter-Frame Gap).

When calculating the frame encapsulation overhead for port scheduling purposes, the system determines the following values:

- **Offered-load** — The offered-load of a queue is calculated by starting with the queue depth in octets, adding the received octets at the queue and subtracting queue discard octets. The result is the number of octets the queue has available to transmit. This is the packet based offered-load.

- **Frame encapsulation overhead** — Using the avg-frame-overhead parameter, the frame encapsulation overhead is simply the queue’s current offered-load (how much has been received by the queue) multiplied by the avg-frame-overhead. If a queue had an offered load of 10000 octets and the avg-frame-overhead equals 10%, the frame encapsulation overhead would be 10000 x 0.1 or 1000 octets.

  For egress Ethernet queues, the frame encapsulation overhead is calculated by multiplying the number of offered-packets for the queue by 20 bytes. If a queue was offered 50 packets then the frame encapsulation overhead would be 50 x 20 or 1000 octets.

- **Frame based offered-load** — The frame based offered-load is calculated by adding the offered-load to the frame encapsulation overhead. If the offered-load is 10000 octets and the encapsulation overhead was 1000 octets, the frame based offered-load would equal 11000 octets.

- **Packet to frame factor** — The packet to frame factor is calculated by dividing the frame encapsulation overhead by the queue’s offered-load (packet based). If the frame encapsulation overhead is 1000 octets and the offered-load is 10000 octets then the packet to frame factor would be 1000 / 10000 or 0.1. When in use, the avg-frame-overhead will be the same as the packet to frame factor making this calculation unnecessary.

- **Frame based CIR** — The frame based CIR is calculated by multiplying the packet to frame factor with the queue’s configured CIR and then adding that result to that CIR. If the queue CIR is set at 500 octets and the packet to frame factor equals 0.1, the frame based CIR would be 500 x 1.1 or 550 octets.

- **Frame based within-cir offered-load** — The frame based within-cir offered-load is the portion of the frame based offered-load considered to be within the frame-based CIR. The frame based within-cir offered-load is the lesser of the frame based offered-load and the frame based CIR. If the frame based offered-load equaled 11000 octets and the frame based CIR equaled 550 octets, the frame based within-cir offered-load would be limited to 550 octets. If the frame based offered-load equaled 450 octets and the frame based CIR equaled 550 octets, the frame based within-cir offered-load would equal 450 octets (or the entire frame based offered-load).

As a special case, when a queue or associated intermediate scheduler is configured with a CIR-weight equal to 0, the system automatically sets the queue’s frame based within-cir offered-load to 0, preventing it from receiving bandwidth during the port scheduler’s within-cir pass.
• Frame based PIR — The frame based PIR is calculated by multiplying the packet to frame factor with the queue’s configured PIR and then adding the result to that PIR. If the queue PIR is set to 7500 octets and the packet to frame factor equals 0.1, the frame based PIR would be 7500 x 1.1 or 8250 octets.

• Frame based within-pir offered-load — The frame based within-pir offered-load is the portion of the frame based offered-load considered to be within the frame based PIR. The frame based within-pir offered-load is the lesser of the frame based offered-load and the frame based PIR. If the frame based offered-load equaled 11000 octets and the frame based PIR equaled 8250 octets, the frame based within-pir offered-load would be limited to 8250 octets. If the frame based offered-load equaled 7000 octets and the frame based PIR equaled 8250 octets, the frame based within-pir offered load would equal 7000 octets.

Port scheduler operation using frame transformed rates — The port scheduler uses the frame based rates to determine the maximum rates that each queue may receive during the within-cir and above-cir bandwidth allocation passes. During the within-cir pass, a queue may receive up to its frame based within-cir offered-load. The maximum it may receive during the above-cir pass is the difference between the frame based within-pir offered load and the amount of actual bandwidth allocated during the within-cir pass.

SAP and subscriber SLA-profile average frame overhead override — The average frame overhead parameter on a sap-ingress may be overridden at an individual egress queue basis. On each SAP and within the sla-profile policy used by subscribers an avg-frame-overhead command may be defined under the queue-override context for each queue. When overridden, the queue instance will use its local value for the average frame overhead instead of the sap-ingress defined overhead.

The no form of this command restores the average frame overhead parameter for the queue to the default value of 0 percent. When set to 0, the system uses the packet based queue statistics for calculating port scheduler priority bandwidth allocation. If the no avg-frame-overhead command is executed in a queue-override queue id context, the avg-frame-overhead setting for the queue within the sap-ingress QoS policy takes effect.

Default 0

Parameters percent — This parameter sets the average amount of packet-to-frame encapsulation overhead expected for the queue. This value is not used by the system for egress Ethernet queues.

Values 0 — 100

cbs

Syntax cbs size-in-kbytes
no cbs

Context config>service>vprn>if>.sap>egress>queue-override>queue
config>service>vprn>if>.sap>ingress>queue-override>queue

Description This command can be used to override specific attributes of the specified queue’s CBS parameters. It is permissible, and possibly desirable, to oversubscribe the total CBS reserved buffers for a given access port egress buffer pool. Oversubscription may be desirable due to the potential large number of service queues and the economy of statistical multiplexing the individual queue’s CBS setting into the defined reserved total.
When oversubscribing the reserved total, it is possible for a queue depth to be lower than its CBS setting and still not receive a buffer from the buffer pool for an ingress frame. As more queues are using their CBS buffers and the total in use exceeds the defined reserved total, essentially the buffers are being removed from the shared portion of the pool without the shared in use average and total counts being decremented. This can affect the operation of the high and low priority RED slopes on the pool, causing them to miscalculate when to start randomly drop packets.

If the CBS value is larger than the MBS value, an error will occur, preventing the CBS change.

The no form of this command returns the CBS size to the default value.

**Default**

`no cbs`

**Parameters**

`size-in-kbytes` — The size parameter is an integer expression of the number of kilobytes reserved for the queue. If a value of 10KBytes is desired, enter the value 10. A value of 0 specifies that no reserved buffers are required by the queue (a minimal reserved size can still be applied for scheduling purposes).

**Values**

0 — 131072 or default

### high-prio-only

**Syntax**

`high-prio-only percent`

`no high-prio-only`

**Context**

`config>service>vprn>if>sap>egress>queue-override>queue`

`config>service>vprn>if>sap>ingress>queue-override>queue`

**Description**

This command can be used to override specific attributes of the specified queue’s high-prio-only parameters. The `high-prio-only` command configures the percentage of buffer space for the queue, used exclusively by high priority packets.

The priority of a packet can only be set in the SAP ingress QoS policy and is only applicable on the ingress queues for a SAP. The `high-prio-only` parameter is used to override the default value derived from the `network-queue` command.

The defined `high-prio-only` value cannot be greater than the MBS size of the queue. Attempting to change the MBS to a value smaller than the high priority reserve will generate an error and fail execution. Attempting to set the `high-prio-only` value larger than the current MBS size will also result in an error and fail execution.

The no form of this command restores the default high priority reserved size.

**Parameters**

`percent` — The `percent` parameter is the percentage reserved for high priority traffic on the queue. If a value of 10KBytes is desired, enter the value 10. A value of 0 specifies that none of the MBS of the queue will be reserved for high priority traffic. This does not affect RED slope operation for packets attempting to be queued.

**Values**

0 — 100 | default

### mbs

**Syntax**

`mbs {size-in-kbytes | default}`
no mbs

Context  config>service>vprn>if>sap>egress>queue-override>queue
          config>service>vprn>if>sap>egress>hsmda-queue-override>queue

Description  This command can be used to override specific attributes of the specified queue’s MBS parameters. The MBS is a mechanism to override the default maximum size for the queue.

The sum of the MBS for all queues on an egress access port can oversubscribe the total amount of buffering available. When congestion occurs and buffers become scarce, access to buffers is controlled by the RED slope a packet is associated with. A queue that has not exceeded its MBS size is not guaranteed that a buffer will be available when needed or that the packet’s RED slope will not force the discard of the packet. Setting proper CBS parameters and controlling CBS oversubscription is one major safeguard to queue starvation (when a queue does not receive its fair share of buffers). Another is properly setting the RED slope parameters for the needs of services on this port or channel.

If the CBS value is larger than the MBS value, an error will occur, preventing the MBS change.

The no form of this command returns the MBS size assigned to the queue.

Default  default

Parameters  size-in-kbytes — The size parameter is an integer expression of the maximum number of kilobytes of buffering allowed for the queue. For a value of 100 kbps, enter the value 100. A value of 0 causes the queue to discard all packets.

Values  0 — 131072 or default

mbs

Syntax  mbs {size-in-kbytes | default}
         no mbs

Context  config>service>vprn>if>sap>ingress>queue-override>queue

Description  This command can be used to override specific attributes of the specified queue’s MBS parameters. The MBS value is used by a queue to determine whether it has exhausted all of its buffers while enqueuing packets. Once the queue has exceeded the amount of buffers allowed by MBS, all packets are discarded until packets have been drained from the queue.

The sum of the MBS for all queues on an ingress access port can oversubscribe the total amount of buffering available. When congestion occurs and buffers become scarce, access to buffers is controlled by the RED slope a packet is associated with. A queue that has not exceeded its MBS size is not guaranteed that a buffer will be available when needed or that the packet’s RED slope will not force the discard of the packet. Setting proper CBS parameters and controlling CBS oversubscription is one major safeguard to queue starvation (when a queue does not receive its fair share of buffers). Another is properly setting the RED slope parameters for the needs of services on this port or channel.

If the CBS value is larger than the MBS value, an error will occur, preventing the MBS change.

The defined high-prio-only value cannot be greater than the MBS size of the queue. Attempting to change the MBS to a value smaller than the high priority reserve will generate an error and fail execution. Attempting to set the high-prio-only value larger than the current MBS size will also result in an error and fail execution.
The **no** form of this command returns the MBS size assigned to the queue to the value.

**Default**

- `default`

**Parameters**

- `size-in-kbytes` — The size parameter is an integer expression of the maximum number of kilobytes of buffering allowed for the queue. For a value of 100 kbps, enter the value 100. A value of 0 causes the queue to discard all packets.

**Values**

- `0 — 131072 or default`

---

### rate

**Syntax**

```
rate pir-rate [cir cir-rate]
```

```
o rate
```

**Context**

```
config>service>vprn>if>sap>egress>queue-override>queue
```

```
config>service>vprn>if>sap>ingress>queue-override>queue
```

**Description**

This command can be used to override specific attributes of the specified queue’s Peak Information Rate (PIR) and the Committed Information Rate (CIR) parameters. The PIR defines the maximum rate that the queue can transmit packets out an egress interface (for SAP egress queues). Defining a PIR does not necessarily guarantee that the queue can transmit at the intended rate. The actual rate sustained by the queue can be limited by oversubscription factors or available egress bandwidth.

The CIR defines the rate at which the system prioritizes the queue over other queues competing for the same bandwidth. In-profile packets are preferentially queued by the system at egress and at subsequent next hop nodes where the packet can traverse. To be properly handled as in- or out-of-profile throughout the network, the packets must be marked accordingly for profiling at each hop.

The CIR can be used by the queue’s parent commands `cir-level` and `cir-weight` parameters to define the amount of bandwidth considered to be committed for the child queue during bandwidth allocation by the parent scheduler.

The **rate** command can be executed at any time, altering the PIR and CIR rates for all queues created through the association of the SAP egress QoS policy with the `queue-id`.

The **no** form of the command returns all queues created with the `queue-id` by association with the QoS policy to the default PIR and CIR parameters (**max**, 0).

**Default**

- `rate max cir 0` — The **max** default specifies the amount of bandwidth in kilobits per second (thousand bits per second). The **max** value is mutually exclusive to the **pir-rate** value.

**Parameters**

- `pir-rate` — Defines the administrative PIR rate, in kilobits, for the queue. When the **rate** command is executed, a valid PIR setting must be explicitly defined. When the **rate** command has not been executed, the default PIR of **max** is assumed.

  Fractional values are not allowed and must be given as a positive integer.

  The actual PIR rate is dependent on the queue’s **adaptation-rule** parameters and the actual hardware where the queue is provisioned.

**Values**

- `1 — 100000000`

**Default**

- `max`
Interface Commands

cir-rate — The cir parameter overrides the default administrative CIR used by the queue. When the rate command is executed, a CIR setting is optional. When the rate command has not been executed or the cir parameter is not explicitly specified, the default CIR (0) is assumed. Fractional values are not allowed and must be given as a positive integer. The sum keyword specifies that the CIR be used as the summed CIR values of the children schedulers or queues.

Values 0 — 100000000, max, sum
Default 0

rate

Syntax rate pir-rate
no rate

Context config>service>vprn>if>sap>egress>hsmda-queue-overide>queue

Description This command can be used to override specific attributes of the specified queue’s Peak Information Rate (PIR). The PIR defines the maximum rate that the queue can transmit packets out an egress interface (for SAP egress queues). Defining a PIR does not necessarily guarantee that the queue can transmit at the intended rate. The actual rate sustained by the queue can be limited by oversubscription factors or available egress bandwidth.

The rate command can be executed at any time, altering the PIR rates for all queues created through the association of the SAP egress QoS policy with the queue-id.

The no form of the command returns all queues created with the queue-id by association with the QoS policy to the default PIR parameters (max, 0).

Default pir-rate — Defines the administrative PIR rate, in kilobits, for the queue. When the rate command is executed, a valid PIR setting must be explicitly defined. When the rate command has not been executed, the default PIR of max is assumed. Fractional values are not allowed and must be given as a positive integer.

The actual PIR rate is dependent on the queue’s adaptation-rule parameters and the actual hardware where the queue is provisioned.

Values 1 — 100000000
Default max

scheduler-override

Syntax [no] scheduler-override

Context config>service>vprn>if>sap>egress
config>service>vprn>if>sap>ingress

Description This command specifies the set of attributes whose values have been overridden via management on this virtual scheduler. Clearing a given flag will return the corresponding overridden attribute to the value defined on the SAP’s ingress scheduler policy.
scheduler

Syntax

**scheduler** scheduler-name

**no scheduler** scheduler-name

Context

config>service>vprn>if.sap>egress>sched-override
config>service>vprn>if.sap>ingress>sched-override

Description

This command can be used to override specific attributes of the specified scheduler name.

A scheduler defines a bandwidth controls that limit each child (other schedulers and queues) associated with the scheduler. Scheduler objects are created within the hierarchical tiers of the policy. It is assumed that each scheduler created will have queues or other schedulers defined as child associations. The scheduler can be a child (take bandwidth from a scheduler in a higher tier, except for schedulers created in tier 1). A total of 32 schedulers can be created within a single scheduler policy with no restriction on the distribution between the tiers.

Each scheduler must have a unique name within the context of the scheduler policy; however the same name can be reused in multiple scheduler policies. If scheduler-name already exists within the policy tier level (regardless of the inclusion of the keyword create), the context changes to that scheduler name for the purpose of editing the scheduler parameters. Modifications made to an existing scheduler are executed on all instantiated schedulers created through association with the policy of the edited scheduler. This can cause queues or schedulers to become orphaned (invalid parent association) and adversely affect the ability of the system to enforce service level agreements (SLAs).

If the scheduler-name exists within the policy on a different tier (regardless of the inclusion of the keyword create), an error occurs and the current CLI context will not change.

If the scheduler-name does not exist in this or another tier within the scheduler policy, it is assumed that an attempt is being made to create a scheduler of that name. The success of the command execution is dependent on the following:

1. The maximum number of schedulers has not been configured.
2. The provided scheduler-name is valid.
3. The create keyword is entered with the command if the system is configured to require it (enabled in the environment create command).

When the maximum number of schedulers has been exceeded on the policy, a configuration error occurs and the command will not execute, nor will the CLI context change. If the provided scheduler-name is invalid according to the criteria below, a name syntax error will occur, the command will not execute, and the CLI context will not change.

Parameters

**scheduler-name** — The name of the scheduler.

**Values**
Valid names consist of any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

**Default**
None. Each scheduler must be explicitly created.

create — This optional keyword explicitly specifies that it is acceptable to create a scheduler with the given scheduler-name. If the create keyword is omitted, scheduler-name is not created when the system environment variable create is set to true. This safeguard is meant to avoid accidental
creation of system objects (such as schedulers) while attempting to edit an object with a mistyped name or ID. The keyword has no effect when the object already exists.

**rate**

**Syntax**

```
rate pir-rate [cir cir-rate]
no rate
```

**Context**

```
config>service>vprn>if>sap>egress>sched-override>scheduler
```

**Description**

This command can be used to override specific attributes of the specified scheduler rate. The `rate` command defines the maximum bandwidth that the scheduler can offer its child queues or schedulers. The maximum rate is limited to the amount of bandwidth the scheduler can receive from its parent scheduler. If the scheduler has no parent, the maximum rate is assumed to be the amount available to the scheduler. When a parent is associated with the scheduler, the CIR parameter provides the amount of bandwidth to be considered during the parent scheduler’s ‘within CIR’ distribution phase.

The actual operating rate of the scheduler is limited by bandwidth constraints other than its maximum rate. The scheduler’s parent scheduler may not have the available bandwidth to meet the scheduler’s needs or the bandwidth available to the parent scheduler could be allocated to other child schedulers or child queues on the parent based on higher priority. The children of the scheduler may not need the maximum rate available to the scheduler due to insufficient offered load or limits to their own maximum rates.

When a scheduler is defined without specifying a rate, the default rate is `max`. If the scheduler is a root scheduler (no parent defined), the default maximum rate must be changed to an explicit value. Without this explicit value, the scheduler will assume that an infinite amount of bandwidth is available and allow all child queues and schedulers to operate at their maximum rates.

The `no` form of this command returns all queues created with this `queue-id` by association with the QoS policy to the default PIR and CIR parameters.

**Parameters**

- `pir-rate` — The `pir` parameter accepts a step multiplier value that specifies the multiplier used to determine the PIR rate at which the queue will operate. A value of 0 to 100000000 or the keyword `max` or `sum` is accepted. Any other value will result in an error without modifying the current PIR rate.

  To calculate the actual PIR rate, the rate described by the queue’s `rate` is multiplied by the `pir-rate`.

  The SAP ingress context for PIR is independent of the defined forwarding class (fc) for the queue. The default `pir` and definable range is identical for each class. The PIR in effect for a queue defines the maximum rate at which the queue will be allowed to forward packets in a given second, thus shaping the queue’s output.

  The PIR parameter for SAP ingress queues do not have a negate (`no`) function. To return the queue’s PIR rate to the default value, that value must be specified as the PIR value.

**Values**

- `Values` 1 — 100000000, `max`

**Default**

- `max`
**cir cir-rate** — The cir parameter accepts a step-multiplier value that specifies the multiplier used to determine the CIR rate at which the queue will operate. A value of 0 to 250 or the keyword max is accepted. Any other value will result in an error without modifying the current CIR rate.

To calculate the actual CIR rate, the rate described by the rate pir pir-rate is multiplied by the cir cir-rate. If the cir is set to max, then the CIR rate is set to infinity.

The SAP ingress context for CIR is dependent on the defined forwarding class (fc) for the queue. The default CIR and definable range is different for each class. The CIR in effect for a queue defines both its profile (in or out) marking level as well as the relative importance compared to other queues for scheduling purposes during congestion periods.

<table>
<thead>
<tr>
<th>Values</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 — 10000000, max, sum</td>
<td>sum</td>
</tr>
</tbody>
</table>
**ETH-CFM Service Commands**

**eth-cfm**

**Syntax**

```
eth-cfm
```

**Context**

```
config>service>vprn
config>service>vprn>if>sap
config>service>vprn>if>spoke-sdp
```

**Description**

This command enables the context to configure ETH-CFM parameters.

**mep**

**Syntax**

```
mep mep-id domain md-index association ma-index [direction {up | down}]
no mep mep-id domain md-index association ma-index
```

**Context**

```
config>service>vprn>if>sap>eth-cfm
config>service>vprn>if>spoke-sdp>eth-cfm
```

**Description**

This command configures the ETH-CFM maintenance endpoint (MEP).

**Parameters**

- **mep-id** — Specifies the maintenance association end point identifier.
  - **Values**
    - 1 — 8191
- **domain**
- **md-index** — Specifies the maintenance domain (MD) index value.
  - **Values**
    - 1 — 4294967295
- **association**
- **ma-index** — Specifies the MA index value.
  - **Values**
    - 1 — 4294967295
- **direction up|down** — Indicates the direction in which the maintenance association (MEP) faces on the bridge port. Direction UP is not supported on VPRN MEPs.
  - **down** — Sends continuity check messages away from the MAC relay entity.
  - **up** — Sends continuity check messages towards the MAC relay entity.

**ais-enable**

**Syntax**

```
[no] ais-enable
```

**Context**

```
config>service>vprn>sap>eth-cfm>mep
config>service>vprn>if>spoke-sdp>eth-cfm
```

**Description**

This command configures the reception of Alarm Indication Signal (AIS) message.
interface-support-enable

Syntax  
[no] interface-support-enable

Context  
config>service>vprn>sap>eth-cfm>mep>ais-enable  
cfg>service>vprn>spoke-sdp>eth-cfm>mep>ais-enable

Description  
This command enables the AIS function to consider the operational state of the entity on which it is configured. With this command, ETH-AIS on DOWN MEPS will be triggered and cleared based on the operational status of the entity on which it is configured. If CCM is also enabled then transmission of the AIS PDU will be based on either the non operational state of the entity or on ANY CCM defect condition. AIS generation will cease if BOTH operational state is UP and CCM has no defect conditions. If the MEP is not CCM enabled then the operational state of the entity is the only consideration assuming this command is present for the MEP.

Default  
no interface-support-enabled (AIS will not be generated or stopped based on the state of the entity on) which the DOWN MEP is configured.

ccm-enable

Syntax  
[no] ccm-enable

Context  
config>service>vprn>if>sap>eth-cfm>mep  
cfg>service>vprn>if>spoke-sdp>eth-cfm>mep

Description  
This command enables the generation of CCM messages. The no form of the command disables the generation of CCM messages.

ccm-ltm-priority

Syntax  
ccm-ltm-priority priority  
no ccm-ltm-priority

Context  
config>service>vprn>if>sap>eth-cfm>mep  
cfg>service>vprn>if>spoke-sdp>eth-cfm>mep

Description  
This command specifies the priority value for CCMs and LTMs transmitted by the MEP. The no form of the command removes the priority value from the configuration.

Default  
The highest priority on the bridge-port.

Parameters  

priority — Specifies the priority of CCM and LTM messages.

Values  
0 — 7

ccm-padding-size

Syntax  
[no] ccm-padding-size ccm-padding
**ETH-CFM Service Commands**

### Context
config>service>vprn>interface>sap>eth-cfm>mep
config>service>vprn>interface>spoke-sdp>eth-cfm>mep
config>service>vprn>subscriber-interface>group-interface>sap>eth-cfm>mep

### Description
This command sets the byte size of the optional Data TLV to be included in the ETH-CC PDU. This will increase the size of the ETH-CC PDU by the configured value. The base size of the ETH-CC PDU, including the Interface Status TLV and Port Status TLV, is 83 bytes not including the Layer Two encapsulation. CCM padding is not supported when the CCM-Interval is less than one second.

### Default
ccm-padding-size

### Parameters
- **ccm-padding** — specifies the byte size of the Optional Data TLV
  - **Values** 3 — 1500

### csf-enable

#### Syntax
[no] csf-enable

#### Context
config>service>vprn>interface>sap>eth-cfm>mep
config>service>vprn>interface>spoke-sdp>eth-cfm>mep
config>service>vprn>subscriber-interface>group-interface>sap>eth-cfm>mep

#### Description
This command enables the reception and local processing of ETH-CSF frames.

### multiplier

#### Syntax
multiplier multiplier-value
no multiplier

#### Context
config>service>vprn>interface>sap>eth-cfm>mep>cfs-enable
config>service>vprn>interface>spoke-sdp>eth-cfm>mep>cfs-enable
config>service>vprn>subscriber-interface>group-interface>sap>eth-cfm>mep>cfs-enable

#### Description
This command enables the multiplication factor applied to the receive time used to clear the CSF condition in increments of .5.

#### Default
3.5

#### Parameters
- **multiplier-value** — Specifies the multiplier used for timing out CSF.
  - **Values** 0.0, 2.0 .. 30.0

### eth-test-enable

#### Syntax
[no] eth-test-enable

#### Context
config>service>vprn>if>sap>eth-cfm>mep
Description  This command enables eth-test functionality on MEP. For this test to work, operators need to configure ETH-test parameters on both sender and receiver nodes. The ETH-test then can be done using the following OAM commands:

```
oam eth-cfm eth-test mac-address mep mep-id domain md-index
association ma-index [priority priority] [data-length data-length]
```

A check is done for both the provisioning and test to ensure the MEP is an Y.1731 MEP (MEP provisioned with domain format none, association format icc-based). If not, the operation fails. An error message in the CLI and SNMP will indicate the problem.

test-pattern

 Syntax  `test-pattern {all-zeros | all-ones} [crc-enable]`

 Context  `config>service>vprn>if>sap>eth-cfm>mep>eth-test-enable`

 Description  This command configures the test pattern for eth-test frames.

 The `no` form of the command removes the values from the configuration.

 Parameters  `all-zeros` — Specifies to use all zeros in the test pattern.

 `all-ones` — Specifies to use all ones in the test pattern.

 `crc-enable` — Generates a CRC checksum.

 Default  all-zeros

bit-error-threshold

 Syntax  `bit-error-threshold bit-errors`

 Context  `config>service>vprn>if>sap>eth-cfm>mep`

 Description  This command specifies the lowest priority defect that is allowed to generate a fault alarm.

 Default  1

 Parameters  `bit-errors` — Specifies the lowest priority defect.

 Values  0 — 11840

one-way-delay-threshold

 Syntax  `one-way-delay-threshold time`

 Context  `config>service>vprn>if>sap>eth-cfm`

 `config>service>vprn>if>spoke-sdp>eth-cfm`
Description
This command enables one way delay threshold time limit.

Default
3 seconds

Parameters
priority — Specifies the value for the threshold.

<table>
<thead>
<tr>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 — 600</td>
</tr>
</tbody>
</table>

tunnel-fault

Syntax
tunnel-fault \{accept | ignore\}

Context
cfg>service>vprn>eth-cfm
cfg>service>vprn>if>sap>eth-cfm

description
Allows the individual service SAPs to react to changes in the tunnel MEP state. When tunnel-fault accept is configured at the service level, the SAP will react according to the service type. Epipe will set the operational flag and VPLS, IES and VPRN SAP operational state will become down on failure or up on clear. This command triggers the OAM mapping functions to mate SAPs and bindings in an Eppe service as well as setting the operational flag. If AIS generation is the requirement for the Eppe services this command is not required. See the command ais-enable under epipe>sap>eth-cfm>ais-enable for more details. This works in conjunction with the tunnel-fault accept on the individual SAPs. Both must be set to accept to react to the tunnel MEP state. By default the service level command is “ignore” and the sap level command is “accept”. This means simply changing the service level command to “accept” will enable the feature for all SAPs. This is not required for Eppe services that only wish to generate AIS on failure.

Parameters
accept — Share fate with the facility tunnel MEP
ignore — Do not share fate with the facility tunnel MEP

Default
ignore (Service Level)
accept (SAP Level for Eppe and VPLS)

fault-propagation-enable

Syntax
fault-propagation-enable \{use-if-tlv | suspend-ccm\)
no fault-propagation-enable

Context
cfg>service>vprn>if>sap>eth-cfm>mep
cfg>service>vprn>if>spoke-sdp>eth-cfm>mep

description
This command configures the fault propagation for the MEP.

Parameters
use-if-tlv — Specifies to use the interface TLV.
suspend-ccm — Specifies to suspend the continuity check messages.

low-priority-defect
Syntax  low-priority-defect (allDef | macRemErrXcon | remErrXcon | errXcon | xcon | noXcon)

Context  config>service>vprn>if>sap>eth-cfm>mep
         config>service>vprn>if>spoke-sdp>eth-cfm>mep

Description  This command specifies the lowest priority defect that is allowed to generate a fault alarm.

Default  macRemErrXcon

Values

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>allDef</td>
<td>DefRDICCM, DefMACstatus, DefRemoteCCM, DefErrorCCM, and DefXconCCM</td>
</tr>
<tr>
<td>macRemErrXcon</td>
<td>Only DefMACstatus, DefRemoteCCM, DefErrorCCM, and DefXconCCM</td>
</tr>
<tr>
<td>remErrXcon</td>
<td>Only DefRemoteCCM, DefErrorCCM, and DefXconCCM</td>
</tr>
<tr>
<td>errXcon</td>
<td>Only DefErrorCCM and DefXconCCM</td>
</tr>
<tr>
<td>xcon</td>
<td>Only DefXconCCM; or</td>
</tr>
<tr>
<td>noXcon</td>
<td>No defects DefXcon or lower are to be reported</td>
</tr>
</tbody>
</table>
Interface VRRP Commands

**vrrp**

**Syntax**

```
vrrp virtual-router-id [owner]
no vrrp virtual-router-id
```

**Context**

```
config>service>vprn>if
```

**Description**

This command creates or edits a Virtual Router ID (VRID) on the service IP interface. A VRID is internally represented in conjunction with the IP interface name. This allows the VRID to be used on multiple IP interfaces while representing different virtual router instances.

Two VRRP nodes can be defined on an IP interface. One, both, or none may be defined as owner. The nodal context of vrrp virtual-router-id is used to define the configuration parameters for the VRID.

The **no** form of this command removes the specified VRID from the IP interface. This terminates VRRP participation for the virtual router and deletes all references to the VRID. The VRID does not need to be shutdown in order to remove the virtual router instance.

**Default**

No default

**Parameters**

- `virtual-router-id` — The virtual-router-id parameter specifies a new virtual router ID or one that can be modified on the IP interface.

  **Values**

  - `1 — 255`

**authentication-key**

**Syntax**

```
authentication-key [authentication-key | hash-key] [hash | hash2]
no authentication-key
```

**Context**

```
config>service>vprn>if>vrrp
```

**Description**

The `authentication-key` command, within the vrrp `virtual-router-id` context, is used to assign a simple text password authentication key to generate master VRRP advertisement messages and validate received VRRP advertisement messages.

The `authentication-key` command is one of the few commands not affected by the presence of the `owner` keyword. If simple text password authentication is not required, this command is not required. If the command is re-executed with a different password key defined, the new key will be used immediately. If a **no** `authentication-key` command is executed, the password authentication key is restored to the default value. The `authentication-key` command may be executed at any time, altering the simple text password used when `authentication-type password` authentication method is used by the virtual router instance. The `authentication-type password` command does not need to be executed prior to defining the `authentication-key` command.

To change the current in-use password key on multiple virtual router instances:

- Identify the current master
Virtual Private Routed Network Services

- Shutdown the virtual router instance on all backups
- Execute the authentication-key command on the master to change the password key
- Execute the authentication-key command and no shutdown command on each backup key

The `no` form of this command restores the default null string to the value of key.

**Default**

No default. The authentication data field contains the value 0 in all 16 octets.

**Parameters**

`authentication-key` — The `key` parameter identifies the simple text password used when VRRP Authentication Type 1 is enabled on the virtual router instance. Type 1 uses a string eight octets long that is inserted into all transmitted VRRP advertisement messages and compared against all received VRRP advertisement messages. The authentication data fields are used to transmit the key.

The `key` parameter is expressed as a string consisting of up to eight alpha-numeric characters. Spaces must be contained in quotation marks (" "). The quotation marks are not considered part of the string.

The string is case sensitive and is left-justified in the VRRP advertisement message authentication data fields. The first field contains the first four characters with the first octet (starting with IETF RFC bit position 0) containing the first character. The second field holds the fifth through eighth characters. Any unspecified portion of the authentication data field is padded with the value 0 in the corresponding octet.

**Values**

Any 7-bit printable ASCII character.

Exceptions: Double quote (") ASCII 34
Carriage Return ASCII 13
Line Feed ASCII 10
Tab ASCII 9
Backspace ASCII 8

`hash-key` — The hash key. The key can be any combination of ASCII characters up to 22 characters in length (encrypted). If spaces are used in the string, enclose the entire string in quotation marks (" ").

This is useful when a user must configure the parameter, but, for security purposes, the actual unencrypted key value is not provided.

`hash` — Specifies the key is entered in an encrypted form. If the `hash` parameter is not used, the key is assumed to be in a non-encrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the `hash` parameter specified.

`hash2` — Specifies the key is entered in a more complex encrypted form. If the `hash2` parameter is not used, the less encrypted `hash` form is assumed.

authentication-type

**Syntax**

`authentication-type {password | message-digest}`

`no authentication-type`

**Context**

`config>service>vprn>if>vrrp`
**Description**

The `authentication-type` command, within the `vrrp virtual-router-id` context, is used to assign the authentication method to generate master VRRP advertisement messages and validate received VRRP advertisement messages.

**NOTE:** The authentication management for VRRP closely follows the authentication management format used for IS-IS.

The `authentication-type` command is one of the commands not affected by the presence of the owner keyword. If authentication is not required, the authentication-type command must not be executed. If the command is re-executed with a different authentication type defined, the new type will be used. If the no authentication-type command is executed, authentication is removed and no authentication is performed. The authentication-type command may be executed at any time, altering the authentication method used by the virtual router instance.

The `no` form of this command removes authentication from the virtual router instance. All VRRP Advertisement messages sent will have the Authentication Type field set to 0 and the Authentication Data fields will contain 0 in all octets. VRRP Advertisement messages received with Authentication Type fields containing a value other than 0 will be discarded.

`password` — The password keyword identifies VRRP Authentication Type 1. Type 1 requires the definition of a string of eight octets long using the `authentication-key` command. All transmitted VRRP Advertisement messages must have the Authentication Type field set to 1 and the Authentication Data fields must contain the authentication-key password.

All received VRRP advertisement messages must contain a value of 1 in the Authentication Type field and the Authentication Data fields must match the defined authentication-key. All other received messages will be silently discarded.

`message-digest` — The message-digest keyword identifies VRRP Authentication Type 2. Type 2 defines a lower IP layer MD5 authentication mechanism using HMAC and IP authentication header standards. An MD5 key must be defined using the `message-digest-key` command. All transmitted VRRP advertisement messages must have the Authentication Type field set to 2 and the Authentication Data fields must contain 0 in all octets. The message-digest key is used in the hashing process when populating the IP Authentication Header fields. A sequential incrementing counter (set to zero when the message-digest-key is set) is incremented and then used in the IP Authentication Header to prevent replay attacks on authorized participating virtual router instances.

All received VRRP advertisement messages must contain a value of 2 in the Authentication Type field and the Authentication Data fields are ignored. The message must have been authorized by the lower layer IP Authentication Header process with the sequential counter field and the source IP address presented to the virtual router instance. To track the validity of the received counter, the virtual router instance maintains a master counter table containing up to 32 source IP addresses and the last received counter value. Populate the table as follows:

1. Check to see if source IP address exists in table.
   - If non-existent, create an entry if available.
   - If no entry is available, delete the oldest and create an entry.
   The new entry should have a counter value of zero.
2. Compare the message counter value to the entry value (0 if new entry or equal to the previous message counter from the source IP address).
   - If the message counter is not greater than the entry counter value, silently discard the packet.
backup

**Syntax**

```
[no] backup ip-address
```

**Context**

config>service>vprn>if>vrrp
config>service>vprn>if>ipv6>vrrp

**Description**

This command configures virtual router IP addresses for the interface.

bfd-enable

**Syntax**

```
bfd-enable interface interface-name dst-ip ip-address
bfd-enable service-id interface interface-name dst-ip ip-address
no bfd-enable interface interface-name dst-ip ip-address
no bfd-enable service-id interface interface-name dst-ip ip-address
```

**Context**

config>service>vprn>if>vrrp
config>service>vprn>if>ipv6>vrrp

**Description**

This commands assigns a bi-directional forwarding (BFD) session providing heart-beat mechanism for the given VRRP/SRRP instance. There can be only one BFD session assigned to any given VRRP/SRRP instance, but there can be multiple SRRP/VRRP sessions using the same BFD session. If the interface used is configured with centralized BFD, the BFD transmit and receive intervals need to be set to at least 300ms.

BFD control the state of the associated interface. By enabling BFD on a given protocol interface, the state of the protocol interface is tied to the state of the BFD session between the local node and the remote node. The parameters used for the BFD are set via the BFD command under the IP interface. The specified interface may not be configured with BFD; when it is, the virtual router will then initiate the BFD session.

The **no** form of this command removes BFD from the configuration.

**Default**

none

**Parameters**

- **service-id** — Specifies the service ID of the interface running BFD.
  
  **Values**
  
  service-id: 1 — 2147483648
  
  svc-name: Specifies an existing service name up to 64 characters in length.
  
  No service ID indicates a network interface.
  
- **interface interface-name** — Specifies the name of the interface running BFD.
  
- **dst-ip ip-address** — Specifies the destination address to be used for the BFD session.

init-delay
init-delay

Syntax
init-delay seconds
no init-delay

Context
config>service>vprn>if>vrrp
config>service>vprn>if>ipv6>vrrp

Description
This command configures a VRRP initialization delay timer.

Default
no init-delay

Parameters
seconds — Specifies the initialization delay timer for VRRP, in seconds.

Values
1 — 65535

mac

Syntax
[no] mac ieee-mac-address

Context
config>service>vprn>if>vrrp
config>service>vprn>if>ipv6>vrrp

Description
This command assigns a specific MAC address to an IP interface.

The no form of this command returns the MAC address of the IP interface to the default value.

Default
The physical MAC address associated with the Ethernet interface that the SAP is configured on.

Parameters
ieee-mac-address — Specifies the 48-bit MAC address for the static ARP in the form
aa:bb:cc:dd:ee:ff or aa-bb-cc-dd-ee ff where aa, bb, cc, dd, ee and ff are hexadecimal numbers.
Allowed values are any non-broadcast, non-multicast MAC and non-IEEE reserved MAC addresses.

master-int-inherit

Syntax
[no] master-int-inherit

Context
config>service>vprn>if>vrrp
config>service>vprn>if>ipv6>vrrp

Description
This command allows the master instance to dictate the master down timer (non-owner context only).

Default
no master-int-inherit

message-interval

Syntax
message-interval {[[seconds] [milliseconds milliseconds]]
no message-interval

Context
config>service>vprn>if
config>service>vprn>if>ipv6>vrrp
Description

This command sets the advertisement timer and indirectly sets the master down timer on the virtual router instance. The message-interval setting must be the same for all virtual routers participating as a virtual router. Any VRRP advertisement message received with an Advertisement Interval field different than the virtual router instance configured message-interval value will be silently discarded.

The message-interval command is available in both non-owner and owner vrrp virtual-router-id nodal contexts. If the message-interval command is not executed, the default message interval of 1 second will be used.

The no form of this command restores the default message interval value of 1 second to the virtual router instance.

Parameters

seconds — The number of seconds that will transpire before the advertisement timer expires.

Values 1 — 255

Default 1

milliseconds milliseconds — Specifies the milliseconds time interval between sending advertisement messages. This parameter is not supported on single-slot chassis.

Values 100 — 900

ping-reply

Syntax [no] ping-reply

Context config>service>vprn>if>vrrp
config>service>vprn>if>ipv6>vrrp

Description

This command enables the non-owner master to reply to ICMP Echo Requests directed at the virtual router instances IP addresses. The ping request can be received on any routed interface.

Ping must not have been disabled at the management security level (either on the parental IP interface or based on the Ping source host address). When ping-reply is not enabled, ICMP Echo Requests to non-owner master virtual IP addresses are silently discarded.

Non-owner backup virtual routers never respond to ICMP Echo Requests regardless of the setting of ping-reply configuration.

The ping-reply command is only available in non-owner vrrp virtual-router-id nodal context. If the ping-reply command is not executed, ICMP Echo Requests to the virtual router instance IP addresses will be silently discarded.

The no form of this command restores the default operation of discarding all ICMP Echo Request messages destined to the non-owner virtual router instance IP addresses.

Default no ping-reply

policy

Syntax policy vrrp-policy-id
no policy
**Context**
cfg>service>vprn>if>vrrp

cfg>service>vprn>if>ipv6>vrrp

**Description**
This command associates a VRRP priority control policy with the virtual router instance (non-owner context only).

**Parameters**

- **vrrp-policy-id** — Specifies a VRRP priority control policy.
  
  **Values**
  
  1 — 9999

**preempt**

- **Syntax**
  
  preempt
  
  no preempt

- **Context**
  
  cfg>service>vprn>if
  
  cfg>service>vprn>if>ipv6>vrrp

- **Description**
  
  This command provides the ability of overriding an existing non-owner master to the virtual router instance. Enabling preempt mode is recommended for proper operation of the base-priority and vrrp-policy-id definitions on the virtual router instance. If the virtual router cannot preempt an existing non-owner master, the effect of the dynamic changing of the in-use priority is greatly diminished.

  The preempt command is only available in the non-owner **vrrp virtual-router-id** nodal context. The owner may not be preempted due to the fact that the priority of non-owners can never be higher than the owner. The owner will always preempt all other virtual routers when it is available.

  Non-owner virtual router instances will only preempt when preempt is set and the current master has an in-use message priority value less than the virtual router instances in-use priority.

  A master non-owner virtual router will only allow itself to be preempted when the incoming VRRP Advertisement message Priority field value is one of the following:

  - Greater than the virtual router in-use priority value
  - Equal to the in-use priority value and the source IP address (primary IP address) is greater than the virtual router instance primary IP address

  The **no** form of this command prevents a non-owner virtual router instance from preempting another, less desirable virtual router. Use the preempt command to restore the default mode.

  **Default**
  
  preempt

**priority**

- **Syntax**
  
  priority priority
  
  no priority

- **Context**
  
  cfg>service>vprn>if>vrrp
  
  cfg>service>vprn>if>ipv6>vrrp
**Description**  
The priority command provides the ability to configure a specific priority value to the virtual router instance. In conjunction with an optional policy command, the base-priority is used to derive the in-use priority of the virtual router instance.

The priority command is only available in the non-owner `vrrp virtual-router-id` nodal context. The priority of owner virtual router instances is permanently set to 255 and cannot be changed. For non-owner virtual router instances, if the priority command is not executed, the base-priority will be set to 100.

The `no` form of this command restores the default value of 100 to base-priority.

**Parameters**  
`base-priority` — The base-priority parameter configures the base priority used by the virtual router instance. If a VRRP priority control policy is not also defined, the base-priority will be the in-use priority for the virtual router instance.

- **Values**  
  1 — 254
- **Default**  
  100

---

**ssh-reply**

**Syntax**  
`[no] ssh-reply`

**Context**  
`config>service>vprn>if>vrrp`

**Description**  
This command enables the non-owner master to reply to SSH Requests directed at the virtual router instance’s IP addresses. The SSH request can be received on any routed interface. SSH must not have been disabled at the management security level (either on the parental IP interface or based on the SSH source host address). Proper login and CLI command authentication is still enforced.

When `ssh-reply` is not enabled, SSH packets to non-owner master virtual IP addresses are silently discarded. Non-owner backup virtual routers never respond to SSH regardless of the `ssh-reply` configuration.

The `ssh-reply` command is only available in non-owner `vrrp virtual-router-id` nodal context. If the `ssh-reply` command is not executed, SSH packets to the virtual router instance IP addresses will be silently discarded.

The `no` form of this command restores the default operation of discarding all SSH packets destined to the non-owner virtual router instance IP addresses.

- **Default**  
  `no ssh-reply`

---

**standby-forwarding**

**Syntax**  
`[no] standby-forwarding`

**Context**  
`config>service>vprn>if>vrrp`

**Description**  
This command allows the forwarding of packets by a standby router.
The `no` form of the command specifies that a standby router should not forward traffic sent to virtual router's MAC address. However, the standby router should forward traffic sent to the standby router’s real MAC address.

**Default**

no standby-forwarding

telnet-reply

**Syntax**

`[no] telnet-reply`

**Context**

`config>service>vprn>if>vrrp`
`config>service>vprn>if>ipv6>vrrp`

**Description**

This command enables the non-owner master to reply to TCP port 23 Telnet Requests directed at the virtual router instance’s IP addresses. The Telnet request can be received on any routed interface. Telnet must not have been disabled at the management security level (either on the parental IP interface or based on the Telnet source host address). Proper login and CLI command authentication is still enforced.

When telnet-reply is not enabled, TCP port 23 Telnet packets to non-owner master virtual IP addresses are silently discarded.

Non-owner backup virtual routers never respond to Telnet Requests regardless of the telnet-reply configuration.

The telnet-reply command is only available in non-owner VRRP nodal context. If the telnet-reply command is not executed, Telnet packets to the virtual router instance IP addresses will be silently discarded.

The `no` form of this command restores the default operation of discarding all Telnet packets destined to the non-owner virtual router instance IP addresses.

**Default**

no telnet-reply

traceroute-reply

**Syntax**

`[no] traceroute-reply`

**Context**

`config>service>vprn>if>vrrp`
`config>service>vprn>if>ipv6>vrrp`

**Description**

This command is valid only if the VRRP virtual router instance associated with this entry is a non-owner.

When this command is enabled, a non-owner master can reply to traceroute requests directed to the virtual router instance IP addresses.

A non-owner backup virtual router never responds to such traceroute requests regardless of the traceroute-reply status.

**Default**

no traceroute-reply
PIM Commands

pim

Syntax  
[no] pim

Context  
config>service>vprn

Description  
This command configures a Protocol Independent Multicast (PIM) instance in the VPRN service. When an PIM instance is created, the protocol is enabled. PIM is used for multicast routing within the network. Devices in the network can receive the multicast feed requested and non-participating routers can be pruned. The router supports PIM sparse mode (PIM-SM).

The no form of the command deletes the PIM protocol instance removing all associated configuration parameters.

Default  
none

apply-to

Syntax  
apply-to {all | none}

Context  
config>service>vprn>pim

Description  
This command creates a PIM interface with default parameters. If a manually created interface or modified interface is deleted, the interface will be recreated when the apply-to command is executed. If PIM is not required on a specific interface, then execute a shutdown command.

The apply-to command is saved first in the PIM configuration structure, all subsequent commands either create new structures or modify the defaults as created by the apply-to command.

Default  
none (keyword)

Parameters  
all — Specifies that all VPRN and non-VPRN interfaces are automatically applied in PIM.

none — No interfaces are automatically applied in PIM. PIM interfaces must be manually configured.

import

Syntax  
import {join-policy | register-policy} [policy-name [.. policy-name] policy-name]

no import {join-policy | register-policy}

Context  
config>service>vprn>pim
**PIM Commands**

**Description**
This command specifies the import route policy to be used for determining which routes are accepted from peers. Route policies are configured in the `config>router>policy-options` context. When an import policy is not specified, BGP routes are accepted by default.

The **no** form of the command removes the policy association from the IGMP instance.

**Default**
no import join-policy
no import register-policy

**Parameters**
- **join-policy** — Use this command to filter PIM join messages which prevents unwanted multicast streams from traversing the network.
- **register-policy** — This keyword filters register messages. PIM register filters prevent register messages from being processed by the RP. This filter can only be defined on an RP. When a match is found, the RP immediately sends back a register-stop message.
- **policy-name** — The route policy name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes. Route policies are configured in the `config>router>policy-options` context.

**interface**

**Syntax**
```
[no] interface ip-int-name
```

**Context**
`config>service>vprn>pim`

**Description**
This command enables PIM on an interface and enables the context to configure interface-specific parameters. By default interfaces are activated in PIM based on the **apply-to** command, and do not have to be configured on an individual basis unless the default values must be changed.

The **no** form of the command deletes the PIM interface configuration for this interface. If the **apply-to** command parameter is configured, then the **no interface** form must be saved in the configuration to avoid automatic (re)creation after the next **apply-to** is executed as part of a reboot.

The **shutdown** command can be used to disable an interface without removing the configuration for the interface.

**Default**
Interfaces are activated in PIM based on the apply-to command.

**Parameters**
- **ip-int-name** — Specify the interface name. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

**assert-period**

**Syntax**
```
assert-period assert-period
no assert-period
```

**Context**
`config>service>vprn>pim>if`

**Description**
This command configures the period in seconds for periodic refreshes of PIM Assert messages on an interface.
The no form of the command reverts to the default.

**bff-enable**

**Syntax**

```plaintext
[bfd-enable | no bfd-enable [ipv4|ipv6]]
```

**Context**

`config>service>vprn>pim>if`

**Description**

This command enables the use of bi-directional forwarding (BFD) to control the state of the associated protocol interface. By enabling BFD on a given protocol interface, the state of the protocol interface is tied to the state of the BFD session between the local node and the remote node. The parameters used for the BFD are set via the BFD command under the IP interface. The no form of this command removes BFD from the associated IGP protocol adjacency.

**Default**

`no bfd-enable`

**bssh-check-rtr-alert**

**Syntax**

```plaintext
[no] bssh-check-rtr-alert
```

**Context**

`config>service>vprn>pim>if`

**Description**

This command enables the checking of router alert option in the bootstrap messages received on this interface.

**Default**

`no bssh-check-rtr-alert`

**hello-interval**

**Syntax**

```plaintext
hello-interval  hello-interval
no hello-interval
```

**Context**

`config>service>vprn>pim>if`

**Description**

This command configures the frequency at which PIM Hello messages are transmitted on this interface. The no form of this command reverts to the default value.

**Default**

`30`

**Parameters**

`hello-interval` — Specifies the hello interval in seconds. A 0 (zero) value disables the sending of hello messages.
hello-multiplier

Syntax

```
hello-multiplier deci-units
no hello-multiplier
```

Context

`config>service>vprn>pim>if`

Description

This command configures the multiplier to determine the holdtime for a PIM neighbor.

The `hello-multiplier` in conjunction with the `hello-interval` determines the holdtime for a PIM neighbor.

Parameters

- `deci-units` — Specify the value, specified in multiples of 0.1, for the formula used to calculate the hello-holdtime based on the hello-multiplier:

  \[
  \text{hello-holdtime} = \frac{(\text{hello-interval} \times \text{hello-multiplier})}{10}
  \]

  This allows the PIMv2 default timeout of 3.5 seconds to be supported.

Values

- 20 — 100
- Default: 35

improved-assert

Syntax

```
[no] improved-assert
```

Context

`config>service>vprn>pim>if`

Description

This command enables improved assert processing on this interface. The PIM assert process establishes a forwarder for a LAN and requires interaction between the control and forwarding planes.

The assert process is started when data is received on an outgoing interface. This could impact performance if data is continuously received on an outgoing interface.

When enabled, the PIM assert process is done entirely on the control-plane with no interaction between the control and forwarding plane.

Default

- enabled

instant-prune-echo

Syntax

```
[no] instant-prune-echo
```

max-groups
Syntax  max-groups value  
no max-groups

Context  config>service>vprn>pim>if

Description  This command configures the maximum number of groups for which PIM can have downstream state based on received PIM Joins on this interface. This does not include IGMP local receivers on the interface. When this configuration is changed dynamically to a value lower than the currently accepted number of groups, the groups that are already accepted are not deleted. Only new groups will not be allowed. When this object has a value of 0, there is no limit to the number of groups.

Parameters  value — Specifies the maximum number of groups for this interface.  

Values  1 — 16000

multicast-senders

Syntax  multicast-senders {auto | always | never}  
no multicast-senders

Context  config>service>vprn>pim>if

Description  This command configures the way subnet matching is done for incoming data packets on this interface. An IP multicast sender is an user entity to be authenticated in a receiving host.

Parameters  auto — Subnet matching is automatically performed for incoming data packets on this interface.  
always — Subnet matching is always performed for incoming data packets on this interface.  
never — Subnet matching is never performed for incoming data packets on this interface.

priority

Syntax  priority dr-priority  
no priority

Context  config>service>vprn>pim>if

Description  This command sets the priority value to become the rendezvous point (RP) that is included in bootstrap messages sent by the router. The RP is sometimes called the bootstrap router. The priority command indicates whether the router is eligible to be a bootstrap router. The no form of the command disqualifies the router to participate in the bootstrap election.

Default  1 (The router is the least likely to become the designated router.)

Parameters  dr-priority — Specifies the priority to become the designated router. The higher the value, the higher the priority.  

Values  1 — 4294967295
stickyc-dr

Syntax

stickyc-dr [priority dr-priority]
no stickyc-dr

Context
config>service>vprn>pim>if

Description
This command enables stickyc-dr operation on this interface. When enabled, the priority in PIM hellos sent on this interface when elected as the designateed router (DR) will be modified to the value configured in dr-priority. This is done to avoid the delays in forwarding caused by DR recovery, when switching back to the old DR on a LAN when it comes back up.

By enabling stickyc-dr on this interface, it will continue to act as the DR for the LAN even after the old DR comes back up.

The no form of the command disables stickyc-dr operation on this interface.

Default
disabled

Parameters

priority dr-priority — Sets the DR priority to be sent in PIM Hello messages following the election of that interface as the DR, when stickyc-dr operation is enabled.

Values
1 — 4294967295

three-way-hello

Syntax

three-way-hello [compatibility-mode]
no three-way-hello

Context
config>service>vprn>pim>if

Description
This command configures the compatibility mode for enabling the three way hello.

Parameters
compatibility-mode — Specifies to enable the three way hello.

tracking-support

Syntax

[no] tracking-support

Context
config>service>vprn>pim>if

Description
This command sets the T bit in the LAN Prune Delay option of the Hello Message. This indicates the router's capability to disable Join message suppression.

Default
no tracking-support
ipv4-multicast-disable

Syntax  

[no] ipv4-multicast-disable

Context  

config>service>vprn>pim  
config>service>vprn>pim>interface

Description  This command administratively disables/enables PIM operation for IPv4.

Default  

no ipv4-multicast-disable

ipv6-multicast-disable

Syntax  

ipv6-multicast-disable

Context  

config>service>vprn>pim  
config>service>vprn>pim>interface

Description  This command administratively disables/enables PIM operation for IPv6.

Default  

ipv6-multicast-disable

mc-ecmp-balance

Syntax  

[no] mc-ecmp-balance

Context  

config>service>vprn>pim

Description  This command enables multicast balancing of traffic over ECMP links. When enabled, each multicast stream that needs to be forwarded over an ECMP link will be re-evaluated for the total multicast bandwidth utilization. Re-evaluation occurs on the ECMP interface in question.  

The no form of the command disables the multicast balancing.

mc-ecmp-balance-hold

Syntax  

mc-ecmp-balance-hold minutes  
no mc-ecmp-balance-hold

Context  

config>service>vprn>pim

Description  This command configures the hold time for multicast balancing over ECMP links.

Parameters  

minutes — Specifies the hold time, in minutes, that applies after an interface has been added to the ECMP link.

non-dr-attract-traffic
**Syntax**

\[ \text{no\ non-dr-attract-traffic} \]

**Context**

config>service>vprn>pim

**Description**

This command specifies whether the router should ignore the designated router state and attract traffic even when it is not the designater router.

An operator can configure an interface (router or IES or VPRN interfaces) to IGMP and PIM. The interface IGMP state will be synchronized to the backup node if it is associated with the redundant peer port. The interface can be configured to use PIM which will cause multicast streams to be sent to the elected DR only. The DR will also be the router sending traffic to the DSLAM. Since it may be required to attract traffic to both routers a flag \text{non-dr-attract-traffic} can be used in the PIM context to have the router ignore the DR state and attract traffic when not DR. Note that while using this flag the router may not send the stream down to the DSLAM while not DR.

When enabled, the designated router state is ignored. When disabled, \text{no\ non-dr-attract-traffic}, the designated router value is honored.

**Default**

\text{no\ non-dr-attract-traffic}

---

**rp**

**Syntax**

\text{rp}

**Context**

config>service>vprn>pim

**Description**

This command enables access to the context to configure the rendezvous point (RP) of a PIM protocol instance.

An Alcatel-Lucent PIM router acting as an RP must respond to a PIM register message specifying an SSM multicast group address by sending to the first hop router stop register message(s). It does not build an (S, G) shortest path tree toward the first hop router. An SSM multicast group address can be either from the SSM default range of 232/8 or from a multicast group address range that was explicitly configured for SSM.

**Default**

rp enabled when PIM is enabled.

---

**anycast**

**Syntax**

\[ \text{no\ anycast\ rp-ip-address} \]

**Context**

config>service>vprn>pim>rp

**Description**

This command configures a PIM anycast protocol instance for the RP being configured. Anycast enables fast convergence when a PIM RP router fails by allowing receivers and sources to rendezvous at the closest RP.

The \text{no} form of the command removes the anycast instance from the configuration.

**Default**

none

**Parameters**

\text{rp-ip-address} — Configure the loopback IP address shared by all routes that form the RP set for this anycast instance. Only a single address can be configured. If another anycast command is entered
with an address then the old address will be replaced with the new address. If no ip-address is entered then the command is simply used to enter the anycast CLI level.

Values
Any valid loopback address configured on the node.

rp-set-peer

Syntax
[no] rp-set-peer ip-address

Context
config>service>vprn>pim>rp>anycast

Description
This command configures a peer in the anycast rp-set. The address identifies the address used by the other node as the RP candidacy address for the same multicast group address range as configured on this node.

This is a manual procedure. Caution should be taken to produce a consistent configuration of an RP-set for a given multicast group address range. The priority should be identical on each node and be a higher value than any other configured RP candidate that is not a member of this rp-set.

Although there is no set maximum of addresses that can be configured in an rp-set, up to 15 multicast addresses is recommended.

The no form of the command removes an entry from the list.

Default
None

Parameters
ip-address — Specifies the address used by the other node as the RP candidacy address for the same multicast group address range as configured on this node.

auto-rp-discovery

Syntax
[no] auto-rp-discovery

Context
config>service>vprn>pim>rp

Description
This command enables Auto-RP protocol in discovery mode. In discovery mode, RP-mapping and RP-candidate messages are received and forwarded to downstream nodes. RP-mapping messages are received locally to learn about availability of RP nodes present in the network.

The no form of the command disables auto RP.

Default
disabled

bootstrap-export

Syntax
bootstrap-export policy-name [policy-name... up to five]
no bootstrap-export

Context
config>service>vprn>pim>rp
**bootstrap-import**

**Syntax**

`bootstrap-import policy-name [policy-name... up to five]`

`no bootstrap-import policy-name [policy-name... up to five]`

**Context**

config>service>vprn>pim>rp

**Description**

This command imports policies to control the flow of bootstrap messages into the RP. Up to five policies can be defined.

The **no** form of this command removes the specified policy names from the configuration.

**Default**

none

**Parameters**

`policy-name` — Specify the policy name. The policy statement must already be configured in the config>router>policy-options context.

---

**address**

**Syntax**

`[no] address ip-address`

**Context**

config>service>vprn>pim>rp>bsr-candidate

config>service>vprn>pim>rp>rp-candidate

**Description**

This command configures a static bootstrap or rendezvous point (RP) as long as the source is not directly attached to this router.

Use the **no** form of this command to remove the static RP from the configuration.

---

**PIM Commands**

**Description**

This command exports policies to control the flow of bootstrap messages from the RP. Up to five policies can be defined.

The **no** form of this command removes the specified policy names from the configuration.

**Default**

none

**Parameters**

`policy-name` — Specify the policy name. The policy statement must already be configured in the config>router>policy-options context.

---

**bsr-candidate**

**Syntax**

`bsr-candidate`

**Context**

config>service>vprn>pim>rp

config>service>vprn>pim>rp>ipv6

**Description**

This command enables the context to configure a local rendezvous point (RP) of a PIM protocol instance.

**Default**

Enabled when PIM is enabled.
Default

No IP address is specified.

Parameters

*ip-address* — The static IP address of the RP. The *ip-address* portion of the address command specifies the IP host address that will be used by the IP interface within the subnet. This address must be unique within the subnet and specified in dotted decimal notation.

**Values**

1.0.0.0 – 223.255.255.255

address

**Syntax**

[no] address *ipv6-address*

**Context**

config>service>vprn>pim>rp>ipv6>bsr-candidate

cfg>service>vprn>pim>rp>ipv6>rp-candidate

**Description**

This command configures a static bootstrap or rendezvous point (RP) as long as the source is not directly attached to this router.

Use the no form of this command to remove the static RP from the configuration.

Default

No IP address is specified.

Parameters

*ipv6-address* — The static IP address of the RP. The *ip-address* portion of the address command specifies the IP host address that will be used by the IP interface within the subnet. This address must be unique within the subnet and specified in dotted decimal notation.

**Values**

ipv6-address : x:x:x:x:x:x:x:x (eight 16-bit pieces)

x:x:x:x:x:d.d.d

x [0..FFFF]H

d [0..255]D

hash-mask-len

**Syntax**

hash-mask-len *hash-mask-length*

no hash-mask-len

**Context**

config>service>vprn>pim>rp>bsr-candidate

**Description**

This command is used to configure the length of a mask that is to be combined with the group address before the hash function is called. All groups with the same hash map to the same RP. For example, if this value is 24, only the first 24 bits of the group addresses matter. This mechanism is used to map one group or multiple groups to an RP.

Default

30

Parameters

*hash-mask-length* — The hash mask length.

**Values**

0 — 32

hash-mask-length
Syntax hash-mask-length hash-mask-length
no hash-mask-length

Context config>service>vprn>pim>rp>ipv6>bsr-candidate

Description This command is used to configure the length of a mask that is to be combined with the group address before the hash function is called. All groups with the same hash map to the same RP. For example, if this value is 24, only the first 24 bits of the group addresses matter. This mechanism is used to map one group or multiple groups to an RP.

Default 126

Parameters hash-mask-length — The hash mask length.

Values 0 — 128

priority

Syntax priority bootstrap-priority

Context config>service>vprn>pim>rp>bsr-candidate
cfg>service>vprn>pim>rp>ipv6>bsr-candidate

Description This command defines the priority used to become the rendezvous point (RP). The higher the priority value the more likely that this router becomes the RP. If there is a tie, the router with the highest IP address is elected.

Parameters bootstrap-priority — The priority to become the bootstrap router.

Values 0 — 255

Default 0 (the router is not eligible to be the bootstrap router)

ipv6

Syntax ipv6

Context config>service>vprn>pim>rp

Description This command enables access to the context to configure the rendezvous point (RP) of a PIM IPv6 protocol instance.

An Alcatel-Lucent IPv6 PIM router acting as an RP must respond to an IPv6 PIM register message specifying an SSM multicast group address by sending to the first hop router stop register message(s). It does not build an (S, G) shortest path tree toward the first hop router. An SSM multicast group address can be either from the SSM default range or from a multicast group address range that was explicitly configured for SSM.

Default ipv6 RP enabled when IPv6 PIM is enabled.

anycast
**Syntax**

`anycast ipv6-address`

`no anycast ipv6-address`

**Context**

`config>service>vprn>pim>rp>ipv6`

**Description**

This command configures an IPv6 PIM anycast protocol instance for the RP being configured. Anycast enables fast convergence when a PIM RP router fails by allowing receivers and sources to rendezvous at the closest RP.

The `no` form of the command removes the anycast instance from the configuration.

**Default**

None

**Parameters**

`ipv6-address` — Configures the loopback IP address shared by all routes that form the RP set for this anycast instance. Only a single address can be configured. If another anycast command is entered with an address then the old address will be replaced with the new address. If no address is entered then the command is simply used to enter the anycast CLI level. --the highlighted text is invalid, don’t add here and please remove from IPv4 command

**Values**

`ipv6-address`: x:x:x:x:x:x:x:x (eight 16-bit pieces)

<table>
<thead>
<tr>
<th>x:x:x:x:x:d.d.d</th>
</tr>
</thead>
<tbody>
<tr>
<td>x [0..FFFF]H</td>
</tr>
<tr>
<td>d [0..255]D</td>
</tr>
</tbody>
</table>

**rp-set-peer**

**Syntax**

`[no] rp-set-peer ipv6-address`

**Context**

`config>service>vprn>pim>rp>ipv6>anycast`

**Description**

This command configures an IPv6 peer in the anycast rp-set. The address identifies the address used by the other node as the RP candidacy address for the same multicast group address range as configured on this node.

This is a manual procedure. Caution should be taken to produce a consistent configuration of an RP-set for a given multicast group address range. The priority should be identical on each node and be a higher value than any other configured RP candidate that is not a member of this rp-set.

Although there is no set maximum of addresses that can be configured in an rp-set, up to 15 multicast addresses is recommended.

The `no` form of the command removes an entry from the list.

**Default**

None

**Parameters**

`ipv6-address` — Specifies the address used by the other node as the RP candidacy address for the same multicast group address range as configured on this node.

**Values**

`ipv6-address`: x:x:x:x:x:x:x:x (eight 16-bit pieces)

<table>
<thead>
<tr>
<th>x:x:x:x:x:d.d.d</th>
</tr>
</thead>
<tbody>
<tr>
<td>x [0..FFFF]H</td>
</tr>
<tr>
<td>d [0..255]D</td>
</tr>
</tbody>
</table>
PIM Commands

**embedded-rp**

Syntax: `embedded-rp`

Context: `config>service>vprn>pim>rp>ipv6`

Description: This command enables context to configure IPv6 embedded RP parameters.

**group-range**

Syntax: `[no] group-range {ipv6-address/prefix-length}

Context: `config>service>vprn>pim>rp>ipv6>embedded-rp`

Description: This command configures the group address or range of group addresses for which this router can be the rendezvous point (RP).

Use the no form of this command to remove the group address or range of group addresses for which this router can be the RP from the configuration.

Default: none

Parameters:
- `ipv6-address` — Specify the addresses or address ranges that this router can be an RP.
- `prefix-length` — Specify the address prefix length.

Values:
- `ipv6-address`: `x:x:x:x:x:x:x:x (eight 16-bit pieces)`
- `x`: `[0..FFFF] H`
- `d`: `[0..255] D`

- `prefix-length`: `[8..128] // for embedded-rp`
- `prefix-length`: `[16..128] // for rp-candidate`

**group-prefix**

Syntax: `[no] group-prefix grp-ipv6-address/prefix-length`

Context: `config>service>vprn>pim>rp>ipv6>static`

Description: The group-prefix for a static-rp defines a range of multicast-ip-addresses for which this static RP is applicable.

The no form of the command removes the criterion.

Default: none

Parameters:
- `grp-ipv6-address` — Specifies the multicast IPv6 address.
- `prefix-length` — Specifies the address prefix length.
Values
group-ipv6-address x:x:x:x:x:x:x (eight 16-bit pieces)

\[x:x:x:x:x:d.d.d\]
x \([0..FFFF] \) H
\[d \([0..255] \) D\]

prefix-length \([8..128] \)

rp-candidate

Syntax \rp-candidate

Context config>service>vprn>pim>rp
config>service>vprn>pim>rp>ipv6

Description This command enables the context to configure the candidate rendezvous point (RP) parameters.

Default Enabled when PIM is enabled.

group-range

Syntax \[no\] group-range \{ip-prefix/mask \| ip-prefix netmask\}

Context config>service>vprn>pim>rp>rp-candidate
config>service>vprn>pim>ssm

Description This command configures the group address or range of group addresses for which this router can be the rendezvous point (RP).

Use the no form of this command to remove the group address or range of group addresses for which this router can be the RP from the configuration.

Default none

Parameters \ip-prefix — Specify the addresses or address ranges that this router can be an RP.

Values
ipv4-prefix - a.b.c.d
ipv4-prefix-le - [0..32]
ipv6-prefix - x:x:x:x:x:x (eight 16-bit pieces)
\[x:x:x:x:d.d.d\]
x \([0..FFFF] \) H
\[d \([0..255] \) D\]

ipv6-prefix-le - [0..128]

mask — Specify the address mask with the address to define a range of addresses.

netmask — Specify the subnet mask in dotted decimal notation.

Values :a.b.c.d (network bits all 1 and host bits all 0)
PIM Commands

holdtime

Syntax

```
holdtime holdtime
no holdtime holdtime
```

Context

```
config>service>vprn>pim>rp rp-candidate
config>service>vprn>pim>rp ipv6>rp-candidate
```

Description

Use this command to define the length of time neighboring router consider this router to be up.

Use the `no` form of this command to revert to the default value.

Default

150

Parameters

```
holdtime — Specify the length of time, in seconds, that neighbor should consider the sending router to be operational.
```

```
Values  0 — 255
```

priority

Syntax

```
priority priority
no priority priority
```

Context

```
config>router>pim>rp local
config>service>vprn>pim>rp rp-candidate
```

Description

This command defines the priority used to become the rendezvous point (RP). The higher the priority value, the more likely that this router will become the RP.

Use the `no` form of this command to revert to the default value.

Default

1

Parameters

```
priority — Specify the priority to become the designated router. The higher the value the more likely the router will become the RP.
```

```
Values  0 — 255
```

static

Syntax

```
static
```

Context

```
config>service>vprn>pim>rp
```

Description

This command enables access to the context to configure a static rendezvous point (RP) of a PIM-SM protocol instance.

Default

none

address
Syntax \[ no \] address ip-address

Context config>service>vprn>pim>rp>static

Description This command configures the static rendezvous point (RP) address. The \textit{no} form of this command removes the static RP entry from the configuration.

Default none

---

**group-prefix**

Syntax \[ no \] group-prefix \{ grp-ip-address/mask | grp-ip-address netmask \}

Context config>service>vprn>pim>rp>static

Description The \textit{group-prefix} for a static-rp defines a range of multicast-ip-addresses for which a certain RP is applicable. The \textit{no} form of the command removes the criterion.

Default none

Parameters
- **grp-ip-address** — Specify the multicast IP address.
- **mask** — Defines the mask of the multicast-ip-address.
  
  \textbf{Values} \hspace{1cm} 4 — 32

- **netmask** — Enter the subnet mask in dotted decimal notation.
  
  \textbf{Values} \hspace{1cm} 0.0.0.0 — 255.255.255.255 (network bits all 1 and host bits all 0)

---

**override**

Syntax \[ no \] override

Context config>service>vprn>pim>rp>static

Description This command changes the precedence of static RP over dynamically learned Rendezvous Point (RP).

When enabled, the static group-to-RP mappings take precedence over the dynamically learned mappings.

Default no override

---

**rpf-table**

Syntax \[ no \] rpf-table \{ rtable-m | rtable-u | both \}

Context config>service>vprn>pim
PIM Commands

**Description**  This command configures the sequence of route tables used to find a Reverse Path Forwarding (RPF) interface for a particular multicast route.

By default, only the unicast route table is looked up to calculate RPF interface towards the source/rendezvous point. However, the operator can specify the following:

a) Use unicast route table only
b) Use multicast route table only or
c) Use both the route tables.

**Default**  rpf-table rtable-u

**Parameters**

rtable-m — Specified that only the multicast route table is to be used by the multicast protocol (PIM) for IPv4 RPF checks. This route table contains routes submitted by static routes and OSPF.

rtable-u — Specifies that only the unicast route table is to be used by the multicast protocol (PIM) for IPv4 RPF checks. This route table contains routes submitted by all the unicast routing protocols.

both — Specifies that PIM always lookup first in the multicast route table, and if there is a route, PIM use it. If PIM does not find a route in the first lookup, it will try to find it in the unicast route table. rtable-m is checked before rtable-u.

**spt-switchover-threshold**

**Syntax**  spt-switchover-threshold {grp-ip-address/mask | grp-ip-address netmask} spt-threshold

**Context**  config>service>vprn>pim

**Description**  This command configures a shortest path tree (SPT tree) switchover threshold for a group prefix.

**Parameters**

grp-ip-address — Specify the multicast group address.

mask — Defines the mask of the multicast-ip-address.

Values  4 — 32

netmask — Enter the subnet mask in dotted decimal notation.

Values  0.0.0.0 — 255.255.255.255 (network bits all 1 and host bits all 0)

spt-threshold — Specifies the configured threshold in kilo-bits per second(kbps) for the group to which this (S,G) belongs. For a group G configured with a threshold, switchover to SPT for an (S,G) is attempted only if the (S,G)'s rate exceeds this configured threshold.

**ssm-assert-compatible-mode**

**Syntax**  ssm-assert-compatible-mode [enable|disable]

**Context**  config>service>vprn>pim
**Virtual Private Routed Network Services**

**Description**
This command specifies whether SSM assert is enabled in compatibility mode for this PIM protocol instance. When enabled, for SSM groups, PIM will consider the SPT bit to be implicitly set to compute the value of CouldAssert (S,G,I) as defined in RFC 4601, *Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)*. When disabled, for SSM groups, PIM will not assume the SPT bit to be set. The SPT bit will be set by Update_SPTbit(S,G,iif) macro defined in RFC 4601.

**Default**
disable

**Parameters**
- **enable** — Enables SSM assert in compatibility mode for this PIM protocol instance.
- **disable** — Disabled SSM assert in compatibility mode for this PIM protocol instance.

**ssm-default-range-disable**

**Syntax**
```
ssm-default-range-disable ipv4
```

**Context**
```
config>service>vprn>pim
```

**Description**
This command specifies whether to disable the use of default range (232/8) for SSM so that it can be used by ASM to process (*,G). When enabled, the use of default range is disabled for SSM and it can be used by ASM. When disabled, the SSM default range is enabled.

**Default**
disable

**ssm-groups**

**Syntax**
```
[no] ssm-groups
```

**Context**
```
config>service>vprn
```

**Description**
This command enables access to the context to enable a source-specific multicast (SSM) configuration instance.

**Default**
none
C-MLDP Commands

mld

Syntax  
[no] mld

Context  
config>service>vprn

Description  
This command enables the context to configure Multicast Listener Discovery (MLD) parameters. The no form of the command disables MLD.

Default  
no mld

interface

Syntax  
[no] interface ip-int-name

Context  
config>service>vprn>mld

Description  
This command enables the context to configure an Multicast Listener Discovery (MLD) interface. The interface is a local identifier of the network interface on which reception of the specified multicast address is to be enabled or disabled. The no form of the command deletes the MLD interface. The shutdown command in the config>router>mld>interface context can be used to disable an interface without removing the configuration for the interface.

Default  
no interface — No interfaces are defined.

Parameters  
Ip-int-name — The IP interface name. Interface names must be unique within the group of defined IP interfaces for config router interface and config service ies interface commands. An interface name cannot be in the form of an IP address. Interface names can be any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

If the IP interface name does not exist or does not have an IP address configured an error message will be returned.

If the IP interface exists in a different area it will be moved to this area.

disable-router-alert-check

Syntax  
[no] disable-router-alert-check

Context  
config>service>vprn>mld>interface

Description  
This command enables router alert checking for MLD messages received on this interface.
The no form of the command disables the router alert checking.

Default none

import

Syntax import policy-name
no import

Context config>service>vprn>mld>interface

Description This command specifies the import route policy to be used for determining which membership reports are accepted by the router. Route policies are configured in the config>router>policy-options context.

When an import policy is not specified, all the MLD reports are accepted. The no form of the command removes the policy association from the MLD instance.

Default no import — No import policy specified.

Parameters policy-name — The route policy name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes. Route policies are configured in the config>router>policy-options context.

max-groups

Syntax max-groups value
no max-groups

Context config>service>vprn>mld>interface

Description This command specifies the maximum number of groups for which MLD can have local receiver information based on received MLD reports on this interface. When this configuration is changed dynamically to a value lower than the currently accepted number of groups, the groups that are already accepted are not deleted. Only new groups will not be allowed.

Default 0, no limit to the number of groups.

Parameters value — Specifies the maximum number of groups for this interface.

Values 1 — 16000
query-interval

Syntax  
query-interval seconds
no query-interval

Context  
config>service>vprn>mld>interface

Description  
This command specifies the frequency that the querier router transmits general host-query messages. The host-query messages solicit group membership information and are sent to the all-systems multicast group address, 224.0.0.1.

Default  
125

Parameters  
seconds — The time frequency, in seconds, that the router transmits general host-query messages.

Values  
2 — 1024

query-last-member-interval

Syntax  
query-last-member-interval seconds

Context  
config>service>vprn>mld>interface

Description  
This command configures the frequency at which the querier sends group-specific query messages including messages sent in response to leave-group messages. The lower the interval, the faster the detection of the loss of the last member of a group.

Default  
1

Parameters  
seconds — Specifies the frequency, in seconds, at which query messages are sent.

Values  
1 — 1024

query-response-interval

Syntax  
query-response-interval seconds

Context  
config>service>vprn>mld>interface

Description  
This command specifies how long the querier router waits to receive a response to a host-query message from a host.

Default  
10

Parameters  
seconds — Specifies the length of time to wait to receive a response to the host-query message from the host.

Values  
1 — 1023
### static

**Syntax**
```
static
```

**Context**
```
config>service>vprn>mld>interface
```

**Description**
This command tests multicast forwarding on an interface without a receiver host. When enabled, data is forwarded to an interface without receiving membership reports from host members.

**Default**
none

### group

**Syntax**
```
[no] group ipv6-address
```

**Context**
```
config>service>vprn>mld>interface>static
```

**Description**
This command enables the context to add a static multicast group either as a (*,G) or one or more (S,G) records. Use MLD static group memberships to test multicast forwarding without a receiver host. When MLD static groups are enabled, data is forwarded to an interface without receiving membership reports from host members.

When static MLD group entries on point-to-point links that connect routers to a rendezvous point (RP) are configured, the static MLD group entries do not generate join messages toward the RP.

The **no** form of the command removes the IPv6 address from the configuration.

**Default**
none

**Parameters**
- `ipv6-address` — Specifies an MLD multicast group address that receives data on an interface. The IP address must be unique for each static group.

### source

**Syntax**
```
[no] source ipv6-address
```

**Context**
```
config>service>vprn>mld>interface>static>group
```

**Description**
This command specifies an IPv6 unicast address that sends data on an interface. This enables a multicast receiver host to signal a router the group to receive multicast traffic from, and from the source(s) that the traffic is expected.

The **source** command is mutually exclusive with the specification of individual sources for the same group.

The source command, in combination with the group, is used to create a specific (S,G) static group entry.

The **no** form of the command removes the source from the configuration.

**Default**
none

**Parameters**
- `ip-address` — Specifies the IPv6 unicast address.
C-MLDP Commands

starg

Syntax  [no] starg

Context  config>service>vprn>mld>interface>static>group

Description  This command adds a static (*,G) entry. This command can only be enabled if no existing source addresses for this group are specified.

Use the no form of the command to remove the starg entry from the configuration.

Default  none

version

Syntax  version version

no version

Context  config>service>vprn>mld>interface

Description  This command specifies the MLD version. If routers run different versions, they will negotiate the lowest common version of MLD that is supported by hosts on their subnet and operate in that version. For MLD to function correctly, all routers on a LAN should be configured to run the same version of MLD on that LAN.

Default  1

Parameters  version — Specifies the MLD version number.

Values  1, 2

robust-count

Syntax  robust-count robust-count

no robust-count

Context  config>service>vprn>mld

Description  This command configures the robust count. The robust-count variable allows tuning for the expected packet loss on a subnet. If a subnet anticipates losses, the robust-count variable can be increased.

Default  2

Parameters  robust-count — Specify the robust count value.

Values  2 — 10
ssm-translate

Syntax  ssm-translate
Context  config>service>vprn>mld
Description  This command enables the context to configure group ranges which are translated to SSM (S,G) entries. If the static entry needs to be created, it has to be translated from a IGMPv1 IGMPv2 request to a Source Specific Multicast (SSM) join. An SSM translate source can only be added if the starg command is not enabled. An error message is generated if you try to configure the source command with starg command enabled.

grp-range

Syntax  [no] grp-range start end
Context  config>service>vprn>mld>ssm-translate
Description  This command is used to configure group ranges which are translated to SSM (S,G) entries.
Parameters  start — An IP address that specifies the start of the group range.
end — An IP address that specifies the end of the group range. This value should always be greater than or equal to the value of the start value.

source

Syntax  [no] source ip-address
Context  config>service>vprn>mld>ssm-translate>grp-range
Description  This command specifies the source IP address for the group range. Whenever a (*,G) report is received in the range specified by grp-range start and end parameters, it is translated to an (S,G) report with the value of this object as the source address.
Parameters  ip-address — Specifies the IP address that will be sending data.
network-interface

**Syntax**

```
network-interface interface-name [create]
no network-interface interface-name
```

**Context**

```
config>service>vprn
```

**Description**

This command configures a network interface in a VPRN that acts as a CSC interface to a CSC-CE in a Carrier Supporting Carrier IP VPN deployment model.
BGP Commands

bgp

Syntax  [no] bgp
Context  service>vprn
Description  This command enables the BGP protocol with the VPRN service.
The no form of the command disables the BGP protocol from the given VPRN service.
Default  no bgp

bgp-shared-queue

Syntax  bgp-shared-queue [cir rate] [pir rate]
no bgp-shared-queue
Context  config>service>vprn
Description  This command enables all BGP peers within a VPRN instance to share a single CPM queue. This command takes affect on new BGP connections established; already established BGP peers continue to use their own CPM queue. Any changes to PIR/CIR of the shared queue takes effect only after BGP connections are re-established.
Parameters  cir rate — Specifies the CIR rate for the shared queue.
pir rate — Specifies the PIR rate for the shared queue.

advertise-inactive

Syntax  [no] advertise-inactive
Context  config>service>vprn>bgp
           config>service>vprn>bgp>group
           config>service>vprn>bgp>group>neighbor
Description  This command enables or disables the advertising of inactive BGP routers to other BGP peers.
By default, BGP only advertises BGP routes to other BGP peers if a given BGP route is chosen by the route table manager as the most preferred route within the system and is active in the forwarding plane. This command allows system administrators to advertise a BGP route even though it is not the most preferred route within the system for a given destination.
Default  no advertise-inactive
aggregator-id-zero

**Syntax**  
[no] aggregator-id-zero

**Context**  
config>service>vprn:bgp  
config>service>vprn:bgp>group  
config>service>vprn:bgp>group>neighbor

**Description**  
This command is used to set the router ID in the BGP aggregator path attribute to zero when BGP aggregates routes. This prevents different routers within an AS from creating aggregate routes that contain different AS paths.

When BGP is aggregating routes, it adds the aggregator path attribute to the BGP update messages. By default, BGP adds the AS number and router ID to the aggregator path attribute.

When this command is enabled, BGP adds the router ID to the aggregator path attribute. This command is used at the group level to revert to the value defined under the global level, while this command is used at the neighbor level to revert to the value defined under the group level.

The **no** form of the command used at the global level reverts to default where BGP adds the AS number and router ID to the aggregator path attribute.

The **no** form of the command used at the group level reverts to the value defined at the group level.

The **no** form of the command used at the neighbor level reverts to the value defined at the group level.

**Default**  
no aggregator-id-zero — BGP adds the AS number and router ID to the aggregator path attribute.

always-compare-med

**Syntax**  
always-compare-med {zero | infinity}  
no always-compare-med strict-as {zero | infinity}  
no always-compare-med

**Context**  
config>router:bgp>best-path-selection

**Description**  
This command configures the comparison of BGP routes based on the MED attribute. The default behavior of SR-OS (equivalent to the **no** form of the command) is to only compare two routes on the basis of MED if they have the same neighbor AS (the first non-confed AS in the received AS_PATH attribute). Also by default, a route without a MED attribute is handled the same as though it had a MED attribute with the value 0. The **always-compare-med** command without the **strict-as** keyword allows MED to be compared even if the paths have a different neighbor AS; in this case, if neither **zero** or **infinity** is specified, the **zero** option is inferred, meaning a route without a MED is handled the same as though it had a MED attribute with the value 0. When the **strict-as** keyword is present, MED is only compared between paths from the same neighbor AS, and in this case, **zero** or **infinity** is mandatory and tells BGP how to interpret paths without a MED attribute.

**Default**  
no always-compare-med

**Parameters**  
**zero** — Specifies that for routes learned without a MED attribute that a zero (0) value is used in the MED comparison. The routes with the lowest metric are the most preferred.

**infinity** — Specifies for routes learned without a MED attribute that a value of infinity (2^32-1) is used in the MED comparison. This in effect makes these routes the least desirable.
strike-as — Specifies BGP paths to be compared even with different neighbor AS.

as-path-ignore

Syntax [no] as-path-ignore
Context config>service>vprn>bgp
Description This command determines whether the AS path is used to determine the best BGP route. If this option is present, the AS paths of incoming routes are not used in the route selection process. The no form of the command removes the parameter from the configuration.
Default no as-path-ignore

deterministic-med

Syntax [no] deterministic-med
Context config>service>vprn>bgp>best-path-selection
Description This command controls how the BGP decision process compares routes on the basis of MED. When deterministic-med is configured, BGP groups paths that are equal up to the MED comparison step based on neighbor AS, and then compares the best path from each group to arrive at the overall best path. This change to the BGP decision process makes best path selection completely deterministic in all cases. Without deterministic-med, the overall best path selection is sometimes dependent on the order of the route arrival because of the rule that MED cannot be compared in routes from different neighbor AS.
Default no deterministic-med

as-override

Syntax [no] as-override
Context config>service>vprn>bgp>group
config>service>vprn>bgp>group>neighbor
Description This command replaces all instances of the peer's AS number with the local AS number in a BGP route's AS_PATH. This command breaks BGP's loop detection mechanism. It should be used carefully.
Default as-override is not enabled by default.

authentication-key
Syntax  
*authentication-key [authentication-key | hash-key] [hash | hash2]*

no authentication-key

Context  
config>service>vprn:bgp
config>service>vprn:bgp>group
config>service>vprn:bgp>group>neighbor

Description  
This command configures the BGP authentication key.

Authentication is performed between neighboring routers before setting up the BGP session by verifying the password. Authentication is performed using the MD-5 message-based digest. The authentication key can be any combination of letters or numbers from 1 to 16.

The no form of the command removes the authentication password from the configuration and effectively disables authentication.

Default  
Authentication is disabled and the authentication password is empty.

Parameters  
*authentication-key* — The authentication key. The key can be any combination of ASCII characters up to 255 characters in length (unencrypted). If spaces are used in the string, enclose the entire string in quotation marks (" ").

*hash-key* — The hash key. The key can be any combination of ASCII characters up to 342 characters in length (encrypted). If spaces are used in the string, enclose the entire string in quotation marks (" ").

This is useful when a user must configure the parameter, but, for security purposes, the actual unencrypted key value is not provided.

*hash* — Specifies the key is entered in an encrypted form. If the *hash* parameter is not used, the key is assumed to be in a non-encrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the *hash* parameter specified.

*hash2* — Specifies the key is entered in a more complex encrypted form. If the *hash2* parameter is not used, the less encrypted *hash* form is assumed.

auth-keychain

Syntax  
*auth-keychain name*

Context  
config>service>vprn:bgp
config>service>vprn:bgp>group
config>service>vprn:bgp>group>neighbor

Description  
This command configures the BGP authentication key for all peers.

The keychain allows the rollover of authentication keys during the lifetime of a session.

Default  
no auth-keychain

Parameters  
*name* — Specifies the name of an existing keychain, up to 32 characters, to use for the specified TCP session or sessions.
backup-path

Syntax  [no] backup-path [ipv4] [ipv6]
Context  config>router
         config>router:bgp
         config>service>vprn:bgp

Description  This command enables the computation and use of a backup path for IPv4 and/or IPv6 BGP-learned prefixes belonging to the base router or a particular VPRN. Multiple paths must be received for a prefix in order to take advantage of this feature. When a prefix has a backup path and its primary path(s) fail the affected traffic is rapidly diverted to the backup path without waiting for control plane re-convergence to occur. When many prefixes share the same primary path(s), and in some cases also the same backup path, the time to failover traffic to the backup path is independent of the number of prefixes. In some cases prefix independent convergence may require use of FP2 or later IOMs/IMMs/XMAs.

By default, IPv4 and IPv6 prefixes do not have a backup path installed in the IOM.

Default  no backup-path

Parameters  ipv4 — enable the use of a backup path for BGP-learned IPv4 prefixes.
            ipv6 — enable the use of a backup path for BGP-learned IPv6 prefixes.

best-path-selection

Syntax  best-path-selection
Context  config>service>vprn:bgp

Description  This command enables path selection configuration.

bfd-enable

Syntax  [no] bfd-enable
Context  config>router:bgp
         config>router:bgp>group
         config>router:bgp>group>neighbor

Description  This command enables the use of bi-directional forwarding (BFD) to control the state of the associated protocol interface. By enabling BFD on a given protocol interface, the state of the protocol interface is tied to the state of the BFD session between the local node and the remote node. The parameters used for the BFD are set via the BFD command under the IP interface.

The no form of this command removes BFD from the associated BGP protocol peering.

Default  no bfd-enable
cluster

Syntax  

cluster  

Syntax  cluster  

command  

cluster-id  

no  

cluster  

no  

cluster  

Context  

config>service>vprn:bgp  

config>service>vprn:bgp>group  

config>service>vprn:bgp>group>neighbor  

Description  

This command configures the cluster ID for a route reflector server.  

Route reflectors are used to reduce the number of IBGP sessions required within an AS. Normally, all  

BGP speakers within an AS must have a BGP peering with every other BGP speaker in an AS. A  

route reflector and its clients form a cluster. Peers that are not part of the cluster are considered to be  

non-clients.  

When a route reflector receives a route, first it must select the best path from all the paths received. If  

the route was received from a non-client peer, then the route reflector sends the route to all clients in  

the cluster. If the route came from a client peer, the route reflector sends the route to all non-client  

peers and to all client peers except the originator.  

For redundancy, a cluster can have multiple route reflectors.  

Confederations can also be used to remove the full IBGP mesh requirement within an AS.  

The  

no  

form of the command deletes the cluster ID and effectively disables the Route Reflection for  

the given group.  

Default  

no  

cluster — No cluster ID is defined.  

Parameters  

cluster-id — The route reflector cluster ID is expressed in dot decimal notation.  

Values  

Any 32 bit number in dot decimal notation. (0.0.0.1 — 255.255.255.255)  

connect-retry  

Syntax  

connect-retry  

seconds  

no  

connect-retry  

Syntax  

connect-retry  seconds  

Context  

config>service>vprn:bgp  

config>service>vprn:bgp>group  

config>service>vprn:bgp>group>neighbor  

Description  

This command configures the BGP connect retry timer value in seconds.  

When this timer expires, BGP tries to reconnect to the configured peer. This configuration parameter  

can be set at three levels: global level (applies to all peers), peer-group level (applies to all peers in  
group) or neighbor level (only applies to specified peer). The most specific value is used.  

The  

no  

form of the command used at the global level reverts to the default value.  

The  

no  

form of the command used at the group level reverts to the value defined at the global level.  

The  

no  

form of the command used at the neighbor level reverts to the value defined at the group level.  

Default  

120 seconds  

Parameters  

seconds — The BGP Connect Retry timer value in seconds, expressed as a decimal integer.
damp-peer-oscillations

Syntax  
\texttt{damp-peer-oscillations [idle-hold-time initial-wait second-wait max-wait] [error-interval minutes]}

Context  
\texttt{config>service>vprn>bgp}
\texttt{config>service>vprn>bgp>group}
\texttt{config>service>vprn>bgp>group>neighbor}

Description  
This command controls how long a BGP peer session remains in the idle-state after some type of error causes the session to reset. In the idle state, BGP does not initiate or respond to attempts to establish a new session. Repeated errors that occur a short while after each session reset cause longer and longer hold times in the idle state. This command supports the DampPeerOscillations FSM behavior described in section 8.1 of RFC 4271, A Border Gateway Protocol 4 (BGP-4).

The default behavior, which applies when no damp-peer-oscillations is configured, is to immediately transition out of the idle-state after every reset.

Default  
\texttt{no damp-peer-oscillations}

Parameters  
\texttt{initial-wait} — The amount of time, in minutes, that a session remains in the idle-state after it has been stable for a while.

Values  
0 — 2048

Default  
0

\texttt{second-wait} — A period of time, in minutes, that is doubled after each repeated session failure that occurs within a relatively short span of time.

Values  
0 — 2048

Default  
5

\texttt{max-wait} — The maximum amount of time, in minutes, that a session remains in the idle-state after it has experienced repeated instability.

Values  
0 — 2048

Default  
60

\texttt{minutes} — The interval of time, in minutes after a session reset, during which the session must be error-free in order to reset the penalty counter and return to idle-hold-time to initial-wait.

Values  
0 — 2048

Default  
30

damping

Syntax  
\texttt{[no] damping}

Context  
\texttt{config>service>vprn>bgp}
BGP Commands

config>service>vprn>bgp>group
config>service>vprn>bgp>group>neighbor

Description
This command enables BGP route damping for learned routes which are defined within the route policy. Use damping to reduce the number of update messages sent between BGP peers and reduce the load on peers without affecting the route convergence time for stable routes. Damping parameters are set via route policy definition.

The no form of the command used at the global level disables route damping. The no form of the command used at the group level reverts to the value defined at the global level.

When damping is enabled and the route policy does not specify a damping profile, the default damping profile is used. This profile is always present and consists of the following parameters:

- Half-life: 15 minutes
- Max-suppress: 60 minutes
- Suppress-threshold: 3000
- Reuse-threshold: 750

Default
no damping — Learned route damping is disabled.

disable-4byte-asn

Syntax
[no] disable-4byte-asn

Context
config>service>vprn>bgp
config>service>vprn>bgp>group
config>service>vprn>bgp>group>neighbor

Description
This command disables the use of 4-byte ASNs. It can be configured at all 3 level of the hierarchy so it can be specified down to the per peer basis.

If this command is enabled 4-byte ASN support should not be negotiated with the associated remote peer(s).

The no form of the command resets the behavior to the default which is to enable the use of 4-byte ASN.

disable-capability-negotiation

Syntax
[no] disable-capability-negotiation

Context
config>service>vprn>bgp>group
config>service>vprn>bgp>group>neighbor

Description
This command disables the exchange of capabilities. When command is enabled and after the peering is flapped, any new capabilities are not negotiated and will strictly support IPv4 routing exchanges with that peer.

The no form of the command removes this command from the configuration and restores the normal behavior.
disable-client-reflect

**Syntax**

[no] disable-client-reflect

**Context**

config>service>vprn>bgp
config>service>vprn>bgp>group
config>service>vprn>bgp>group>neighbor

**Description**

This command disables the reflection of routes by the route reflector to the group or neighbor. This only disables the reflection of routes from other client peers. Routes learned from non-client peers are still reflected to all clients.

The **no** form re-enables client reflection of routes.

**Default**

no disable-client-reflect — Client routes are reflected to all client peers.

disable-communities

**Syntax**

disable-communities [standard] [extended]

no disable-communities

**Context**

config>service>vprn>bgp
config>service>vprn>bgp>group
config>service>vprn>bgp>group>neighbor

**Description**

This command configures BGP to disable sending communities.

**Parameters**

- **standard** — Specifies standard communities that existed before VPRNs or 2547.
- **extended** — Specifies BGP communities used were expanded after the concept of 2547 was introduced, to include handling the VRF target.

disable-fast-external-failover

**Syntax**

[no] disable-fast-external-failover

**Context**

config>service>vprn>bgp
config>service>vprn>bgp>group
config>service>vprn>bgp>group>neighbor

**Description**

This command configures BGP fast external failover.

eibgp-loadbalance

**Syntax**

[no] eibgp-loadbalance
BGP Commands

**Context**
config>service>vprn>bgp

**Description**
This command enables eBGP load sharing so routes with both MP-BGP and IPv4 next-hops can be used simultaneously.

In order for this command to be effective, the **ecmp** and **multipath** commands for the associated VPRN instance must also be configured to allow for multiple routes to the same destination.

The **no** form of the command used at the global level reverts to default values.

**Default**
no eibgp-loadbalance — Multipath disabled.

**enable-bgp-vpn-backup**

**Syntax**
enable-bgp-vpn-backup [ipv4] [ipv6]
no enable-bgp-vpn-backup

**Context**
config>service>vprn

**Description**
This command enables BGP-VPN routes imported into the VPRN to have backup paths calculated for them (when they are the best path) and to be considered as backup path candidates (for other VPN-IP routes and VPRN BGP routes learned from CEs).

**Default**
no enable-bgp-vpn-backup

**enable-peer-tracking**

**Syntax**
[no] enable-peer-tracking

**Context**
config>service>vprn>bgp
config>service>vprn>bgp>group
config>service>vprn>bgp>group>neighbor

**Description**
This command enables BGP peer tracking.

**Default**
no enable-peer-tracking

**graceful-restart**

**Syntax**
[no] graceful-restart

**Context**
config>service>vprn>bgp
config>service>vprn>bgp>group
config>service>vprn>bgp>group>neighbor

**Description**
This command enables or disables graceful-restart for all VPRN BGP peers.
enable-notification

Syntax

enable-notification
no enable-notification

Context

config>service>vprn>bgp>graceful-restart
config>service>vprn>bgp>group>graceful-restart
config>service>vprn>bgp>group>neighbor>graceful-restart

Description

When this command is present, the graceful restart capability sent by this router indicates support for NOTIFICATION messages. If the peer also supports this capability then the session can be restarted gracefully (while preserving forwarding) if either peer needs to send a NOTIFICATION message due to some type of event or error.

Default

no enable-notification

restart-time

Syntax

restart-time seconds
no restart-time

Context

config>service>vprn>bgp>graceful-restart
config>service>vprn>bgp>group>graceful-restart
config>service>vprn>bgp>group>neighbor>graceful-restart

Description

This command sets the value of the restart-time that is advertised in the router’s graceful-restart capability. If this command is not configured, the default is 300.

Default

no restart time

Parameters

seconds — The restart-time that is advertised in the router’s graceful-restart capability.

Values

0 — 4095 seconds

Default

300

stale-routes-time

Syntax

[no] stale-routes-time time

Context

config>service>vprn>bgp>graceful-restart
config>service>vprn>bgp>group>graceful-restart
config>service>vprn>bgp>group>neighbor>graceful-restart

Description

This command configures the time period to keep stale routes before the END-OF-RIB message is received from the restarting router.

Parameters

time — [1..3600 seconds]

Default

360 seconds
error-handling

**Syntax**

```
error-handling
```

**Context**

```
config>service>vprn>bgp
config>service>vprn>bgp>group
config>service>vprn>bgp>group>neighbor
```

**Description**

This command specifies whether the error handling mechanism for optional transitive path attributes is enabled for this peer group.

update-fault-tolerance

**Syntax**

```
[no] update-fault-tolerance
```

**Context**

```
config>service>vprn>bgp>error-handling
config>service>vprn>bgp>group>error-handling
config>service>vprn>bgp>group>neighbor>error-handling
```

**Description**

This command enables `treat-as-withdraw` and other similarly non-disruptive approaches for handling a wide range of UPDATE message errors, as long as there are no length errors that prevent all of the NLRI fields from being correctly identified and parsed.

**Default**

`no fault-tolerance`

export

**Syntax**

```
export policy [policy...]
no export
```

**Context**

```
config>service>vprn>bgp
config>service>vprn>bgp>group
config>service>vprn>bgp>group>neighbor
```

**Description**

This command specifies the export policies to be used to control routes advertised to BGP neighbors. When multiple policy names are specified, the policies are evaluated in the order they are specified. A maximum of five (5) policy names can be configured. The first policy that matches is applied.

Note that if a non-existent route policy is applied to a VPRN instance, the CLI generates a warning message. This message is only generated at an interactive CLI session and the route policy association is made. No warning message is generated when a non-existent route policy is applied to a VPRN instance in a configuration file or when SNMP is used.

The `no` form of this command removes all route policy names from the export list.

**Default**

`no export` — BGP advertises routes from other BGP routes but does not advertise any routes from other protocols unless directed by an export policy.

**Parameters**

`policy` — A route policy statement name.
family

Syntax
family [ipv4][mcast-ipv4] [flow-ipv6] [flow-ipv4]
no family

Context
config>service>vprn:bgp
config>service>vprn:bgp>group
config>service>vprn:bgp>group>neighbor

Description
This command specifies the address families to be negotiated with one or more multi-protocol BGP peers of the VPRN.
The no form of the command removes the specified address family from the associated BGP sessions.

Default
ipv4

Parameters
ipv4 — Provisions IPv4 support.
mcast-ipv4 — Provisions Multicast IPv4 support.
[flow-ipv6] — Exchanges IPv4 flowspec routes belonging to AFI 2 and SAFI 133.
[flow-ipv4] — Specifies to use an address of variable size consisting of 1 or 2-byte NLRI(Network Layer Reachability Information) length followed by a variable length NLRI value.

flowspec-validate

Syntax
flowspec-validate
no flowspec-validate

Context
config>service>vprn:bgp
config>service>vprn:bgp>group
config>service>vprn:bgp>group>neighbor

Description
This command enables/disables validation of received flowspec routes. A flow route with a destination prefix subcomponent received from a particular peer is considered valid if and only if that peer also advertised the best unicast route to the destination prefix and any of its more-specific components. If validation is enabled and a flowspec route is not valid, it is not eligible for import into the RIB, it is not used for filtering, and it is not propagated to other flowspec peers.
The no form of the command disables the validation procedure.

Default
no flowspec-validate

group

Syntax
group name [dynamic-peer]
no group

Context
config>service>vprn:bgp

Description
This command creates a context to configure a BGP peer group.
BGP Commands

The **no** form of the command deletes the specified peer group and all configurations associated with the peer group. The group must be shutdown before it can be deleted.

**Default** None — No peer groups are defined.

**Parameters**
- **name** — The peer group name. Allowed values is a string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.
- **dynamic-peer** — This flag designates that the given BGP group will be used by BGP peers created dynamically based on subscriber-hosts pointing to corresponding BGP peering policy. There can be only one BGP group with this flag set in any given VPRN. No BGP neighbors can be manually configured in a BGP group with this flag set.

**Default** disabled

neighbor

**Syntax** [no] neighbor *ip-address*

**Context** config>service>vprn>bgp>group

**Description** This command creates a BGP peer/neighbor instance within the context of the BGP group. This command can be issued repeatedly to create multiple peers and their associated configuration. The **no** form of the command is used to remove the specified neighbor and the entire configuration associated with the neighbor. The neighbor must be administratively **shutdown** before attempting to delete it. If the neighbor is not shutdown, the command will not result in any action except a warning message on the console indicating that neighbor is still administratively up.

**Default** none — No neighbors are defined.

**Parameters**
- **ip-address** — The IP address of the BGP peer router in dotted decimal notation.

  **Values** ipv4-address : a.b.c.d

family

**Syntax** family [ipv4] [mcast-ipv4]

**no family**

**Context** config>service>vprn>bgp>group

**Description** This command specifies the address family or families to be supported over BGP peerings in the base router. This command is additive so issuing the **family** command adds the specified address family to the list.

The **no** form of the command removes the specified address family from the associated BGP peerings. If an address family is not specified, then reset the supported address family back to the default.
Default ipv4

Parameters

- **ipv4** — Provisions support for IPv4 routing information.
- **mcast-ipv4** — Provisions Multicast IPv4 support.

**hold-time**

**Syntax**

```
hold-time seconds [min seconds2]
no hold-time
```

**Context**

```
config>service>vprn:bgp
config>service>vprn:bgp>group
config>service>vprn:bgp>group>neighbor
```

**Description**

This command configures the BGP hold time, expressed in seconds.

The BGP hold time specifies the maximum time BGP waits between successive messages (either keepalive or update) from its peer, before closing the connection. This configuration parameter can be set at three levels: global level (applies to all peers), group level (applies to all peers in group) or neighbor level (only applies to specified peer). The most specific value is used.

Even though the router OS implementation allows setting the keepalive time separately, the configured keepalive timer is overridden by the hold-time value under the following circumstances:

1. If the specified hold-time is less than the configured keepalive time, then the operational keepalive time is set to a third of the hold-time; the configured keepalive time is not changed.
2. If the hold-time is set to zero, then the operational value of the keepalive time is set to zero; the configured keepalive time is not changed. This means that the connection with the peer is up permanently and no keepalive packets are sent to the peer.

The no form of the command used at the global level reverts to the default value.
The no form of the command used at the group level reverts to the value defined at the global level.
The no form of the command used at the neighbor level reverts to the value defined at the group level.

**Default**

90 seconds

**Parameters**

- **seconds** — The hold-time, in seconds, expressed as a decimal integer. A value of 0 indicates the connection to the peer is up permanently.
- **Values**
  - 0, 3 — 65535
- **seconds2** — The minimum hold-time that will be accepted for the session. If the peer proposes a hold-time lower than this value the session attempt will be rejected.

**ibgp-multipath**

**Syntax**

```
[no] ibgp-multipath
```

**Context**

```
config>service>vprn:bgp
```

**Description**

This command defines the type of IBGP multipath to use when adding BGP routes to the route table if the route resolving the BGP nexthop offers multiple nexthops.
BGP Commands

The **no** form of the command disables the IBGP multipath load balancing feature.

**Default**
none

**import**

**Syntax**
import policy [policy...]
no import

**Context**
config>service>vprn>bgp
config>service>vprn>bgp>group
config>service>vprn>bgp>group>neighbor

**Description**
This command specifies the import policies to be used to control routes advertised to BGP neighbors. Route policies are configured in the config>router>policy-options context. When multiple policy names are specified, the policies are evaluated in the order they are specified. A maximum of five (5) policy names can be specified. The first policy that matches is applied.

The **no** form of this command removes all route policy names from the import list.

**Default**
no import — BGP accepts all routes from configured BGP neighbors. Import policies can be used to limit or modify the routes accepted and their corresponding parameters and metrics.

**Parameters**
policy — A route policy statement name.

**keepalive**

**Syntax**
keepalive seconds
no keepalive

**Context**
config>service>vprn>bgp
config>service>vprn>bgp>group
config>service>vprn>bgp>group>neighbor

**Description**
This command configures the BGP keepalive timer. A keepalive message is sent every time this timer expires. The **seconds** parameter can be set at three levels: global level (applies to all peers), group level (applies to all peers in peer-group) or neighbor level (only applies to specified peer). The most specific value is used.

The **keepalive** value is generally one-third of the **hold-time** interval. Even though the OS implementation allows the **keepalive** value and the **hold-time** interval to be independently set, under the following circumstances, the configured **keepalive** value is overridden by the **hold-time** value:

If the specified **keepalive** value is greater than the configured **hold-time**, then the specified value is ignored, and the **keepalive** is set to one third of the current **hold-time** value.

If the specified **hold-time** interval is less than the configured **keepalive** value, then the **keepalive** value is reset to one third of the specified **hold-time** interval.

If the **hold-time** interval is set to zero, then the configured value of the **keepalive** value is ignored. This means that the connection with the peer is up permanently and no **keepalive** packets are sent to the peer.
The no form of the command used at the global level reverts to the default value.
The no form of the command used at the group level reverts to the value defined at the global level.
The no form of the command used at the neighbor level reverts to the value defined at the group level.

**Default**
30 seconds

**Parameters**
*seconds* — The keepalive timer in seconds, expressed as a decimal integer.

**Values**
0 — 21845

### local-address

**Syntax**
```bash
local-address ip-address
no local-address
```

**Context**
```
config>service>vprn>bgp>group
config>service>vprn>bgp>group>neighbor
```

**Description**
Configures the local IP address used by the group or neighbor when communicating with BGP peers.

Outgoing connections use the `local-address` as the source of the TCP connection when initiating connections with a peer.

When a local address is not specified, the system uses the system IP address when communicating with IBGP peers and uses the interface address for directly connected EBGP peers. This command is used at the neighbor level to revert to the value defined under the group level.

The no form of the command removes the configured local-address for BGP.
The no form of the command used at the group level reverts to the value defined at the global level.
The no form of the command used at the neighbor level reverts to the value defined at the group level.

**Default**
`no local-address` — The router ID is used when communicating with IBGP peers and the interface address is used for directly connected EBGP peers.

*ip-address* — The local address expressed in dotted decimal notation. Allowed values are a valid routable IP address on the router, either an interface or system IP address.

### local-as

**Syntax**
```bash
local-as as-number [private] [no-prepend-global-as]
no local-as
```

**Context**
```
config>service>vprn>bgp
config>service>vprn>bgp>group
config>service>vprn>bgp>group>neighbor
```

**Description**
This command configures a BGP virtual autonomous system (AS) number.

In addition to the global AS number configured for BGP in the config>router>autonomous-system context, a virtual (local) AS number can be configured to support various AS number migration scenarios. The local AS number is added to the beginning the as-path attribute ahead of the router’s AS number.
This configuration parameter can be set at three levels: global level (applies to all EBGP peers), group level (applies to all EBGP peers in peer-group) or neighbor level (only applies to EBGP specified peer). Thus, by specifying this at each neighbor level, it is possible to have a separate local-as per EBGP session. The local-as command is not supported for IBGP sessions. When the optional private keyword is specified in the command the local-as number is not added to inbound routes from the EBGP peer that has local-as in effect.

When a command is entered multiple times for the same AS, the last command entered is used in the configuration. The private attribute can be added or removed dynamically by reissuing the command.

Changing the local AS at the global level in an active BGP instance causes the BGP instance to restart with the new local AS number. Changing the local AS at the global level in an active BGP instance causes BGP to re-establish the peer relationships with all peers in the group with the new local AS number. Changing the local AS at the neighbor level in an active BGP instance causes BGP to re-establish the peer relationship with the new local AS number.

This is an optional command and can be used in the following circumstance:

Provider router P is moved from AS1 to AS2. The customer router that is connected to P, however, is configured to belong to AS1. To avoid reconfiguring the customer router, the local-as value on router P can be set to AS1. Thus, router P adds AS1 to the as-path message for routes it advertises to the customer router.

The no form of the command used at the global level will remove any virtual AS number configured. The no form of the command used at the group level reverts to the value defined at the global level. The no form of the command used at the neighbor level reverts to the value defined at the group level.

**Default**

no local-as

**Parameters**

as-number — The virtual autonomous system number, expressed as a decimal integer.

Value: 1 — 65535

private — Specifies the local-as is hidden in paths learned from the peering.

no-prepend-global-as — Specifies that the global-as is hidden in paths announced to the EBGP peer.

**local-preference**

**Syntax**

local-preference local-preference

no local-preference

**Context**

config>service>vprn>bgp
config>service>vprn>bgp>group
config>service>vprn>bgp>group>neighbor

**Description**

This command enables setting the BGP local-preference attribute in incoming routes if not specified and configures the default value for the attribute. This value is used if the BGP route arrives from a BGP peer without the local-preference integer set.

The specified value can be overridden by any value set via a route policy. This configuration parameter can be set at three levels: global level (applies to all peers), group level (applies to all peers in peer-group) or neighbor level (only applies to specified peer). The most specific value is used.
The **no** form of the command at the global level specifies that incoming routes with local-preference set are not overridden and routes arriving without local-preference set are interpreted as if the route had local-preference value of 100.

The **no** form of the command used at the group level reverts to the value defined at the global level. The **no** form of the command used at the neighbor level reverts to the value defined at the group level.

**Default**
- **no local-preference** — Does not override the local-preference value set in arriving routes and analyze routes without local preference with value of 100.

**Parameters**
- **local-preference** — The local preference value to be used as the override value, expressed as a decimal integer.
  - **Values**
    - 0 — 4294967295

**loop-detect**

**Syntax**
```
loop-detect {drop-peer | discard-route | ignore-loop| off}
```

**Context**
- config>service>vprn>bgp
- config>service>vprn>bgp>group
- config>service>vprn>bgp>group>neighbor

**Description**
This command configures how the BGP peer session handles loop detection in the AS path.

This configuration parameter can be set at three levels: global level (applies to all peers), group level (applies to all peers in peer-group) or neighbor level (only applies to specified peer). The most specific value is used.

Note that dynamic configuration changes of **loop-detect** are not recognized.

The **no** form of the command used at the global level reverts to default, which is **loop-detect ignore-loop**.

The **no** form of the command used at the group level reverts to the value defined at the global level.

The **no** form of the command used at the neighbor level reverts to the value defined at the group level.

**Default**
- loop-detect ignore-loop

**Parameters**
- **drop-peer** — Sends a notification to the remote peer and drops the session.
- **discard-route** — Discards routes received with loops in the AS path.
- **ignore-loop** — Ignores routes with loops in the AS path but maintains peering.
- **off** — Disables loop detection.

**med-out**

**Syntax**
```
med-out {number | igp-cost}
```

**Context**
- config>service>vprn>bgp
- config>service>vprn>bgp>group
- config>service>vprn>bgp>group>neighbor
**BGP Commands**

**Context**
config>service>vprn>bgp
config>service>vprn>bgp>group
config>service>vprn>bgp>group>neighbor

**Description**
This command enables advertising the Multi-Exit Discriminator (MED) and assigns the value used for the path attribute for the MED advertised to BGP peers if the MED is not already set.

The specified value can be overridden by any value set via a route policy.

This configuration parameter can be set at three levels: global level (applies to all peers), group level (applies to all peers in peer-group) or neighbor level (only applies to specified peer). The most specific value is used.

The `no` form of the command used at the global level reverts to default where the MED is not advertised.

The `no` form of the command used at the group level reverts to the value defined at the global level.

The `no` form of the command used at the neighbor level reverts to the value defined at the group level.

**Default**
no med-out

**Parameters**

*number* — The MED path attribute value, expressed as a decimal integer.

**Values**
0 — 4294967295

*igp-cost* — The MED is set to the IGP cost of the given IP prefix.

**min-route-advertisement**

**Syntax**

```
min-route-advertisement seconds
no min-route-advertisement
```

**Context**
config>service>vprn>bgp
config>service>vprn>bgp>group
config>service>vprn>bgp>group>neighbor

**Description**
This command configures the minimum interval, in seconds, at which a prefix can be advertised to a peer.

This configuration parameter can be set at three levels: global level (applies to all peers), group level (applies to all peers in peer-group) or neighbor level (only applies to specified peer). The most specific value is used.

The `no` form of the command reverts to default values.

**Default**
30 seconds

**Parameters**

*seconds* — The minimum route advertising interval, in seconds, expressed as a decimal integer.

**Values**
1—255

**multihop**

**Syntax**

```
multihop ttl-value
```
no multihop

Context

config>service>vprn>bgp
config>service>vprn>bgp>group
config>service>vprn>bgp>group>neighbor

Description

This command configures the time to live (TTL) value entered in the IP header of packets sent to an EBGP peer multiple hops away.

This parameter is meaningful only when configuring EBGP peers. It is ignored if set for an IBGP peer.

The **no** form of the command is used to convey to the BGP instance that the EBGP peers are directly connected.

The **no** form of the command reverts to default values.

Default

1 — EBGP peers are directly connected.

64 — IBGP

Parameters

*ttl-value* — The TTL value, expressed as a decimal integer.

Values

1 — 255

multipath

Syntax

`multipath max-paths [eibgp]`

`no multipath`

Context

config>service>vprn>bgp

Description

This command enables BGP multipath.

When multipath is enabled BGP load shares traffic across multiple links. Multipath can be configured to load share traffic across a maximum of 16 routes. If the equal cost routes available are more than the configured value, then routes with the lowest next-hop IP address value are chosen.

This configuration parameter can be set at three levels: global level (applies to all peers), group level (applies to all peers in group) or neighbor level (only applies to specified peer). The most specific value is used.

Multipath is effectively disabled if the value is set to one. When multipath is disabled, and multiple equal cost routes are available, the route with the lowest next-hop IP address will be used.

The **no** form of the command used at the global level reverts to default values.

Default

no multipath — Multipath disabled.

Parameters

*integer* — The number of equal cost routes to use for multipath routing. If more equal cost routes exist than the configured value, routes with the lowest next-hop value are chosen. Setting this value to 1 disables multipath.

Values

1 — 16

eibgp — Enables EIBGP load balancing so that routes with both MP-BGP and IPv4 next-hops can be used simultaneously. Enabling this option will disable the nexthop type (MP-BGP or IPv4 and also the next-hop metric comparison).
next-hop-resolution

**Syntax**

next-hop-resolution

**Context**

config>service>vprn:bgp

**Description**

This command enables the context to configure next-hop resolution parameters.

next-hop-self

**Syntax**

[no] next-hop-self

**Context**

config>service>vprn:bgp>group
config>service>vprn:bgp>group>neighbor

**Description**

This command configures the group or neighbor to always set the NEXTHOP path attribute to its own physical interface when advertising to a peer.

This is primarily used to avoid third-party route advertisements when connected to a multi-access network.

The **no** form of the command used at the group level allows third-party route advertisements in a multi-access network.

The **no** form of the command used at the neighbor level reverts to the value defined at the group level.

**Default**

no next-hop-self — Third-party route advertisements are allowed.

passive

**Syntax**

[no] passive

**Context**

config>service>vprn:bgp>group
config>service>vprn:bgp>group>neighbor

**Description**

This command enables passive mode for the BGP group or neighbor.

When in passive mode, BGP will not attempt to actively connect to the configured BGP peers but responds only when it receives a connect open request from the peer.

The **no** form of the command used at the group level disables passive mode where BGP actively attempts to connect to its peers.

The **no** form of the command used at the neighbor level reverts to the value defined at the group level.

**Default**

no passive — BGP will actively try to connect to all the configured peers.

peer-as

**Syntax**

peer-as as-number

**Context**

config>service>vprn:bgp>group
config>service>vprn>bgp>group>neighbor

**Description**
This command configures the autonomous system number for the remote peer. The peer AS number must be configured for each configured peer.

For EBGP peers, the peer AS number configured must be different from the autonomous system number configured for this router under the global level since the peer will be in a different autonomous system than this router.

For IBGP peers, the peer AS number must be the same as the autonomous system number of this router configured under the global level.

This is a required command for each configured peer. This may be configured under the group level for all neighbors in a particular group.

**Default**
No AS numbers are defined.

**Parameters**
*as-number* — The autonomous system number, expressed as a decimal integer.

**Values**
1 — 65535

---

**policy**

**Syntax**

```
policy policy-name
no policy
```

**Context**

`config>service>vprn>bgp>next-hop-res`

**Description**
This command specifies the name of a policy statement to use with the BGP next-hop resolution process. The policy controls which IP routes in RTM are eligible to resolve the BGP next-hop addresses of IPv4 and IPv6 routes. The policy has no effect on the resolution of BGP next-hops to MPLS tunnels. If a BGP next-hop of an IPv4 or IPv6 route R is resolved in RTM and the longest matching route for the next-hop address is an IP route N that is rejected by the policy then route R is unresolved; if the route N is accepted by the policy then it becomes the resolving route for R.

The default next-hop resolution policy (when the `no policy` command is configured) is to use the longest matching active route in RTM that is not a BGP route (unless `use-bgp-routes` is configured), an aggregate route or a subscriber management route.

**Default**
`no policy`

**Parameters**
*policy-name* — The route policy name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes. Route policies are configured in the `config>router>policy-options` context.
peer-tracking-policy

Syntax  peer-tracking-policy policy-name
        no peer-tracking-policy

Context  config>router:bgp
        config>service>vprn:bgp

Description  This command specifies the name of a policy statement to use with the BGP peer-tracking function on
the BGP sessions where this is enabled. The policy controls which IP routes in RTM are eligible to
indicate reachability of IPv4 and IPv6 BGP neighbor addresses. If the longest matching route in RTM
for a BGP neighbor address is an IP route that is rejected by the policy, or it is a BGP route accepted
by the policy, or if there is no matching route, the neighbor is considered unreachable and BGP tears
down the peering session and holds it in the idle state until a valid route is once again available and
accepted by the policy.

The default peer-tracking policy (when the no peer-tracking-policy command is configured) is to use
the longest matching active route in RTM that is not an LDP shortcut route or an aggregate route.

Default  no peer-tracking-policy

Parameters  policy-name — The route policy name. Allowed values are any string up to 32 characters long com-
posed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces,
etc.), the entire string must be enclosed within double quotes. Route policies are configured in
the config>router>policy-options context.

preference

Syntax  [no] preference preference

Context  config>service>vprn:bgp
        config>service>vprn:bgp>group

Description  This command configures the route preference for routes learned from the configured peer(s).

This configuration parameter can be set at three levels: global level (applies to all peers), group level
(applies to all peers in peer-group) or neighbor level (only applies to specified peer). The most
specific value is used.

The lower the preference the higher the chance of the route being the active route. The OS assigns
BGP routes highest default preference compared to routes that are direct, static or learned via MPLS
or OSPF.

The no form of the command used at the global level reverts to default value.

The no form of the command used at the group level reverts to the value defined at the global level.

The no form of the command used at the neighbor level reverts to the value defined at the group level.

Default  170

Parameters  preference — The route preference, expressed as a decimal integer.

Values  1 — 255
prefix-limit

**Syntax**

```
prefix-limit limit [log-only] [threshold percent] [idle-timeout {minutes | forever}]
no prefix-limit
```

**Context**

```
config>service>vprn:bgp>group
cfg service vprn bgp group neighbor
```

**Description**

This command configures the maximum number of routes BGP can learn from a peer. When the number of routes reaches a certain percentage (default is 90% of this limit), an SNMP trap is sent. When the limit is exceeded, the BGP peering is dropped and disabled.

The `no` form of the command removes the `prefix-limit`.

**Default**

```
forever
```

**Parameters**

- `log-only` — Enables the warning message to be sent at the specified threshold percentage, and also when the limit is exceeded. However, the BGP peering is not dropped.
- `threshold` — The threshold value (as a percentage) that triggers a warning message to be sent.
- `limit` — The number of routes that can be learned from a peer expressed as a decimal integer.

**Values**

- `threshold` Value: 1 — 4294967295
- `limit` Value: 1 — 4294967295
- `idle-timeout` Value: 1 — 1024
- `forever` — Specifies that the session is reestablished only after `clear router bgp` command is executed.

rapid-update

**Syntax**

```
rapid-update {{l2-vpn} [mvpn-ipv4]}
no rapid-update {{l2-vpn} [mvpn-ipv4]}
```

**Context**

```
config>service>vprn:bgp
```

**Description**

This command enables and disables BGP rapid update for specified address-families. When no parameter is given for the no rapid-update statement, rapid update is disabled for all address-families.

**Default**

```
no rapid-update
```

rapid-withdrawal

**Syntax**

```
[no] rapid-withdrawal
```

**Context**

```
config>service>vprn:bgp
```

**Description**

This command disables the delay (Minimum Route Advertisement) on sending BGP withdrawals. Normal route withdrawals may be delayed up to the minimum route advertisement to allow for efficient packing of BGP updates.
The **no** form of the command removes this command from the configuration and returns withdrawal processing to the normal behavior.

**Default**

no rapid-withdrawal

---

**remove-private**

**Syntax**

[no] remove-private

**Context**

config>service>vprn:bgp
config>service>vprn:bgp>group
config>service>vprn:bgp>group>neighbor

**Description**

This command allows private AS numbers to be removed from the AS path before advertising them to BGP peers.

When the **remove-private** parameter is set at the global level, it applies to all peers regardless of group or neighbor configuration. When the parameter is set at the group level, it applies to all peers in the group regardless of the neighbor configuration.

The OS software recognizes the set of AS numbers that are defined by IANA as private. These are AS numbers in the range 64512 through 65535, inclusive.

The **no** form of the command used at the global level reverts to default value. The **no** form of the command used at the group level reverts to the value defined at the global level. The **no** form of the command used at the neighbor level reverts to the value defined at the group level.

**Default**

no remove-private — Private AS numbers will be included in the AS path attribute.

---

**split-horizon**

**Syntax**

split-horizon

no split-horizon

**Context**

config>service>vprn:bgp
config>service>vprn:bgp>group
config>service>vprn:bgp>group>neighbor

**Description**

This command enables the use of split-horizon. When applied globally, to a group, or a specific peer, split-horizon prevents routes from being reflected back to a peer that sends the best route. It applies to routes of all address families and to any type of sending peer; confed-EBGP, EBGP and IBGP.

The configuration default is **no split-horizon**, meaning that no effort is taken to prevent a best route from being reflected back to the sending peer.

**NOTE:** Use of the **split-horizon** command may have a detrimental impact on peer and route scaling and therefore operators are encouraged to use it only when absolutely needed.

The **no** form of the command disables split horizon command which allows the lower level to inherit the setting from an upper level.

**Default**

no split-horizon
type

Syntax  
[no] type {internal | external}

Context  
config>service>vprn:bgp>group
config>service>vprn:bgp>group>neighbor

Description  
This command designates the BGP peer as type internal or external.

The type of internal indicates the peer is an IBGP peer while the type of external indicates that the peer is an EBGP peer.

By default, the OS derives the type of neighbor based on the local AS specified. If the local AS specified is the same as the AS of the router, the peer is considered internal. If the local AS is different, then the peer is considered external.

The no form of the command used at the group level reverts to the default value.
The no form of the command used at the neighbor level reverts to the value defined at the group level.

Default  
no type — Type of neighbor is derived on the local AS specified.

Parameters  
internal — Configures the peer as internal.
external — Configures the peer as external.

updated-error-handling

Syntax  
[no] updated-error-handling

Context  
config>service>vprn:bgp>group
config>service>vprn:bgp>group>neighbor

Description  
This command controls whether SROS utilizes the new neighbor-complete bit when processing optional transitive path attributes and advertising them to the associated BGP neighbor.

This command also controls if SROS utilizes the error handling mechanism for optional-transitive path attributes.

Default  
no updated-error-handling

ttl-security

Syntax  
ttl-security min-ttl-value
no ttl-security

Context  
config>service>vprn:bgp>group
config>service>vprn:bgp>group>neighbor

Description  
Configure TTL security parameters for incoming packets.

Parameters  
min-ttl-value — Specify the minimum TTL value for an incoming BGP packet.
<table>
<thead>
<tr>
<th><strong>Values</strong></th>
<th>1 — 255</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Default</strong></td>
<td>1</td>
</tr>
</tbody>
</table>
**OSPF Commands**

### ospf

**Syntax**

```
[no] ospf
```

**Context**

`config>service>vprn`

**Description**

This command enables access to the context to enable an OSPF protocol instance. When an OSPF instance is created, the protocol is enabled. To start or suspend execution of the OSPF protocol without affecting the configuration, use the `no shutdown` command. The `no` form of the command deletes the OSPF protocol instance removing all associated configuration parameters.

**Default**

`no ospf` — The OSPF protocol is not enabled.

### ospf3

**Syntax**

```
ospf3 [instance-id] [router-id]
[no] ospf3 instance-id
```

**Context**

`config>service>vprn`

**Description**

This command creates an OSPFv3 routing instance and then enters the associated context to configure associated protocol parameters. When an OSPFv3 instance is created, the protocol is enabled. To start or suspend execution of the OSPF.

The `no` form of the command deletes the OSPFv3 protocol instance, removing all associated configuration parameters.

**Default**

`no default`

**Parameters**

`instance-id` — Specify the instance ID for the OSPFv3 instance being created or modified. The instance ID must match the specified range based on the address family. For ipv6-unicast, the instance id must be between 0 and 31. For ipv4-unicast the instance id must be between 64-95.

- **Values**
  - 0 — 31: IPV6 unicast
  - 64—95: IPV4 unicast
advertise-router-capability

Syntax: advertise-router-capability { link | area | as }

no advertise-router-capability

Context: config>service>vprn>ospf
config>service>vprn>ospf3

Description: This command enables the advertisement of router capabilities as defined in the IETF RFC 4970. This adds a new TLV based mechanism, allowing OSPF (OSPFv2 and OSPFv3) router to advertise specific capabilities including Traffic Engineering capability, graceful restart helper support and stub router support.

The parameters (link, area & as) control the scope of the capabilities advertisements.

The no form of this command, disables this capability.

Default: no advertise-router-capability

Parameters:

link — Capabilities are only advertised over local link and not flooded beyond.

area — Capabilities are only advertised within the area of origin.

as — Capabilities are only advertised throughout the entire autonomous system.

area

Syntax: [no] area area-id

Context: config>service>vprn>ospf
config>service>vprn>ospf3

Description: This command creates the context to configure an OSPF area. An area is a collection of network segments within an AS that have been administratively grouped together. The area ID can be specified in dotted decimal notation or as a 32-bit decimal integer.

The no form of the command deletes the specified area from the configuration. Deleting the area also removes the OSPF configuration of all the interfaces, virtual-links, sham-links, and address-ranges etc., that are currently assigned to this area.

Default: no area — No OSPF areas are defined.

Parameters:

area-id — The OSPF area ID expressed in dotted decimal notation or as a 32-bit decimal integer.

Values:

<table>
<thead>
<tr>
<th>Values</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.0 — 255.255.255.255 (dotted decimal)</td>
<td></td>
</tr>
<tr>
<td>0 — 4294967295  (decimal integer)</td>
<td></td>
</tr>
</tbody>
</table>

area-range

Syntax: area-range ip-prefix/prefix-length [advertise | not-advertise]

no area-range ip-prefix/mask

no area-range ip-prefix/mask
Virtual Private Routed Network Services

Context
config>service>vprn>ospf>area
ospf>service>vprn>nssa
config>service>vprn>ospf3>area

Description
This command creates ranges of addresses on an Area Border Router (ABR) for the purpose of route summarization or suppression. When a range is created, the range is configured to be advertised or not advertised into other areas. Multiple range commands may be used to summarize or hide different ranges. In the case of overlapping ranges, the most specific range command applies.

ABRs send summary link advertisements to describe routes to other areas. To minimize the number of advertisements that are flooded, you can summarize a range of IP addresses and send reachability information about these addresses in an LSA.

The no form of the command deletes the range (non) advertisement.

Default
no area-range — No range of addresses are defined.

Special Cases
NSSA Context — In the NSSA context, the option specifies that the range applies to external routes (via type-7 LSAs) learned within the NSSA when the routes are advertised to other areas as type-5 LSAs.

Area Context — If this command is not entered under the NSSA context, the range applies to summary LSAs even if the area is an NSSA.

Parameters
ipv6-prefix/prefix-length — The IP prefix in dotted decimal notation for the range used by the ABR to advertise that summarizes the area into another area.

Values
ipv6-prefix - x:x:x:x:x:x:x:x (eight 16-bit pieces)
x:x:x:x:x:x:d.d.d
- x [0..FFFF]H - d [0..255]D
prefix-length - [0..128]

mask — The subnet mask for the range expressed as a decimal integer mask length or in dotted decimal notation.

Values
0 — 32 (mask length), 0.0.0.0 — 255.255.255.255 (dotted decimal)

advertise | not-advertise — Specifies whether or not to advertise the summarized range of addresses into other areas. The advertise keyword indicates the range will be advertised, and the keyword not-advertise indicates the range will not be advertised.

The default is advertise.

blackhole-aggregate

Syntax
[no] blackhole-aggregate

Context
config>service>vprn>ospf>area
config>service>vprn>ospf3>area

Description
This command installs a low priority blackhole route for the entire aggregate. Existing routes that make up the aggregate will have a higher priority and only the components of the range for which no route exists are blackholed.
It is possible that when performing area aggregation, addresses may be included in the range for which no actual route exists. This can cause routing loops. To avoid this problem configure the blackhole aggregate option.

The **no** form of this command removes this option.

**Default**

blackhole-aggregate

### interface

**Syntax**  

```  
[no] interface ip-int-name [secondary]  
```  

**Context**  

```  
config>service>vprn>ospf>area  
config>service>vprn>ospf3>area  
```  

**Description**  

This command creates a context to configure an OSPF interface.

By default interfaces are not activated in any interior gateway protocol such as OSPF unless explicitly configured.

The **no** form of the command deletes the OSPF interface configuration for this interface. The `shutdown` command in the `config>router>ospf>interface` context can be used to disable an interface without removing the configuration for the interface.

**Default**  

no interface — No OSPF interfaces are defined.

**Parameters**  

- `ip-int-name` — The IP interface name. Interface names must be unique within the group of defined IP interfaces for `config router interface` and `config service vprn interface` commands. An interface name cannot be in the form of an IP address. Interface names can be any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

If the IP interface name does not exist or does not have an IP address configured an error message will be returned.

If the IP interface exists in a different area it will be moved to this area.

- `secondary` — Allows multiple secondary adjacencies to be established over a single IP interface.

### sham-link

**Syntax**  

```  
sham-link ip-int-name ip-address  
```  

**Context**  

```  
config>service>vprn>ospf>area  
```  

**Description**  

This command is similar to a virtual link with the exception that metric must be included in order to distinguish the cost between the MPLS-VPRN link and the backdoor.

**Parameters**  

- `ip-int-name` — The local interface name used for the sham-link. This is a mandatory parameter and interface names must be unique within the group of defined IP interfaces for `config router interface`, `config service ies interface` and `config service vprn interface` commands. An interface name cannot be in the form of an IP address. Interface names can be any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string
contains special characters, the entire string must be enclosed within double quotes. If the IP interface name does not exist or does not have an IP address configured, an error message will be returned.

\textit{ip-address} — The IP address of the SHAM-link neighbor in IP address dotted decimal notation. This parameter is the remote peer of the sham link’s IP address used to set up the SHAM link. This is a mandatory parameter and must be a valid IP address.

\section*{advertise-subnet}

\textbf{Syntax} \[\text{no}\] advertise-subnet

\textbf{Context} config>service>vprn>ospf>area>if

\textbf{Description} This command enables advertising point-to-point interfaces as subnet routes (network number and mask). When disabled, point-to-point interfaces are advertised as host routes.

Note that this command is not supported in the OSPF3 context.

The \texttt{no} form of the command disables advertising point-to-point interfaces as subnet routes meaning they are advertised as host routes.

\textbf{Default} advertise-subnet — Advertises point-to-point interfaces as subnet routes.

\section*{authentication}

\textbf{Syntax} authentication bidirectional \textit{sa-name}

authentication inbound \textit{sa-name} outbound \textit{sa-name}

\texttt{no} authentication

\textbf{Context} config>service>vprn>ospf3>area>if

\textbf{Description} This command configures OSPFv3 confidentiality authentication.

The \texttt{no} form of the command removes the SA name from the configuration.

\textbf{Parameters} bidirectional \textit{sa-name} — Specifies the IPSec security association name in case the OSPFv3 traffic on the interface has to be authenticated.

inbound \textit{sa-name} — Specifies the IPSec security association name in case the OSPFv3 traffic on the interface has to be authenticated.

outbound \textit{sa-name} — Specifies the IPSec security association name in case the OSPFv3 traffic on the interface has to be authenticated.

\section*{authentication-key}

\textbf{Syntax} authentication-key [authentication-key | hash-key] [hash | hash2]

\texttt{no} authentication-key

\textbf{Context} config>service>vprn>ospf>area>if
config>service>vprn>ospf>area>virtual-link
config>service>vprn>ospf>area>sham-link

**Description**
This command configures the password used by the OSPF interface or virtual-link to send and receive OSPF protocol packets on the interface when simple password authentication is configured.

Note that this command is not valid in the OSPF3 context.

All neighboring routers must use the same type of authentication and password for proper protocol communication. If the `authentication-type` is configured as password, then this key must be configured.

By default, no authentication key is configured.

Note that this command is not supported in the OSPF context.

The **no** form of the command removes the authentication key.

**Default**
`no authentication-key` — No authentication key is defined.

**Parameters**
- `authentication-key` — The authentication key. The key can be any combination of ASCII characters up to 8 characters in length (unencrypted). If spaces are used in the string, enclose the entire string in quotation marks (" ").
- `hash-key` — The hash key. The key can be any combination of ASCII characters up to 22 characters in length (encrypted). If spaces are used in the string, enclose the entire string in quotation marks (" ").

  This is useful when a user must configure the parameter, but, for security purposes, the actual unencrypted key value is not provided.

- `hash` — Specifies the key is entered in an encrypted form. If the `hash` parameter is not used, the key is assumed to be in a non-encrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the `hash` parameter specified.
- `hash2` — Specifies the key is entered in a more complex encrypted form. If the `hash2` parameter is not used, the less encrypted `hash` form is assumed.

**authentication-type**

**Syntax**

```
authentication-type {password | message-digest}
no authentication-type
```

**Context**

```
config>service>vprn>ospf>area>if
config>service>vprn>ospf>area>virtual-link
```

**Description**
This command enables authentication and specifies the type of authentication to be used on the OSPF interface, virtual-link, and sham-link.

Note that this command is not valid in the OSPF3 context.

Both simple `password` and `message-digest` authentication are supported.

By default, authentication is not enabled on an interface.

The **no** form of the command disables authentication on the interface.

Note that this command is not supported in the OSPF context.
Default: no authentication — No authentication is enabled on an interface.

Parameters:
- **password** — This keyword enables simple password (plain text) authentication. If authentication is enabled and no authentication type is specified in the command, simple password authentication is enabled.
- **message-digest** — This keyword enables message digest MD5 authentication in accordance with RFC1321. If this option is configured, then at least one message-digest-key must be configured.

**bfd-enable**

**Syntax:**
bfd-enable [remain-down-on-failure]  
no bfd-enable

**Context:**
config>service>vprn>ospf>area>if  
config>service>vprn>ospf3>area>if

**Description:**
This command enables the use of bi-directional forwarding (BFD) to control the state of the associated protocol interface. By enabling BFD on a given protocol interface, the state of the protocol interface is tied to the state of the BFD session between the local node and the remote node. The parameters used for the BFD are set via the BFD command under the IP interface.

The **no** form of this command removes BFD from the associated IGP protocol adjacency.

**Default:** no bfd-enable

**Parameters:**
- **remain-down-on-failure** — Forces adjacency down on BFD failure.

**dead-interval**

**Syntax:**
dead-interval seconds  
no dead-interval

**Context:**
config>service>vprn>ospf>area>if  
config>service>vprn>ospf>area>virtual-link  
config>service>vprn>ospf3>area>if  
config>service>vprn>ospf3>area>virtual-link  
config>service>vprn>ospf>area>sham-link

**Description:**
This command configures the time, in seconds, that OSPF waits before declaring a neighbor router down. If no hello packets are received from a neighbor for the duration of the dead interval, the router is assumed to be down. The minimum interval must be two times the hello interval.

The **no** form of the command reverts to the default value.

**Default:** 40

**Special Cases:**
- **OSPF Interface** — If the dead-interval configured applies to an interface, then all nodes on the subnet must have the same dead interval.
Virtual Link — If the **dead-interval** configured applies to a virtual link, then the interval on both termination points of the virtual link must have the same dead interval.

Sham-link — If the **dead-interval** configured applies to a sham-link, then the interval on both endpoints of the sham-link must have the same dead interval.

**Parameters**

**seconds** — The dead interval expressed as a decimal integer.

**Values**

- 2 — 2147483647 seconds

**graceful-restart**

**Syntax**

```plaintext
[no] graceful-restart
```

**Context**

```
config>service>vprn>ospf
```

**Description**

This command enables or disables graceful-restart for VPRN OSPF.

This command is not available for OSPF3.

**helper-disable**

**Syntax**

```plaintext
helper-disable
```

**Context**

```
config>service>vprn>ospf>graceful-restart
```

**Description**

This command disables the helper support for graceful restart.

When **graceful-restart** is enabled, the router can be a helper (meaning that the router is helping a neighbor to restart) or be a restarting router or both. The supports only helper mode. This facilitates the graceful restart of neighbors but will not act as a restarting router (meaning that the will not help the neighbors to restart).

This command is not available for OSPF3.

The **no** **helper-disable** command enables helper support and is the default when graceful-restart is enabled.

**Default**

disabled

**ignore-dn-bit**

**Syntax**

```plaintext
[no] ignore-dn-bit
```

**Context**

```
config>service>vprn>ospf
config>service>vprn>ospf3
```

**Description**

This command specifies whether to suppress the setting of the DN bit for OSPF or OSPF3 LSA packets generated by this instance of OSPF or OSPF3 on the router.

The **no** form of the command enables the OSPF or OSPF3 router to follow the normal procedure to determine whether to set the DN bit.
Virtual Private Routed Network Services

**Default**

no ignore-dn-bit

**hello-interval**

**Syntax**

```plaintext
hello-interval seconds
no hello-interval
```

**Context**

```plaintext
config>service>vprn>ospf>area>if
config>service>vprn>ospf3>area>if
config>service>vprn>ospf>area>virtual-link
config>service>vprn>ospf3>area>virtual-link
config>service>vprn>ospf>area>sham-link
```

**Description**

This command configures the interval between OSPF hellos issued on the interface, virtual link, or sham-link.

The hello interval, in combination with the dead-interval, is used to establish and maintain the adjacency. Use this parameter to edit the frequency that hello packets are sent.

Reducing the interval, in combination with an appropriate reduction in the associated dead-interval, allows for faster detection of link and/or router failures at the cost of higher processing costs.

The no form of this command reverts to the default value.

**Default**

```plaintext
hello-interval 10 — A 10-second hello interval.
```

**Special Cases**

**OSPF Interface** — If the hello-interval configured applies to an interface, then all nodes on the subnet must have the same hello interval.

**Virtual Link** — If the hello-interval configured applies to a virtual link, then the interval on both termination points of the virtual link must have the same hello interval.

**Sham Link** — If the hello-interval configured applies to a sham-link, then the interval on both endpoints of the sham-link must have the same hello interval

**Parameters**

```plaintext
seconds — The hello interval in seconds expressed as a decimal integer.

Values

1 — 65535
```

**interface-type**

**Syntax**

```plaintext
interface-type {broadcast | point-to-point}
no interface-type
```

**Context**

```plaintext
config>service>vprn>ospf>area>if
config>service>vprn>ospf3>area>if
```

**Description**

This command configures the interface type to be either broadcast or point-to-point.
Use this command to set the interface type of an Ethernet link to point-to-point to avoid having to carry the broadcast adjacency maintenance overhead if the Ethernet link provided the link is used as a point-to-point.

If the interface type is not known at the time the interface is added to OSPF and subsequently the IP interface is bound (or moved) to a different interface type, this command must be entered manually.

The **no** form of the command reverts to the default value.

**Default**
- `point-to-point` — If the physical interface is SONET.
- `broadcast` — If the physical interface is Ethernet or unknown.

**Special Cases**
- **Virtual-Link** — A virtual link is always regarded as a point-to-point interface and not configurable.

**Parameters**
- `broadcast` — Configures the interface to maintain this link as a broadcast network. To significantly improve adjacency forming and network convergence, a network should be configured as point-to-point if only two routers are connected, even if the network is a broadcast media such as Ethernet.
- `point-to-point` — Configures the interface to maintain this link as a point-to-point link.

---

**loopfree-alternate-exclude**

**Syntax**
- `[no] loopfree-alternate-exclude

**Context**
- `configure>service>vprn>ospf>area`
- `configure>service>vprn>ospf3>area`
- `configure>service>vprn>ospf>area>interface`
- `configure>service>vprn>ospf3>area>interface`

**Description**
This command instructs IGP to not include a specific interface or all interfaces participating in a specific IS-IS level or OSPF area in the SPF LFA computation. This provides a way of reducing the LFA SPF calculation where it is not needed.

When an interface is excluded from the LFA SPF in IS-IS, it is excluded in both level 1 and level 2. When it is excluded from the LFA SPF in OSPF, it is excluded in all areas. However, the above OSPF command can only be executed under the area in which the specified interface is primary and once enabled, the interface is excluded in that area and in all other areas where the interface is secondary. If the user attempts to apply it to an area where the interface is secondary, the command will fail.

The **no** form of this command re-instates the default value for this command.

**Default**
- `no loopfree-alternate-exclude.`
**lsa-filter-out**

**Syntax**

```
lsa-filter-out [all | except-own-rtrlsa | except-own-rtrlsa-and-defaults]
no lsa-filter-out
```

**Context**

```
config>router>ospf>area>interface
config>router>ospf3>area>interface
config>service>vprn>ospf>area>interface
config>service>vprn>ospf3>area>interface
```

**Description**

This command enables filtering of outgoing OSPF LSAs on the selected OSPFv2 or OSPFv3 interface. Three filtering options are provided:

- Do not flood any LSAs out the interface. This option is suitable if the neighbor is simply-connected and has a statically configured default route with the address of this interface as next-hop.
- Flood the router’s own router-LSA out the interface and suppress all other flooded LSAs. This option is suitable if the neighbor is simply-connected and has a statically configured default route with a loopback or system interface address (contained in the router-LSA) as next-hop.
- Flood the router’s own router-LSA and all self-generated type-3, type-5 and type-7 LSAs advertising a default route (0/0) out the interface; suppress all other flooded LSAs. This option is suitable if the neighbor is simply-connected and does not have a statically configured default route.

The `no` form of this command disables OSPF LSA filtering (normal operation).

**Default**

`no lsa-filter-out`

**multicast-import**

**Syntax**

```
[no] multicast-import
```

**Context**

```
config>service>vprn>ospf
config>service>vprn>ospf3
```

**Description**

This command enables the submission of routes into the multicast Route Table Manager (RTM) by OSPF.

The `no` form of the command disables the submission of routes into the multicast RTM.

**Default**

`no multicast-import`

**message-digest-key**

**Syntax**

```
message-digest-key keyid md5 [key | hash-key] [hash]
no message-digest-key keyid
```

**Context**

```
config>service>vprn>ospf>area>if
config>service>vprn>ospf>area>virtual-link
config>service>vprn>ospf>area>sham-link
```
OSPF Commands

**Description**
This command configures a message digest key when MD5 authentication is enabled on the interface, virtual-link or sham-link. Multiple message digest keys can be configured.

Note that this command is not valid in the OSPF3 context.

The no form of the command removes the message digest key identified by the *key-id*.

**Default**
No message digest keys are defined.

**Parameters**
- **keyid** — The *keyid* is expressed as a decimal integer.
  - **Values**
    - 1 — 255
- **md5 key** — The MD5 key. The *key* can be any alphanumeric string up to 16 characters in length.
- **md5 hash-key** — The MD5 hash key. The key can be any combination of ASCII characters up to 32 characters in length (encrypted). If spaces are used in the string, enclose the entire string in quotation marks (" ").
  - This is useful when a user must configure the parameter, but, for security purposes, the actual unencrypted key value is not provided.
- **hash** — Specifies the key is entered in an encrypted form. If the *hash* parameter is not used, the key is assumed to be in a non-encrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the *hash* parameter specified.

**metric**

**Syntax**
```
metric metric
no metric
```

**Context**
```
config>service>vprn>ospf>area>if
config>service>vprn>ospf3>area>if
config>service>vprn>ospf>area>sham-link
```

**Description**
This command configures an explicit route cost metric for the OSPF interface that overrides the metrics calculated based on the speed of the underlying link.

The no form of the command deletes the manually configured interface metric, so the interface uses the computed metric based on the *reference-bandwidth* command setting and the speed of the underlying link.

**Default**
no metric — The metric is based on *reference-bandwidth* setting and the link speed.

**Parameters**
- **metric** — The metric to be applied to the interface expressed as a decimal integer.
  - **Values**
    - 1 — 65535

**mtu**

**Syntax**
```
mtu bytes
no mtu
```

**Context**
```
config>service>vprn>ospf>area>if
```

Virtual Private Routed Network Services

config>service>vprn>ospf3>area>if

Description
This command configures the OSPF packet size used on this interface. If this parameter is not configured, OSPF derives the MTU value from the MTU configured (default or explicitly) in the following contexts:
- config>port>ethernet
- config>port>sonet-sdh>path
- config>port>tdm>t3-e3
- config>port>tdm>t1-e1>channel-group

If this parameter is configured, the smaller value between the value configured here and the MTU configured (default or explicitly) in an above-mentioned context is used.

To determine the actual packet size add 14 bytes for an Ethernet packet and 18 bytes for a tagged Ethernet packet to the size of the OSPF (IP) packet MTU configured in this command.

Use the no form of this command to revert to default.

Default
no mtu — Uses the value derived from the MTU configured in the config>port context.

Parameters
bytes — The MTU to be used by OSPF for this logical interface in bytes.

Values
512 — 9198 (9212-14) (Depends on the physical media)

passive

Syntax
[no] passive

Context
config>service>vprn>ospf>area>if
config>service>vprn>ospf3>area>if

Description
This command adds the passive property to the OSPF interface where passive interfaces are advertised as OSPF interfaces but do not run the OSPF protocol.

By default, only interface addresses that are configured for OSPF will be advertised as OSPF interfaces. The passive parameter allows an interface to be advertised as an OSPF interface without running the OSPF protocol.

While in passive mode, the interface will ignore ingress OSPF protocol packets and not transmit any OSPF protocol packets.

The no form of the command removes the passive property from the OSPF interface.

Default
Service interfaces defined in config>router>service-prefix are passive.
All other interfaces are not passive.

priority

Syntax
priority number
no priority

Context
config>service>vprn>ospf>area>if
config>service>vprn>ospf3>area>if

Description
This command configures the priority of the OSPF interface that is used an election of the designated router on on the subnet.

This parameter is only used if the interface is of type broadcast. The router with the highest priority interface becomes the designated router. A router with priority 0 is not eligible to be Designated Router or Backup Designated Router.

The no form of the command reverts the interface priority to the default value.

Default
priority 1

Parameters
number — The interface priority expressed as a decimal integer. A value of 0 indicates the router is not eligible to be the Designated Router of Backup Designated Router on the interface subnet.

Values
0 — 255

retransmit-interval

Syntax
retransmit-interval seconds
no retransmit-interval

Context
config>service>vprn>ospf>area>if
config>service>vprn>ospf>area>virtual-link
config>service>vprn>ospf3>area>if
config>service>vprn>ospf3>area>virtual-link
config>service>vprn>ospf>area>sham-link

Description
This command specifies the length of time, in seconds, that OSPF will wait before retransmitting an unacknowledged link state advertisement (LSA) to an OSPF neighbor.

The value should be longer than the expected round trip delay between any two routers on the attached network. Once the retransmit-interval expires and no acknowledgement has been received, the LSA will be retransmitted.

The no form of this command reverts to the default interval.

Default
retransmit-interval 5

Parameters
seconds — The retransmit interval in seconds expressed as a decimal integer.

Values
1 — 3600

transit-delay

Syntax
transit-delay seconds
no transit-delay

Context
config>service>vprn>ospf>area>if
config>service>vprn>ospf3>area>if
config>service>vprn>ospf>area>virtual-link
config>service>vprn>ospf3>area>virtual-link
config>service>vprn>ospf>area>sham-link

**Description**
This command configures the estimated time, in seconds, that it takes to transmit a link state advertisement (LSA) on the interface or virtual link or sham-link.

The no form of this command reverts to the default delay time.

**Default**
transit-delay 1

**Parameters**
seconds — The transit delay in seconds expressed as a decimal integer.

<table>
<thead>
<tr>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 — 3600</td>
</tr>
</tbody>
</table>

**key-rollover-interval**

**Syntax**
key-rollover-interval key-rollover-interval

**Context**
config>service>vprn>ospf3>area

**Description**
This command configures the key rollover interval.

The no form of the command reverts to the default.

**Default**
10

**Parameters**
key-rollover-interval — Specifies the time, in seconds, after which a key rollover will start.

<table>
<thead>
<tr>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>10 — 300</td>
</tr>
</tbody>
</table>

**loopfree-alternate-exclude**

**Syntax**
[no] loopfree-alternate-exclude

**Context**
config>service>vprn>ospf3>area

**Description**
This command specifies whether or not the OSPF area should be excluded during LFA calculations. When enabled, the OSPF area is excluded from LFA calculations. When disabled (the default), the OSPF area is included in LFA calculations.

The no form of the command includes the OSPF area in LFA calculations.

**Default**
disabled

**nssa**

**Syntax**
[no] nssa

**Context**
config>service>vprn>ospf>area
cfgur>service>vprn>ospf3>area

**Description**
This command creates the context to configure an OSPF Not So Stubby Area (NSSA) and adds/removes the NSSA designation from the area.
NSSAs are similar to stub areas in that no external routes are imported into the area from other OSPF areas. The major difference between a stub area and an NSSA is an NSSA has the capability to flood external routes that it learns throughout its area and via an ABR to the entire OSPF domain.

Existing virtual links of a non-stub or NSSA area will be removed when the designation is changed to NSSA or stub.

An area can be designated as stub or NSSA but never both at the same time.

By default, an area is not configured as an NSSA area.

The no form of the command removes the NSSA designation and configuration context from the area.

Default no nssa — The OSPF area is not an NSSA.

** originate-default-route **

** Syntax** originate-default-route [type-7]  
no originate-default-route

** Context** config>service>vprn>ospf>area>nssa  
config>service>vprn>ospf3>area>nssa

** Description** This command enables the generation of a default route and its LSA type (3 or 7) into a Not So Stubby Area (NSSA) by an NSSA Area Border Router (ABR).

When configuring an NSSA with no summaries, the ABR will inject a type 3 LSA default route into the NSSA area. Some older implementations expect a type 7 LSA default route.

The no form of the command disables origination of a default route.

Default no originate-default-route — A default route is not originated.

** Parameters** type-7 — Specifies a type 7 LSA should be used for the default route.

Configure this parameter to inject a type-7 LSA default route instead the type 3 LSA into the NSSA configured with no summaries.

To revert to a type 3 LSA, enter originate-default-route without the type-7 parameter.

Default Type 3 LSA for the default route.

** redistribute-external **

** Syntax** [no] redistribute-external

** Context** config>service>vprn>ospf>area>nssa  
config>service>vprn>ospf3>area>nssa

** Description** This command enables the redistribution of external routes into the Not So Stubby Area (NSSA) or an NSSA area border router (ABR) that is exporting the routes into non-NSSA areas.

NSSA or Not So Stubby Areas are similar to stub areas in that no external routes are imported into the area from other OSPF areas. The major difference between a stub area and an NSSA is that the NSSA
has the capability to flood external routes that it learns (providing it is an ASBR) throughout its area and via an Area Border Router to the entire OSPF domain.

The no form of the command disables the default behavior to automatically redistribute external routes into the NSSA area from the NSSA ABR.

Default  

**redistribute-external** — External routes are redistributed into the NSSA.

---

### summaries

**Syntax**  

[no] summaries

**Context**  

config>service>vprn>ospf>area>nssa  
config>service>vprn>ospf>area>stub  
config>service>vprn>ospf3>area>nssa

**Description**  

This command enables sending summary (type 3) advertisements into a stub area or Not So Stubby Area (NSSA) on an Area Border Router (ABR). This parameter is particularly useful to reduce the size of the routing and Link State Database (LSDB) tables within the stub or nssa area. By default, summary route advertisements are sent into the stub area or NSSA.

The no form of the command disables sending summary route advertisements and, for stub areas, only the default route is advertised by the ABR.

Default  

**summaries** — Summary routes are advertised by the ABR into the stub area or NSSA.

---

### stub

**Syntax**  

[no] stub

**Context**  

config>service>vprn>ospf>area  
config>service>vprn>ospf3>area

**Description**  

This command enables access to the context to configure an OSPF stub area and adds/removes the stub designation from the area. External routing information is not flooded into stub areas. All routers in the stub area must be configured with the **stub** command. An OSPF area cannot be both an NSSA and a stub area. Existing virtual links of a non STUB or NSSA area will be removed when its designation is changed to NSSA or STUB.

By default, an area is not a stub area.

The no form of the command removes the stub designation and configuration context from the area.

Default  

**no stub** — The area is not configured as a stub area.

---

### default-metric

**Syntax**  

default-metric metric  
no default-metric
**default-metric**

**Parameters**

- `metric` — The metric expressed as a decimal integer for the default route cost to be advertised into the stub area.

**Values**

- `1 — 16777215`

---

**virtual-link**

**Syntax**

```plaintext
[no] virtual-link router-id transit-area area-id
```

**Context**

- `config>service>vprn>ospf>area`  
- `config>service>vprn>ospf3>area`

**Description**

This command configures a virtual link to connect area border routers to the backbone via a virtual link. The backbone area (area 0.0.0.0) must be contiguous and all other areas must be connected to the backbone area. If it is not practical to connect an area to the backbone (see area 0.0.0.2 in the picture below) then the area border routers (routers 1 and 2 in the picture below) must be connected via a virtual link. The two area border routers will form a point-to-point like adjacency across the transit area (area 0.0.0.1 in the picture below). A virtual link can only be configured while in the area 0.0.0.0 context.

The `router-id` specified in this command must be associated with the virtual neighbor. The transit area cannot be a stub area or a Not So Stubby Area (NSSA).

The **no** form of the command deletes the virtual link.

**Default**

- No virtual link is defined.

**Parameters**

- `router-id` — The router ID of the virtual neighbor in IP address dotted decimal notation.
- `transit-area area-id` — The area-id specified identifies the transit area that links the backbone area with the area that has no physical connection with the backbone.

The OSPF backbone area, area 0.0.0.0, must be contiguous and all other areas must be connected to the backbone area. The backbone distributes routing information between areas. If it is not practical to connect an area to the backbone (see Area 0.0.0.5 in Figure 164) then the area border routers (such as routers Y and Z) must be connected via a virtual link. The two area border routers form a point-to-point-like adjacency across the transit area (see Area 0.0.0.4).
compatible-rfc1583

Syntax

[no] compatible-rfc1583

Context

config>service>vprn>ospf

Description

This command enables OSPF summary and external route calculations in compliance with RFC1583 and earlier RFCs.

RFC1583 and earlier RFCs use a different method to calculate summary and external route costs. To avoid routing loops, all routers in an OSPF domain should perform the same calculation method.

Although it would be favorable to require all routers to run a more current compliancy level, this command allows the router to use obsolete methods of calculation.

This command is not supported in OSPF3.

The no form of the command enables the post-RFC1583 method of summary and external route calculation.

Default

compatible-rfc1583 — RFC1583 compliance is enabled.

export

Syntax

export policy-name [policy-name …]

no export

Context

config>service>vprn>ospf
OSPF Commands

config>service>vprn>ospf3

**Description**
This command associates export route policies to determine which routes are exported from the route table to OSPF. Export policies are only in effect if OSPF is configured as an ASBR.

If no export policy is specified, non-OSPF routes are not exported from the routing table manager to OSPF.

If multiple policy names are specified, the policies are evaluated in the order they are specified. The first policy that matches is applied. If multiple export commands are issued, the last command entered will override the previous command. A maximum of five policy names can be specified.

The **no** form of the command removes all policies from the configuration.

**Default**

**no export** — No export route policies specified.

**Parameters**

- **policy-name** — The export route policy name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

The specified name(s) must already be defined.

---

**ospf3**

**Syntax**

```plaintext
external-db-overflow

limit interval

no external-db-overflow
```

**Context**

```plaintext
config>service>vprn>ospf

config>service>vprn>ospf3
```

**Description**

This command enables limits on the number of non-default AS-external-LSA entries that can be stored in the LSDB and specifies a wait timer before processing these after the limit is exceeded.

The **limit** value specifies the maximum number of non-default AS-external-LSA entries that can be stored in the link-state database (LSDB). Placing a limit on the non-default AS-external-LSAs in the LSDB protects the router from receiving an excessive number of external routes that consume excessive memory or CPU resources. If the number of routes reach or exceed the **limit**, the table is in an overflow state. When in an overflow state, the router will not originate any new AS-external-LSAs. In fact, it withdraws all the self-originated non-default external LSAs.

The **interval** specifies the amount of time to wait after an overflow state before regenerating and processing non-default AS-external-LSAs. The waiting period acts like a dampening period preventing the router from continuously running Shortest Path First (SPF) calculations caused by the excessive number of non-default AS-external LSAs.

The **external-db-overflow** must be set identically on all routers attached to any regular OSPF area. OSPF stub areas and not-so-stubby areas (NSSAs) are excluded.

The **no** form of the command disables limiting the number of non-default AS-external-LSA entries.

**Default**

**no external-db-overflow** — No limit on non-default AS-external-LSA entries.

**Parameters**

- **limit** — The maximum number of non-default AS-external-LSA entries that can be stored in the LSDB before going into an overflow state expressed as a decimal integer.

**Values**

-1 — 2147483647
interval — The number of seconds after entering an overflow state before attempting to process non-default AS-external-LSAs expressed as a decimal integer.

Values 0 — 2147483647

external-preference

Syntax external-preference preference
no external-preference

Context config>service>vprn>ospf
config>service>vprn>ospf3

Description This command configures the preference for OSPF external routes.

A route can be learned by the router from different protocols in which case the costs are not comparable; when this occurs the preference is used to decide which route will be used.

Different protocols should not be configured with the same preference, if this occurs the tiebreaker is per the default preference table as defined in the following table. If multiple routes are learned with an identical preference using the same protocol, the lowest cost route is used.

If multiple routes are learned with an identical preference using the same protocol and the costs (metrics) are equal, then the decision of what route to use is determined by the configuration of the ecmp in the config>router context.

The no form of the command reverts to the default value.

Default external-preference 150 — OSPF external routes have a default preference of 150.

Parameters preference — The preference for external routes expressed as a decimal integer.

<table>
<thead>
<tr>
<th>Route Type</th>
<th>Preference</th>
<th>Configurable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Direct attached</td>
<td>0</td>
<td>No</td>
</tr>
<tr>
<td>Static routes</td>
<td>5</td>
<td>Yes</td>
</tr>
<tr>
<td>OSPF internal</td>
<td>10</td>
<td>Yes</td>
</tr>
<tr>
<td>IS-IS level 1 internal</td>
<td>15</td>
<td>Yes</td>
</tr>
<tr>
<td>IS-IS level 2 internal</td>
<td>18</td>
<td>Yes</td>
</tr>
<tr>
<td>RIP</td>
<td>100</td>
<td>Yes</td>
</tr>
<tr>
<td>OSPF external</td>
<td>150</td>
<td>Yes</td>
</tr>
<tr>
<td>IS-IS level 1 external</td>
<td>160</td>
<td>Yes</td>
</tr>
<tr>
<td>IS-IS level 2 external</td>
<td>165</td>
<td>Yes</td>
</tr>
<tr>
<td>BGP</td>
<td>170</td>
<td>Yes</td>
</tr>
</tbody>
</table>

a. Preference for OSPF internal routes is configured with the preference command.
ignore-dn-bit

**Syntax**

[no] ignore-dn-bit

**Context**
config>service>vprn>ospf

**Description**
This command specifies whether to ignore the DN bit for OSPF LSA packets for this instance of OSPF on the router. When enabled, the DN bit for OSPF LSA packets will be ignored. When disabled, the DN bit will not be ignored for OSPF LSA packets.

loopfree-alternate

**Syntax**

[no] loopfree-alternate

**Context**
config>service>vprn>ospf
config>service>vprn>ospf3

**Description**
This command enables Loop-Free Alternate (LFA) computation by SPF under the IS-IS routing protocol level, or under the OSPF routing protocol instance level.

When this command is enabled, it instructs the IGP SPF to attempt to pre-compute both a primary next-hop and an LFA next-hop for every learned prefix. IS-IS computes the primary SPF first and then computes the LFA SPF. The LFA backup next-hop is only available after the LFA SPF is completed. When found, the LFA next-hop is populated into the routing table along with the primary next-hop for the prefix.

The **no** form of this command disables the LFA computation by IGP SPF.

**Default**
no loopfree-alternate

overload

**Syntax**

overload [timeout seconds]
no overload

**Context**
config>service>vprn>ospf
config>service>vprn>ospf3

**Description**
This command changes the overload state of the local router so that it appears to be overloaded. When overload is enabled, the router can participate in OSPF routing, but is not used for transit traffic. Traffic destined to directly attached interfaces continue to reach the router.

To put the IGP in an overload state enter a timeout value. The IGP will enter the overload state until the timeout timer expires or a **no overload** command is executed.

If the **overload** command is encountered during the execution of an **overload-on-boot** command then this command takes precedence. This could occur as a result of a saved configuration file where
both parameters are saved. When the file is saved by the system the overload-on-boot command is saved after the overload command.

Use the no form of this command to return to the default. When the no overload command is executed, the overload state is terminated regardless the reason the protocol entered overload state.

**Default**

- no overload

**Parameters**

- **timeout seconds** — Specifies the number of seconds to reset overloading.
  - **Values**
    - 60 — 1800
  - **Default**
    - 60

### if-attribute

**Syntax**

if-attribute

**Context**

- config>router
- config>router>interface
- config>service>ies>interface
- config>service>vprn>interface

**Description**

This command creates the context to configure or apply IP interface attributes such as administrative group (admin-group) or Shared Risk Loss Group (SRLG).

### admin-group

**Syntax**

- admin-group group-name [group-name...(up to 5 max)]
- no admin-group group-name [group-name...(up to 5 max)]
- no admin-group

**Context**

- config>router>interface>if-attribute
- config>service>ies>interface>if-attribute
- config>service>vprn>interface>if-attribute
- config>router>mpls>interface

**Description**

This command configures the admin group membership of an interface. The user can apply admin groups to an IES, VPRN, network IP, or MPLS interface.

Each single operation of the admin-group command allows a maximum of five (5) groups to be specified at a time. However, a maximum of 32 groups can be added to a given interface through multiple operations. Once an admin group is bound to one or more interface, its value cannot be changed until all bindings are removed.

The configured admin-group membership will be applied in all levels/areas the interface is participating in. The same interface cannot have different memberships in different levels/areas.

It should be noted that only the admin groups bound to an MPLS interface are advertised in TE link TLVs and sub-TLVs when the traffic-engineering option is enabled in IS-IS or OSPF. IES and VPRN interfaces do not have their attributes advertised in TE TLVs.
The **no** form of this command deletes one or more of the admin-group memberships of an interface. The user can also delete all memberships of an interface by not specifying a group name.

**Parameters**

*group-name* — Specifies the name of the group with up to 32 characters. The association of group name and value should be unique within an IP/MPLS domain.

**srlg-group**

**Syntax**

```
srlg-group group-name [group-name...(up to 5 max)]
no srlg-group group-name [group-name...(up to 5 max)]
no srlg-group
```

**Context**

- config>router>interface>if-attribute
- config>service>ies>interface>if-attribute
- config>service>vprn>interface>if-attribute
- config>router mpls>interface

**Description**

This command configures the SRLG membership of an interface. The user can apply SRLGs to an IES, VPRN, network IP, or MPLS interface.

An interface can belong to up to 64 SRLG groups. However, each single operation of the `srlg-group` command allows a maximum of five (5) groups to be specified at a time. Once an SRLG group is bound to one or more interface, its value cannot be changed until all bindings are removed.

The configured SRLG membership will be applied in all levels/areas the interface is participating in. The same interface cannot have different memberships in different levels/areas.

It should be noted that only the SRLGs bound to an MPLS interface are advertised in TE link TLVs and sub-TLVs when the `traffic-engineering` option is enabled in IS-IS or OSPF. IES and VPRN interfaces do not have their attributes advertised in TE TLVs.

The **no** form of this command deletes one or more of the SRLG memberships of an interface. The user can also delete all memberships of an interface by not specifying a group name.

**Parameters**

*group-name* — Specifies the name of the group, up to 32 characters. The association of group name and value should be unique within an IP/MPLS domain.

**lfa-policy-map**

**Syntax**

```
lfa-policy-map route-nh-template template-name
no lfa-policy-map
```

**Context**

- config>router>ospf>area>interface
- config>router>ospf3>area>interface
- config>router>isis>interface
- config>service>vprn>ospf>area>interface
- config>service>vprn>ospf3>area>interface

**Description**

This command applies a route next-hop policy template to an OSPF or IS-IS interface.

When a route next-hop policy template is applied to an interface in IS-IS, it is applied in both level 1 and level 2. When a route next-hop policy template is applied to an interface in OSPF, it is applied in
all areas. However, the command in an OSPF interface context can only be executed under the area in which the specified interface is primary and then applied in that area and in all other areas where the interface is secondary. If the user attempts to apply it to an area where the interface is secondary, the command will fail.

If the user excluded the interface from LFA using the command `loopfree-alternate-exclude`, the LFA policy, if applied to the interface, has no effect.

Finally, if the user applied a route next-hop policy template to a loopback interface or to the system interface, the command will not be rejected, but it will result in no action being taken.

The `no` form deletes the mapping of a route next-hop policy template to an OSPF or IS-IS interface.

### Parameters

`template-name` — Specifies the name of the template, up to 32 characters.

---

### loopfree-alternate-exclude

#### Syntax

```
loopfree-alternate-exclude prefix-policy prefix-policy [prefix-policy... up to 5]
no loopfree-alternate-exclude
```

#### Context

```
config>router>ospf
config>router>ospf3
config>router>isis
config>service>vprn>ospf
config>service>vprn>ospf3
```

#### Description

This command excludes from LFA SPF calculation prefixes that match a prefix entry or a tag entry in a prefix policy.

The implementation already allows the user to exclude an interface in IS-IS or OSPF, an OSPF area, or an IS-IS level from the LFA SPF.

If a prefix is excluded from LFA, then it will not be included in LFA calculation regardless of its priority. The prefix tag will, however, be used in the main SPF. Note that prefix tags are defined for the IS-IS protocol but not for the OSPF protocol.

The default action of the `loopfree-alternate-exclude` command, when not explicitly specified by the user in the prefix policy, is a “reject”. Thus, regardless if the user did or did not explicitly add the statement “default-action reject” to the prefix policy, a prefix that did not match any entry in the policy will be accepted into LFA SPF.

The `no` form deletes the exclude prefix policy.

#### Parameters

`prefix-policy prefix-policy` — Specifies the name of the prefix policy, up to 32 characters. The specified name must have been already defined.
OSPF Commands

overload-include-ext-2

Syntax  | [no] overload-include-ext-2
Context  | config>service>vprn>ospf
         | config>service>vprn>ospf3
Description | This command is used to control if external type-2 routes should be re-advertised with a maximum metric value when the system goes into overload state for any reason. When this command is enabled and the router is in overload, all external type-2 routes will be advertised with the maximum metric.

Default  | no overload-include-ext-2

overload-include-stub

Syntax  | [no] overload-include-stub
Context  | config>service>vprn>ospf
         | config>service>vprn>ospf3
Description | This command is used to determine if the OSPF stub networks should be advertised with a maximum metric value when the system goes into overload state for any reason. When enabled, the system uses the maximum metric value. When this command is enabled and the router is in overload, all stub interfaces, including loopback and system interfaces, will be advertised at the maximum metric.

Default  | no overload-include-stub

overload-on-boot

Syntax  | overload-on-boot [timeout seconds]
         | no overload
Context  | config>service>vprn>ospf
         | config>service>vprn>ospf3
Description | When the router is in an overload state, the router is used only if there is no other router to reach the destination. This command configures the IGP upon bootup in the overload state until one of the following events occur:

- The timeout timer expires.
- A manual override of the current overload state is entered with the no overload command.

The no overload command does not affect the overload-on-boot function.

The no form of the command removes the overload-on-boot functionality from the configuration.

Default  | no overload-on-boot
Parameters  | timeout seconds — Specifies the number of seconds to reset overloading.
**Values**

60 — 1800

**Default**

60

---

**preference**

**Syntax**

- `preference preference`
- `no preference`

**Context**

- `config>service>vprn>ospf`
- `config>service>vprn>ospf3`

This command configures the preference for OSPF internal routes.

A route can be learned by the router from different protocols in which case the costs are not comparable, when this occurs the preference is used to decide to which route will be used.

Different protocols should not be configured with the same preference, if this occurs the tiebreaker is per the default preference table as defined in the following table. If multiple routes are learned with an identical preference using the same protocol, the lowest cost route is used.

If multiple routes are learned with an identical preference using the same protocol and the costs (metrics) are equal, then the decision of what route to use is determined by the configuration of the `ecmp` in the `config>router` context.

The `no` form of the command reverts to the default value.

**Default**

- `preference 10` — OSPF internal routes have a preference of 10.

**Parameters**

- `preference` — The preference for internal routes expressed as a decimal integer. Defaults for different route types are listed in the following table.

---

<table>
<thead>
<tr>
<th>Route Type</th>
<th>Preference</th>
<th>Configurable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Direct attached</td>
<td>0</td>
<td>No</td>
</tr>
<tr>
<td>Static routes</td>
<td>5</td>
<td>Yes</td>
</tr>
<tr>
<td>OSPF internal</td>
<td>10</td>
<td>Yes^a</td>
</tr>
<tr>
<td>IS-IS level 1 internal</td>
<td>15</td>
<td>Yes</td>
</tr>
<tr>
<td>IS-IS level 2 internal</td>
<td>18</td>
<td>Yes</td>
</tr>
<tr>
<td>RIP</td>
<td>100</td>
<td>Yes</td>
</tr>
<tr>
<td>OSPF external</td>
<td>150</td>
<td>Yes</td>
</tr>
<tr>
<td>IS-IS level 1 external</td>
<td>160</td>
<td>Yes</td>
</tr>
<tr>
<td>IS-IS level 2 external</td>
<td>165</td>
<td>Yes</td>
</tr>
<tr>
<td>BGP</td>
<td>170</td>
<td>Yes</td>
</tr>
</tbody>
</table>

^a. Preference for OSPF internal routes is configured with the `preference` command.
reference-bandwidth

**Syntax**
```
reference-bandwidth reference-bandwidth
no reference-bandwidth
```

**Context**
```
config>service>vprn>ospf
config>service>vprn>ospf3
```

**Description**
This command configures the reference bandwidth in kilobits per second (Kbps) that provides the reference for the default costing of interfaces based on their underlying link speed.

The default interface cost is calculated as follows:

```
cost = reference-bandwidth ÷ bandwidth
```

The default `reference-bandwidth` is 100,000,000 Kbps or 100 Gbps, so the default auto-cost metrics for various link speeds are as follows:

- 10 Mbs link default cost of 10000
- 100 Mbs link default cost of 1000
- 1 Gbps link default cost of 100
- 10 Gbps link default cost of 10

The `reference-bandwidth` command assigns a default cost to the interface based on the interface speed. To override this default cost on a particular interface, use the `metric` command in the `config>router>ospf>area>interface ip-int-name` context.

The `no` form of the command reverts the reference-bandwidth to the default value.

**Default**
```
reference-bandwidth 100000000 — Reference bandwidth of 100 Gbps.
```

**Parameters**
```
reference-bandwidth — The reference bandwidth in kilobits per second expressed as a decimal integer.
```

**Values**
```
1 — 1000000000
```

super-backbone

**Syntax**
```
[no] super-backbone
```

**Context**
```
config>service>vprn>ospf
```

**Description**
This command specifies whether CE-PE functionality is required or not. The OSPF super backbone indicates the type of the LSA generated as a result of routes redistributed into OSPF. When enabled, the redistributed routes are injected as summary, external or NSSA LSAs. When disabled, the redistributed routes are injected as either external or NSSA LSAs only.

**Default**
```
no super-backbone
```
**suppress-dn-bit**

**Syntax**

```plaintext
[no] suppress-dn-bit
```

**Context**

```
config>service>vprn>ospf
config>service>vprn>ospf3
```

**Description**

This command specifies whether to suppress the setting of the DN bit for OSPF LSA packets generated by this instance of OSPF on the router. When enabled, the DN bit for OSPF LSA packets generated by this instance of the OSPF router will not be set. When disabled, this instance of the OSPF router will follow the normal procedure to determine whether to set the DN bit.

**Default**

`no suppress-dn-bit`

**timers**

**Syntax**

`timers`

**Context**

```
config>service>vprn>ospf
config>service>vprn>ospf3
```

**Description**

This command enables the context that allows for the configuration of OSPF timers. Timers control the delay between receipt of a link state advertisement (LSA) requiring a Dijkstra (Shortest Path First (SPF)) calculation and the minimum time between successive SPF calculations.

Changing the timers affect CPU utilization and network reconvergence times. Lower values reduce convergence time but increase CPU utilization. Higher values reduce CPU utilization but increase reconvergence time.

**Default**

`none`

**spf-wait**

**Syntax**

```plaintext
spf-wait max-spf-wait [spf-initial-wait [spf-second-wait]]
no spf-wait
```

**Context**

```
config>service>vprn>ospf>timers
config>service>vprn>ospf3>timers
```

**Description**

This command defines the maximum interval between two consecutive SPF calculations in milliseconds. Timers that determine when to initiate the first, second, and subsequent SPF calculations after a topology change occurs can be controlled with this command. Subsequent SPF runs (if required) will occur at exponentially increasing intervals of the `spf-second-wait` interval. For example, if the `spf-second-wait` interval is 1000, then the next SPF will run after 2000 milliseconds, and then next SPF will run after 4000 milliseconds, etc., until it reaches the `spf-wait` value. The SPF interval will stay at the `spf-wait` value until there are no more SPF runs scheduled in that interval. After a full interval without any SPF runs, the SPF interval will drop back to `spf-initial-wait`.

The timer must be entered in increments of 100 milliseconds. Values entered that do not match this requirement will be rejected.
Use the **no** form of this command to return to the default.

**Default**

`no spf-wait`

**Parameters**

`max-spf-wait` — Specifies the maximum interval in milliseconds between two consecutive SPF calculations.

- **Values**
  - 10 — 120000
  - **Default** 10000

`spf-initial-wait` — Specifies the initial SPF calculation delay in milliseconds after a topology change.

- **Values**
  - 10 — 100000
  - **Default** 1000

`spf-second-wait` — Specifies the hold time in milliseconds between the first and second SPF calculation.

- **Values**
  - 10 — 100000
  - **Default** 1000

**unicast-import-disable**

**Syntax**

`[no] unicast-import-disable`

**Context**

`config>service>vprn>ospf`

**Description**

This command allows one IGP to import its routes into RPF RTM while another IGP imports routes only into the unicast RTM.

Import policies can redistribute routes from an IGP protocol into the RPF RTM (the multicast routing table). By default, the IGP routes will not be imported into RPF RTM as such an import policy must be explicitly configured.

**Default**

`no unicast-import-disable`

**vpn-domain**

**Syntax**

`vpn-domain [type {0005 | 0105 | 0205 | 8005}] id id`

`no vpn-domain`

**Context**

`config>service>vprn>ospf`

**Description**

This command specifies type of the extended community attribute exchanged using BGP to carry the OSPF VPN domain ID. This applies to VPRN instances of OSPF only. An attempt to modify the value of this object will result in an inconsistent value error when is not a VPRN instance. The parameters are mandatory and can be entered in either order. This command is not applicable in the `config>service>vprn>ospf3` context.

This command is not supported in OSPF3.

**Default**

`no vpn-domain`
Parameters

*id* — Specifies the OSPF VPN domain in the “xxxx.xxxx.xxxx” format. This is exchanged using BGP in the extended community attribute associated with a prefix. This object applies to VPRN instances of OSPF only.

*type* — Specifies the type of the extended community attribute exchanged using BGP to carry the OSPF VPN domain ID.

**Values**

0005, 0105, 0205, 8005

### vpn-tag

**Syntax**

```
vpn-tag vpn-tag
no vpn-tag
```

**Context**

```
config>service>vprn>ospf
```

**Description**

This command specifies the route tag for an OSPF VPN on a PE router. This field is set in the tag field of the OSPF external LSAs generated by the PE. This is mainly used to prevent routing loops. This applies to VPRN instances of OSPF only. An attempt to modify the value of this object will result in an inconsistent value error when it is not a VPRN instance.

This command is not supported in OSPF3.

**Default**

```
vpn-tag 0
```

### lsa-arrival

**Syntax**

```
lsa-arrival lsa-arrival-time
no lsa-arrival
```

**Context**

```
config>service>vprn>ospf>timers
config>service>vprn>ospf3>timers
```

**Description**

This parameter defines the minimum delay that must pass between receipt of the same Link State Advertisements (LSAs) arriving from neighbors. It is recommended that the neighbors configured (lsa-generate) lsa-second-wait interval is equal or greater than the lsa-arrival timer configured here. Use the `no` form of this command to return to the default.

**Default**

```
no lsa-arrival
```

**Parameters**

*ls-arrival-time* — Specifies the timer in milliseconds. Values entered that do not match this requirement will be rejected.

**Values**

0 — 600000

### lsa-generate

**Syntax**

```
lsa-generate max-lsa-wait [lsa-initial-wait [lsa-second-wait]]
no lsa-generate-interval
```
Context  config>service>vprn>ospf>timers
        config>service>vprn>ospf3>timers

Description  This parameter customizes the throttling of OSPF LSA-generation. Timers that determine when to
generate the first, second, and subsequent LSAs can be controlled with this command. Subsequent
LSAs are generated at increasing intervals of the lsa-second-wait timer until a maximum value is
reached. Configuring the lsa-arrival interval to equal or less than the lsa-second-wait interval
configured in the lsa-generate command is recommended.

Use the no form of this command to return to the default.

Default  no lsa-generate

Parameters  max-lsa-wait — Specifies the maximum interval, in milliseconds, between two consecutive
        occurrences of an LSA being generated.

        The timer must be entered as either 1 or in millisecond increments. Values entered that do not
        match this requirement will be rejected.

        Values  1 — 600000

Description  Default
VLL Show Commands

sap-using

Syntax

```
sap-using [msap] [dyn-script] [description]
sap-using [sap sap-id] [vlan-translation | anti-spoof] [description]
sap-using interface [ip-address | ip-int-name]
sap-using [ingress | egress] filter filter-id
sap-using [ingress | egress] qos-policy qos-policy-id
```

Context

```
show>service
```

Description

This command displays SAP information.

If no optional parameters are specified, the command displays a summary of all defined SAPs.

The optional parameters restrict output to only SAPs matching the specified properties.

Parameters

- **ingress** — Specifies matching an ingress policy.
- **ingress** — Specifies matching an ingress policy.
- **ingress** — Specifies matching an ingress policy.
- **egress** — Specifies matching an egress policy.
- **qos-policy qos-policy-id** — The ingress QoS Policy ID for which to display matching SAPs.
  
  Values
  1 — 65535
- **filter filter-id** — The ingress or egress filter policy ID for which to display matching SAPs.

  Values
  1 — 65535
- **sap sap-id** — Specifies the physical port identifier portion of the SAP definition. See Common CLI Command Descriptions on page 1783 for command syntax.

**dyn-script** — Displays dynamic service SAPs information.

Output

**Show Service SAP** — The following table describes show service SAP output fields:

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port ID</td>
<td>The ID of the access port where the SAP is defined.</td>
</tr>
<tr>
<td>Svc ID</td>
<td>The service identifier.</td>
</tr>
<tr>
<td>MTU</td>
<td>The SAP MTU value.</td>
</tr>
<tr>
<td>Ing. QoS</td>
<td>The SAP ingress QoS policy number specified on the ingress SAP.</td>
</tr>
<tr>
<td>Ing Fltr</td>
<td>The MAC or IP filter policy ID applied to the ingress SAP.</td>
</tr>
</tbody>
</table>
### Sample Output

*A:Dut-A# show service sap-using

<table>
<thead>
<tr>
<th>PortId</th>
<th>SvcId</th>
<th>QoS</th>
<th>Fltr</th>
<th>Ing. QoS</th>
<th>Ing. Fltr</th>
<th>Egr. QoS</th>
<th>Egr. Fltr</th>
<th>Adm</th>
<th>Opr</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1/1:1</td>
<td>1</td>
<td>none</td>
<td>none</td>
<td>1</td>
<td>none</td>
<td>1</td>
<td>none</td>
<td>Up</td>
<td>Up</td>
</tr>
<tr>
<td>2/1/2:10/11</td>
<td>1</td>
<td>none</td>
<td>none</td>
<td>1</td>
<td>none</td>
<td>1</td>
<td>none</td>
<td>Up</td>
<td>Up</td>
</tr>
<tr>
<td>2/1/2:10/12</td>
<td>1</td>
<td>none</td>
<td>none</td>
<td>1</td>
<td>none</td>
<td>1</td>
<td>none</td>
<td>Up</td>
<td>Up</td>
</tr>
<tr>
<td>2/1/2:20/11</td>
<td>1</td>
<td>none</td>
<td>none</td>
<td>1</td>
<td>none</td>
<td>1</td>
<td>none</td>
<td>Up</td>
<td>Up</td>
</tr>
<tr>
<td>2/1/2:20/12</td>
<td>1</td>
<td>none</td>
<td>none</td>
<td>1</td>
<td>none</td>
<td>1</td>
<td>none</td>
<td>Up</td>
<td>Up</td>
</tr>
<tr>
<td>2/1/4:cp.10</td>
<td>10</td>
<td>none</td>
<td>none</td>
<td>1</td>
<td>none</td>
<td>1</td>
<td>none</td>
<td>Up</td>
<td>Up</td>
</tr>
<tr>
<td>2/1/4:cp.20</td>
<td>20</td>
<td>none</td>
<td>none</td>
<td>1</td>
<td>none</td>
<td>1</td>
<td>none</td>
<td>Up</td>
<td>Up</td>
</tr>
</tbody>
</table>

Number of SAPs: 7
sdp

**Syntax**

sdp [[sdp-id]:vc-id] | far-end ip-address] [detail]
sdp sdp-id:vc-id mrp

**Context**

show>service>id

**Description**

This command displays SDP information.

If no optional parameters are specified, a summary SDP output for all SDPs is displayed.

**Parameters**

- **sdp-id** — Specifies the SDP ID.
  
  1 — 17407

- **vc-id** — The virtual circuit ID on the SDP ID to be reset.
  
  Values 1 — 4294967295

- **far-end ip-address** — Displays only SDPs matching with the specified far-end IP address.
  
  **Default** SDPs with any far-end IP address.

- **mrp** — Specifies to display Multiple Registration Protocol (MRP) information.

- **detail** — Displays detailed SDP information.
  
  **Default** SDP summary output.

— **Show Service SDP** — The following table describes show service SDP output fields:

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SDP Id</td>
<td>The SDP identifier.</td>
</tr>
<tr>
<td>Adm MTU</td>
<td>Specifies the desired largest service frame size (in octets) that can be transmitted through this SDP to the far-end router, without requiring the packet to be fragmented.</td>
</tr>
<tr>
<td>Opr MTU</td>
<td>Specifies the actual largest service frame size (in octets) that can be transmitted through this SDP to the far-end router, without requiring the packet to be fragmented.</td>
</tr>
<tr>
<td>IP address</td>
<td>Specifies the IP address of the remote end of the GRE or MPLS tunnel defined by this SDP.</td>
</tr>
<tr>
<td>Adm Admin State</td>
<td>Specifies the desired state of the SDP.</td>
</tr>
<tr>
<td>Opr Oper State</td>
<td>Specifies the operating state of the SDP.</td>
</tr>
<tr>
<td>Deliver Delivery</td>
<td>Specifies the type of delivery used by the SDP: GRE or MPLS.</td>
</tr>
<tr>
<td>Flags</td>
<td>Specifies all the conditions that affect the operating status of this SDP.</td>
</tr>
<tr>
<td>Signal Signaling</td>
<td>Specifies the signaling protocol used to obtain the ingress and egress labels used in frames transmitted and received on the SDP.</td>
</tr>
</tbody>
</table>
Show, Clear, Debug Commands

<table>
<thead>
<tr>
<th>Label</th>
<th>Description (Continued)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last Status Change</td>
<td>Specifies the time of the most recent operating status change to this SDP.</td>
</tr>
<tr>
<td>Last Mgmt Change</td>
<td>Specifies the time of the most recent management-initiated change to this SDP.</td>
</tr>
<tr>
<td>Number of SDPs</td>
<td>Specifies the total number of SDPs displayed according to the criteria specified.</td>
</tr>
<tr>
<td>Hello Time</td>
<td>Specifies how often the SDP echo request messages are transmitted on this SDP.</td>
</tr>
<tr>
<td>Number of SDPs</td>
<td>Specifies the total number of SDPs displayed according to the criteria specified.</td>
</tr>
<tr>
<td>Hello Time</td>
<td>Specifies how often the SDP echo request messages are transmitted on this SDP.</td>
</tr>
<tr>
<td>Hello Msg Len</td>
<td>Specifies the length of the SDP echo request messages transmitted on this SDP.</td>
</tr>
<tr>
<td>Hello Timeout</td>
<td>Specifies the number of seconds to wait for an SDP echo response message before declaring a timeout.</td>
</tr>
<tr>
<td>Unmatched Replies</td>
<td>Specifies the number of SDP unmatched message replies.</td>
</tr>
<tr>
<td>Max Drop Count</td>
<td>Specifies the maximum number of consecutive SDP echo request messages that can be unacknowledged before the keepalive protocol reports a fault.</td>
</tr>
<tr>
<td>Hold Down Time</td>
<td>Specifies the amount of time to wait before the keepalive operating status is eligible to enter the alive state.</td>
</tr>
<tr>
<td>TX Hello Msgs</td>
<td>Specifies the number of SDP echo request messages transmitted since the keepalive was administratively enabled or the counter was cleared.</td>
</tr>
<tr>
<td>Rx Hello Msgs</td>
<td>Specifies the number of SDP echo request messages received since the keepalive was administratively enabled or the counter was cleared.</td>
</tr>
<tr>
<td>Associated LSP List</td>
<td>When the SDP type is MPLS, a list of LSPs used to reach the far-end router displays. All the LSPs in the list must terminate at the IP address specified in the far end field.</td>
</tr>
<tr>
<td></td>
<td>If the SDP type is GRE, then the following message displays: SDP Delivery Mechanism is not MPLS</td>
</tr>
</tbody>
</table>

Sample Output

*A:ALA-12# show service sdp
==============================================================================
<p>| Services: Service Destination Points |</p>
<table>
<thead>
<tr>
<th>SdpId</th>
<th>Adm MTU</th>
<th>Opr MTU</th>
<th>IP address</th>
<th>Adm Opr</th>
<th>Deliver Signal</th>
</tr>
</thead>
</table>

10  4462  4462  10.20.1.3  Up  Dn  NotReady  MPLS  TLDP
40  4462  1534  10.20.1.20  Up  Up  MPLS  TLDP
60  4462  1514  10.20.1.21  Up  Up  GRE  TLDP
100  4462  4462  180.0.0.2  Down  Down  GRE  TLDP
500  4462  4462  10.20.1.50  Up  Dn  NotReady  GRE  TLDP

Number of SDPs : 5

*A:ALA-12#

*A:ALA-12# show service sdp 2 detail

Service Destination Point (Sdp Id : 2) Details

Description : GRE-10.10.10.104
SDP Id : 2
Admin Path MTU : 0  Oper Path MTU : 0
Far End : 10.10.10.104  Delivery : GRE
Admin State : Up  Oper State : Down
Flags : SignalingSessDown TransportTunnDown
Signaling : TLDP  VLAN VC Etype : 0x8100
Last Status Change : 02/01/2007 09:11:39  Adv. MTU Over. : No
Last Mgmt Change : 02/01/2007 09:11:46

Keep Alive Information :
Admin State : Disabled  Oper State : Disabled
Hello Time : 10  Hello Msg Len : 0
Hello Timeout : 5  Unmatched Replies : 0
Max Drop Count : 3  Hold Down Time : 10
Tx Hello Msgs : 0  Rx Hello Msgs : 0

Associated LSP LIST :
SDP Delivery Mechanism is not MPLS

*A:ALA-12#

*A:ALA-12# show service sdp 8

Service Destination Point (Sdp Id : 8)

SDP Id : 2
Admin Path MTU : 0  Oper Path MTU : 0
Far End : 10.10.10.104  Delivery : MPLS
Admin State : Up  Oper State : Down
Flags : SignalingSessDown TransportTunnDown

Description : MPLS-10.10.10.104
SDP Id : 8
Admin Path MTU : 0  Oper Path MTU : 0
Far End : 10.10.10.104  Delivery : MPLS
Admin State : Up  Oper State : Down
Flags : SignalingSessDown TransportTunnDown
When network domains are configured, the SDP egress interface state can be verified by using the following command:

*A:Dut-T# show service sdp egressifs
SDP Egress Ifs State Table
SDP Id Network Domain State
100 net1 consistent
SDPs: 1
*A:Dut-Tr#

sdp-using

Syntax sdp-using [sdp-id[:vc-id] | far-end ip-address]

Context show>service

Description Display services using SDP or far-end address options.

Parameters

sdp-id — Displays only services bound to the specified SDP ID.

Values 1 — 17407

vc-id — The virtual circuit identifier.

Values 1 — 4294967295

far-end ip-address — Displays only services matching with the specified far-end IP address.

Default Services with any far-end IP address.
**Output**

**Show Service SDP Using** — The following table describes show service sdp-using output fields.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Svc ID</td>
<td>The service identifier.</td>
</tr>
<tr>
<td>Sdp ID</td>
<td>The SDP identifier.</td>
</tr>
<tr>
<td>Type</td>
<td>Type of SDP: spoke or mesh.</td>
</tr>
<tr>
<td>Far End</td>
<td>The far end address of the SDP.</td>
</tr>
<tr>
<td>Oper State</td>
<td>The operational state of the service.</td>
</tr>
<tr>
<td>Ingress Label</td>
<td>The label used by the far-end device to send packets to this device in this service by this SDP.</td>
</tr>
<tr>
<td>Egress Label</td>
<td>The label used by this device to send packets to the far-end device in this service by this SDP.</td>
</tr>
</tbody>
</table>

**Sample Output**

*A:ALA-1# show service sdp-using 300

===============================================================================
Service Destination Point (Sdp Id : 300)
===============================================================================
SvcId       SdpId               Type Far End        Opr State I.Label  E.Label
-------------------------------------------------------------------------------
1           300:1               Mesh 10.0.0.13      Up        131071   131071
2           300:2               Spok 10.0.0.13      Up        131070   131070
100         300:100             Mesh 10.0.0.13      Up        131069   131069
101         300:101             Mesh 10.0.0.13      Up        131068   131068
102         300:102             Mesh 10.0.0.13      Up        131067   131067
-------------------------------------------------------------------------------
Number of SDPs : 5
-------------------------------------------------------------------------------
*A:ALA-1#*

**service-using**

**Syntax**

(service-using)

**Context**

show>service

**Description**

This command displays the services matching certain usage properties.

If no optional parameters are specified, all services defined on the system are displayed.

**Parameters**

-[service] — Displays information for the specified service type.

-b-vpls — Specifies the B-component instance of the Provider Backbone Bridging (PBB/IEEE 802.1ah) feature. It represents the multi-point tunneling component that multiplexes multiple customer VPNs (ISIDs) together. It is similar to a regular VPLS instance that operates on the backbone MAC addresses.
**i-vpls** — Specifies the I-component instance of the Provider Backbone Bridging (PBB/IEEE 802.1ah) feature. It identifies the specific VPN entity associated to a customer multipoint (ELAN) service. It is similar to a regular VPLS instance that operates on the customer MAC addresses.

**m-vpls** — Specifies the M-component (managed VPLS) instance of the Provider Backbone Bridging (PBB/IEEE 802.1ah) feature.

**sdp sdp-id** — Displays only services bound to the specified SDP ID.

- **Default** Services bound to any SDP ID.
- **Values** 1 — 17407

**customer customer-id** — Displays services only associated with the specified customer ID.

- **Default** Services associated with any customer.
- **Values** 1 — 2147483647

### Output

**Show service-using output** — The following table describes the command output fields:

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Id</td>
<td>The service identifier.</td>
</tr>
<tr>
<td>Type</td>
<td>Specifies the service type configured for the service ID.</td>
</tr>
<tr>
<td>Adm</td>
<td>The desired state of the service.</td>
</tr>
<tr>
<td>Opr</td>
<td>The operating state of the service.</td>
</tr>
<tr>
<td>CustomerID</td>
<td>The ID of the customer who owns this service.</td>
</tr>
<tr>
<td>Last Mgmt Change</td>
<td>The date and time of the most recent management-initiated change to this service.</td>
</tr>
</tbody>
</table>

### Sample Output

```
*A:ALA-12# show service service-using customer 10

Services
---
ServiceId  Type     Adm Opr   CustomerId   Last Mgmt Change
-------  --------   ------   -------   ---------------
    1       VPLS     Up Up  10          09/05/2006 13:24:15
   300     Epipe     Up Up  10          09/05/2006 13:24:15

Matching Services :

*A:ALA-12#
```

```
*A:ALA-12# show service service-using

Services
---
ServiceId  Type     Adm Opr   CustomerId   Last Mgmt Change
-------  --------   ------   -------   ---------------

*A:ALA-12#
```
spoke-sdp-fec-using

**Syntax**

```
spoke-sdp-fec-using [spoke-sdp-fec-id] [saii-type2 global-id:prefix:ac-id] [taii-type2 global-id:prefix:ac-id] [path name]
```

**Context**

```
show>service
```

**Description**

Displays the SDPs used by spoke-sdp-fecs at this node.

**Sample Output**

```bash
*A:Dut-C# show service spoke-sdp-fec-using
```

```
Service Spoke-SDP-Fec Information
```

```
SvcId SpokeSdpFec Oper-SdpBind SAII-Type2 TAII-Type2
```

```
Path n/a n/a n/a n/a
```

```
1 1 17407:4294967245 3:10.20.1.3:1 6:10.20.1.6:1
```

```
2 2 17407:4294967247 3:10.20.1.3:2 6:10.20.1.6:2
```

```
3 3 17407:4294967248 3:10.20.1.3:3 6:10.20.1.6:3
```

```
4 4 17407:4294967249 3:10.20.1.3:4 6:10.20.1.6:4
```

```
5 5 17407:4294967250 3:10.20.1.3:5 6:10.20.1.6:5
```

```
6 6 17407:4294967251 3:10.20.1.3:6 6:10.20.1.6:6
```

```
7 7 17407:4294967252 3:10.20.1.3:7 6:10.20.1.6:7
```

```
8 8 17407:4294967253 3:10.20.1.3:8 6:10.20.1.6:8
```

```
9 9 17407:4294967254 3:10.20.1.3:9 6:10.20.1.6:9
```

```
10 10 17407:4294967255 3:10.20.1.3:10 6:10.20.1.6:10
```

```
Enteries found: 10
```

Matching Services : 8

*A:ALA-12#
Show, Clear, Debug Commands

id

Syntax  
\texttt{id service-id \{all | arp | base | endpoint | fdb | interface | labels | sap | sdp | split-horizon-group | stp\}}

Context  
show>service

Description  
This command displays information for a particular service-id.

Parameters  
\texttt{service-id} — The service identification number that identifies the service in the domain.

Values  
\begin{align*}
\text{service-id:} & \quad 1 \ldots 2\text{,}147\text{,}483\text{,}64 \\
\text{svc-name:} & \quad \text{A string up to 64 characters in length.}
\end{align*}

\textbf{all} — Display detailed information about the service.

\textbf{arp} — Display ARP entries for the service.

\textbf{base} — Display basic service information.

\textbf{endpoint} — Display service endpoint information.

\textbf{interface} — Display service interfaces.

\textbf{labels} — Display labels being used by this service.

\textbf{sap} — Display SAPs associated to the service.

\textbf{sdp} — Display SDPs associated with the service.

\textbf{split-horizon-group} — Display split horizon group information.

\textbf{stp} — Display STP information.

Sample Output

\texttt{A:bksim611>config>service>ipipe\# show service id 1009 all}

\begin{verbatim}
Service Detailed Information

Service Id        : 1009                Vpn Id            : 0
Service Type      : Ipipe
Name              : (Not Specified)
Description       : (Not Specified)
Customer Id       : 1
Admin State       : Up                  Oper State        : Up
MTU               : 1500
Vc Switching      : False
SAP Count         : 1                   SDP Bind Count    : 1
CE IPv4 Discovery : Enabled             CE IPv6 Discovery : Enabled

Service Destination Points(SDPs)

Sdp Id 5:1009 -(5.5.5.5)

Description     : (Not Specified)
SDP Id             : 5:1009                   Type              : Spoke
Spoke Descr     : (Not Specified)
\end{verbatim}
VLL Show Commands

Split Horiz Grp : (Not Specified)
VC Type : Ipipe
Admin Path MTU : 0
Far End : 5.5.5.5
Tunnel Far End : n/a
Hash Label : Disabled

Admin State : Up
Acct. Pol : None
Ingress Label : 131048
Ingr Mac Fltr-Id : n/a
Ingr IP Fltr-Id : n/a
Ingr IPv6 Fltr-Id : n/a
Admin ControlWord : Not Preferred
Admin BW(Kbps) : 0
Last Status Change : 09/15/2010 13:06:46
Endpoint : N/A

Oper State : Up
Collect Stats : Disabled
Egress Label : 131053
Egr Mac Fltr-Id : n/a
Egr IP Fltr-Id : n/a
Egr IPv6 Fltr-Id : n/a
Oper ControlWord : False
Oper BW(Kbps) : 0
Last Mgmt Change : 09/15/2010 13:06:02
Precedence : 4

Delivery : MPLS
Tunnel Far End : n/a
Hash Label : Disabled
Admin State : Up
Acct. Pol : None
Ingress Label : 131048
Ingr Mac Fltr-Id : n/a
Ingr IP Fltr-Id : n/a
Ingr IPv6 Fltr-Id : n/a
Admin ControlWord : Not Preferred
Admin BW(Kbps) : 0
Last Status Change : 09/15/2010 13:06:46
Endpoint : N/A

Oper State : Up
Collect Stats : Disabled
Egress Label : 131053
Egr Mac Fltr-Id : n/a
Egr IP Fltr-Id : n/a
Egr IPv6 Fltr-Id : n/a
Oper ControlWord : False
Oper BW(Kbps) : 0
Last Mgmt Change : 09/15/2010 13:06:02
Precedence : 4

KeepAlive Information :
Admin State : Disabled
Hello Time : 10
Max Drop Count : 3

Oper State : Disabled
Hello Msg Len : 0
Hold Down Time : 10

Statistics :
I. Fwd. Pkts. : 15
I. Fwd. Octs. : 1460
E. Fwd. Pkts. : 17
E. Fwd. Octets : 1604

RSVP/Static LSPs
Associated LSP LIST :
Lsp Name : to-bksim180-1
Admin State : Up
Oper State : Up
Time Since Last Tr*: 16h07m44s

Lsp Name : to-bksim180-2
Admin State : Up
Oper State : Up
Time Since Last Tr*: 16h07m45s

Class-based forwarding :
Class forwarding : Enabled
EnforceDSTELspFc : Disabled
Default LSP : to-bksim180-1
Multicast LSP : None

FC Mapping Table
FC Name LSP Name
ef to-bksim180-2
### IPIPE Service Destination Point specifics

<table>
<thead>
<tr>
<th>Configured CE IP Addr</th>
<th>Peer CE IP Addr</th>
</tr>
</thead>
<tbody>
<tr>
<td>n/a</td>
<td>0.0.0.0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Peer IPV6 Capability</th>
<th>Peer IPv6 LL Addr</th>
<th>Peer IPv6 Global Addr</th>
</tr>
</thead>
</table>

Number of SDPs: 1

### Service Access Points

<table>
<thead>
<tr>
<th>SAP 1/7/3:1009</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Service Id</th>
<th>SAP</th>
<th>Encap</th>
</tr>
</thead>
<tbody>
<tr>
<td>1009</td>
<td>1/7:3:1009</td>
<td>q-tag</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Description</th>
<th>Admin State</th>
<th>Oper State</th>
<th>Flags</th>
<th>Multi Svc Site</th>
<th>Last Status Change</th>
<th>Last Mgmt Change</th>
<th>Sub Type</th>
<th>Dot1Q Ethertype</th>
<th>QinQ Ethertype</th>
<th>Split Horizon Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Not Specified)</td>
<td>Up</td>
<td>Up</td>
<td>None</td>
<td>None</td>
<td>09/15/2010 13:06:21</td>
<td>09/15/2010 13:06:02</td>
<td>regular</td>
<td>0x8100</td>
<td>0x8100</td>
<td>(Not Specified)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Admin MTU</th>
<th>Oper MTU</th>
</tr>
</thead>
<tbody>
<tr>
<td>1518</td>
<td>1518</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Ingr IP Fltr-Id</th>
<th>Egr IP Fltr-Id</th>
</tr>
</thead>
<tbody>
<tr>
<td>n/a</td>
<td>n/a</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Ingr Mac Fltr-Id</th>
<th>Egr Mac Fltr-Id</th>
</tr>
</thead>
<tbody>
<tr>
<td>n/a</td>
<td>n/a</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Ingr IPv6 Fltr-Id</th>
<th>Egr IPv6 Fltr-Id</th>
<th>qinq-pbit-marking</th>
<th>Egr Agg Rate Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>n/a</td>
<td>n/a</td>
<td>both</td>
<td>max</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Ingr Agg Rate Limit</th>
<th>Egr Agg Rate Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>max</td>
<td>max</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Endpoint</th>
<th>Q Frame-Based Acct</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Acct. Pol</th>
<th>Collect Stats</th>
<th>Oper Group</th>
<th>Monitor Oper Grp</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>Disabled</td>
<td>(none)</td>
<td>(none)</td>
</tr>
</tbody>
</table>

### ETH-CFM SAP specifics

<table>
<thead>
<tr>
<th>Tunnel Faults</th>
<th>CPM Hold-Timer</th>
</tr>
</thead>
<tbody>
<tr>
<td>n/a</td>
<td>n/a</td>
</tr>
</tbody>
</table>

Ipipe SAP Configuration Information

<table>
<thead>
<tr>
<th>Configured CE IP</th>
<th>Discovered CE IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>n/a</td>
<td>209.1.1.1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SAP MAC Address</th>
<th>Mac Refresh Inter*</th>
</tr>
</thead>
<tbody>
<tr>
<td>ac:55:01:07:00:03</td>
<td>14400</td>
</tr>
</tbody>
</table>

Ipipe SAP IPV4 ARP Entry Info

<table>
<thead>
<tr>
<th>209.1.1.1</th>
<th>00:11:22:33:44:55 dynamic</th>
</tr>
</thead>
</table>
Ipipes SAP IPv6 Neighbor Entry Info


QOS

Ingress qos-policy : 1  Egress qos-policy : 1
Shared Q policy : n/a  Multipoint shared : Disabled
I. Sched Pol : (Not Specified)  E. Sched Pol : (Not Specified)
I. Policer Ctl Pol : (Not Specified)  E. Policer Ctl Pol : (Not Specified)

Sap Statistics

Last Cleared Time : N/A

Packets  Octets
Forwarding Engine Stats
Dropped : 2 172
Off. HiPrio : 0 0
Off. LowPrio : 17 1978
Off. Uncolor : 0 0

Queueing Stats(Ingress QoS Policy 1)
Dro. HiPrio : 0 0
Dro. LowPrio : 0 0
For. InProf : 0 0
For. OutProf : 17 1978

Queueing Stats(Egress QoS Policy 1)
Dro. InProf : 0 0
Dro. OutProf : 0 0
For. InProf : 0 0
For. OutProf : 15 1790

Sap per Queue stats

Ingress Queue 1 (Unicast) (Priority)
Off. HiPrio : 0 0
Off. LoPrio : 17 1978
Dro. HiPrio : 0 0
Dro. LoPrio : 0 0
For. InProf : 0 0
For. OutProf : 17 1978

Egress Queue 1
For. InProf : 0 0
For. OutProf : 15 1790
Dro. InProf : 0 0
Dro. OutProf : 0 0

Service Endpoints
No Endpoints found.
VPLS Sites

<table>
<thead>
<tr>
<th>Site</th>
<th>Site-Id</th>
<th>Dest</th>
<th>Mesh-SDP</th>
<th>Admin</th>
<th>Oper</th>
<th>Fwdr</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No Matching Entries</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

show service id x all

SAP 1/1/4:500

<table>
<thead>
<tr>
<th>Service Id</th>
<th>: 500</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAF</td>
<td>: 1/1/4:500</td>
</tr>
<tr>
<td>Encap</td>
<td>: q-tag</td>
</tr>
<tr>
<td>Description</td>
<td>: (Not Specified)</td>
</tr>
<tr>
<td>Admin State</td>
<td>: Up</td>
</tr>
<tr>
<td>Oper State</td>
<td>: Down</td>
</tr>
<tr>
<td>Flags</td>
<td>: PortOperDown</td>
</tr>
<tr>
<td>Multi Svc Site</td>
<td>: None</td>
</tr>
<tr>
<td>Last Status Change</td>
<td>: 09/19/2013 11:43:04</td>
</tr>
<tr>
<td>Last Mgmt Change</td>
<td>: 09/19/2013 11:43:05</td>
</tr>
<tr>
<td>Sub Type</td>
<td>: regular</td>
</tr>
<tr>
<td>Dot1Q Ethertype</td>
<td>: 0x8100</td>
</tr>
<tr>
<td>QinQ Ethertype</td>
<td>: 0x8100</td>
</tr>
<tr>
<td>Split Horizon Group</td>
<td>: (Not Specified)</td>
</tr>
<tr>
<td>Admin MTU</td>
<td>: 1518</td>
</tr>
<tr>
<td>Oper MTU</td>
<td>: 1518</td>
</tr>
<tr>
<td>Ingr IP Fltr-Id</td>
<td>: n/a</td>
</tr>
<tr>
<td>Egr IP Fltr-Id</td>
<td>: n/a</td>
</tr>
<tr>
<td>Ingr Mac Fltr-Id</td>
<td>: n/a</td>
</tr>
<tr>
<td>Egr Mac Fltr-Id</td>
<td>: n/a</td>
</tr>
<tr>
<td>Ingr IPv6 Fltr-Id</td>
<td>: n/a</td>
</tr>
<tr>
<td>Egr IPv6 Fltr-Id</td>
<td>: n/a</td>
</tr>
<tr>
<td>tod-suite</td>
<td>: None</td>
</tr>
<tr>
<td>qinq-pbit-marking</td>
<td>: both</td>
</tr>
<tr>
<td>Egr Agg Rate Limit</td>
<td>: max</td>
</tr>
<tr>
<td>Endpoint</td>
<td>: N/A</td>
</tr>
<tr>
<td>Q Frame-Based Acct</td>
<td>: Disabled</td>
</tr>
<tr>
<td>Vlan-translation</td>
<td>: None</td>
</tr>
<tr>
<td>Acct. Pol</td>
<td>: None</td>
</tr>
<tr>
<td>Collect Stats</td>
<td>: Disabled</td>
</tr>
<tr>
<td>Application Profile</td>
<td>: None</td>
</tr>
<tr>
<td>Transit Policy</td>
<td>: None</td>
</tr>
<tr>
<td>Oper Group</td>
<td>: (none)</td>
</tr>
<tr>
<td>Monitor Oper Grp</td>
<td>: (none)</td>
</tr>
<tr>
<td>Host Lockout Plcy</td>
<td>: n/a</td>
</tr>
<tr>
<td>Ignore Oper Down</td>
<td>: Disabled</td>
</tr>
<tr>
<td>Lag Link Map Prof</td>
<td>: (none)</td>
</tr>
<tr>
<td>Cflowd</td>
<td>: Disabled</td>
</tr>
</tbody>
</table>

ETH-CFM SAP specifics

| Tunnel Faults | : n/a |
| AIS | : Disabled |
| MC Prop-Hold-Timer | : n/a |
| Squelch Levels | : 0 1 2 3 4 5 6 7 |

QOS

Ingress qos-policy : 1
Egress qos-policy : 1
.
.
.

Service Destination Points(SDPs)
### VLL Show Commands

**Sdp Id 1:2 {1.1.1.1}**

<table>
<thead>
<tr>
<th>Description : (Not Specified)</th>
<th>SDP Id : 1:2</th>
<th>Type : Spoke</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spoke Descr : (Not Specified)</td>
<td>Split Horiz Grp : (Not Specified)</td>
<td></td>
</tr>
<tr>
<td>VC Type : Ether</td>
<td>VC Tag : n/a</td>
<td></td>
</tr>
<tr>
<td>Admin Path MTU : 0</td>
<td>Oper Path MTU : 0</td>
<td></td>
</tr>
<tr>
<td>Delivery : GRE</td>
<td>Far End : 1.1.1.1</td>
<td></td>
</tr>
<tr>
<td>Tunnel Far End : n/a</td>
<td>LSP Types : n/a</td>
<td></td>
</tr>
<tr>
<td>Hash Label : Disabled</td>
<td>Hash Lbl Sig Cap : Disabled</td>
<td></td>
</tr>
<tr>
<td>Oper Hash Label : Disabled</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Admin State : Up</th>
<th>Oper State : Down</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acct. Pol : None</td>
<td>Collect Stats : Disabled</td>
</tr>
<tr>
<td>Ingr Mac Fltr-Id : n/a</td>
<td>Egr Mac Fltr-Id : n/a</td>
</tr>
<tr>
<td>Ingr IP Fltr-Id : n/a</td>
<td>Egr IP Fltr-Id : n/a</td>
</tr>
<tr>
<td>Ingr IPv6 Fltr-Id : n/a</td>
<td>Egr IPv6 Fltr-Id : n/a</td>
</tr>
<tr>
<td>Admin ControlWord : Not Preferred</td>
<td>Oper ControlWord : False</td>
</tr>
<tr>
<td>Last Status Change : 09/11/2013 20:02:40</td>
<td>Signaling : TLDP</td>
</tr>
<tr>
<td>Last Mgmt Change : 09/15/2013 13:56:56</td>
<td>Force Vlan-Vc : Disabled</td>
</tr>
<tr>
<td>Endpoint : N/A</td>
<td>Precedence : 4</td>
</tr>
<tr>
<td>FW Status Sig : Enabled</td>
<td></td>
</tr>
<tr>
<td>Class Fwding State : Down</td>
<td></td>
</tr>
</tbody>
</table>

| Flags : SdpOperDown NoIngVCLabel NoEgrVCLabel PathMTUTooSmall |

<table>
<thead>
<tr>
<th>Time to RetryReset : never</th>
<th>Retries Left : 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mac Move : Blockable</td>
<td>Blockable Level : Tertiary</td>
</tr>
<tr>
<td>Local Fw Bits : None</td>
<td></td>
</tr>
<tr>
<td>Peer Fw Bits : None</td>
<td></td>
</tr>
<tr>
<td>Peer Fault Ip : None</td>
<td></td>
</tr>
<tr>
<td>Peer Vccv CV Bits : None</td>
<td></td>
</tr>
<tr>
<td>Peer Vccv CC Bits : None</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Application Profile: None</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Transit Policy : None</td>
<td></td>
</tr>
<tr>
<td>Max Nbr of MAC Addr : No Limit</td>
<td>Total MAC Addr : 0</td>
</tr>
<tr>
<td>Learned MAC Addr : 0</td>
<td>Static MAC Addr : 0</td>
</tr>
<tr>
<td>OAM MAC Addr : 0</td>
<td>DHCP MAC Addr : 0</td>
</tr>
<tr>
<td>Host MAC Addr : 0</td>
<td>Intf MAC Addr : 0</td>
</tr>
<tr>
<td>SFB MAC Addr : 0</td>
<td>Cond MAC Addr : 0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>MAC Learning : Enabled</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Aging : Enabled</td>
<td></td>
</tr>
<tr>
<td>BPDU Translation : Disabled</td>
<td></td>
</tr>
<tr>
<td>L2PT Termination : Disabled</td>
<td></td>
</tr>
<tr>
<td>MAC Pinning : Disabled</td>
<td></td>
</tr>
<tr>
<td>Ignore Standby Sig : False</td>
<td>Block On Mesh Fail : False</td>
</tr>
<tr>
<td>Oper Group : (none)</td>
<td>Monitor Oper Grp : (none)</td>
</tr>
<tr>
<td>Rest Prot Src Mac : Disabled</td>
<td></td>
</tr>
<tr>
<td>Auto Learn Mac Prot : Disabled</td>
<td>RestProtSrcMacAct : Disable</td>
</tr>
<tr>
<td>Ingress Qos Policy : (none)</td>
<td>Egress Qos Policy : (none)</td>
</tr>
<tr>
<td>Ingress FP QGrp : (none)</td>
<td>Egress Port QGrp : (none)</td>
</tr>
<tr>
<td>Ing FP QGrp Inst : (none)</td>
<td>Egr Port QGrp Inst : (none)</td>
</tr>
</tbody>
</table>
authentication

**Syntax**
authentication

**Context**
show>service>id

**Description**
This command enables the context to display subscriber authentication information.

statistics

**Syntax**
statistics [policy name] [sap sap-id]

**Context**
show>service>id>authentication

**Description**
This command displays session authentication statistics for this service.

**Parameters**
policy name — Specifies the subscriber authentication policy statistics to display.
sap sap-id — Specifies the SAP ID statistics to display. See Common CLI Command Descriptions on page 1783 for command syntax.

**Sample Output**

```
*A:ALA-1# show service id 11 authentication statistics
=================================================================================================
Authentication statistics
=================================================================================================
<table>
<thead>
<tr>
<th>Interface / SAP</th>
<th>Authentication Successful</th>
<th>Authentication Failed</th>
</tr>
</thead>
<tbody>
<tr>
<td>vpls-11-90.1.0.254</td>
<td>1582</td>
<td>3</td>
</tr>
</tbody>
</table>

Number of entries: 1
```

*A:ALA-1#*
all

Syntax: `all`

Context: `show>service>id`

Description: This command displays detailed information for all aspects of the service.

Output: **Show service ID Output** — The following table describes the output fields when the `all` option is specified:

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Id</td>
<td>The service identifier.</td>
</tr>
<tr>
<td>VPN Id</td>
<td>The number which identifies the VPN.</td>
</tr>
<tr>
<td>Service Type</td>
<td>Specifies the type of service.</td>
</tr>
<tr>
<td>VLL Type</td>
<td>Specifies the VLL type.</td>
</tr>
<tr>
<td>Description</td>
<td>Generic information about the service.</td>
</tr>
<tr>
<td>Customer Id</td>
<td>The customer identifier.</td>
</tr>
<tr>
<td>Last Mgmt Change</td>
<td>The date and time of the most recent management-initiated change.</td>
</tr>
<tr>
<td>Flags</td>
<td>Specifies the conditions that affect the operating status of this SAP. Display output includes: ServiceAdminDown, SapAdminDown, InterfaceAdminDown, PortOperDown, L2OperDown, RelearnLimitExceeded, RxProtSrcMac, ParentIfAdminDown, NoSapIpipeCeIpAddr, TodResourceUnavail, TodMssResourceUnavail, SapParamMismatch, CemSapNoEcidOrMacAddr, StandByForMcRing, SapIngressNamedPoolMismatch, SapEgressNamedPoolMismatch, NoSapEpipeRingNode.</td>
</tr>
<tr>
<td>SAP Count</td>
<td>The number of SAPs specified for this service.</td>
</tr>
</tbody>
</table>

Sample Output
Show, Clear, Debug Commands

**base**

**Syntax**

```
base
```

**Context**

```
show>service>id
```

**Description**

Displays basic information about the service ID including service type, description, SAPs.

**Output**

**Show Service-ID Base** — The following table describes show service-id base output fields:

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Id</td>
<td>The service identifier.</td>
</tr>
<tr>
<td>Vpn Id</td>
<td>Specifies the VPN ID assigned to the service.</td>
</tr>
<tr>
<td>Service Type</td>
<td>The type of service: Epipe, Ipipe, VPLS, IES, VPRN.</td>
</tr>
<tr>
<td>Description</td>
<td>Generic information about the service.</td>
</tr>
<tr>
<td>Customer Id</td>
<td>The customer identifier.</td>
</tr>
<tr>
<td>Last Mgmt Change</td>
<td>The date and time of the most recent management-initiated change to this customer.</td>
</tr>
<tr>
<td>Adm</td>
<td>The desired state of the service.</td>
</tr>
<tr>
<td>Oper</td>
<td>The operating state of the service.</td>
</tr>
<tr>
<td>Mtu</td>
<td>The largest frame size (in octets) that the service can handle.</td>
</tr>
<tr>
<td>Def. Mesh VC Id</td>
<td>This object is only valid in services that accept mesh SDP bindings. It is used to validate the VC ID portion of each mesh SDP binding defined in the service.</td>
</tr>
<tr>
<td>SAP Count</td>
<td>The number of SAPs defined on the service.</td>
</tr>
<tr>
<td>SDP Bind Count</td>
<td>The number of SDPs bound to the service.</td>
</tr>
<tr>
<td>Identifier</td>
<td>Specifies the service access (SAP) and destination (SDP) points.</td>
</tr>
<tr>
<td>Type</td>
<td>Specifies the signaling protocol used to obtain the ingress and egress labels used in frames transmitted and received on the SDP.</td>
</tr>
<tr>
<td>AdmMTU</td>
<td>Specifies the desired largest service frame size (in octets) that can be transmitted through this SDP to the far-end ESR, without requiring the packet to be fragmented.</td>
</tr>
<tr>
<td>PBB Tunnel Point</td>
<td>Specifies the endpoint in the B-VPLS environment where the Epipe terminates.</td>
</tr>
<tr>
<td>Admin MTU</td>
<td>Specifies the B-VPLS admin MTU.</td>
</tr>
<tr>
<td>Backbone-Flooding</td>
<td>Specifies whether or not the traffic is flooded in the B-VPLS for the destination instead of unicast. If the backbone destination MAC is in the B-VPLS FDB, then it will be unicast.</td>
</tr>
</tbody>
</table>
Sample Output

```
*A:ALA-48>config>service>epipe>sap# show service id 6 base

Service Basic Information

<table>
<thead>
<tr>
<th>Service Id</th>
<th>6</th>
<th>Vpn Id</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Type</td>
<td>Epipe</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td>Distributed Epipe service to east coast</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Customer Id</td>
<td>6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Last Status Change</td>
<td>02/02/2009 09:27:55</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Last Mgmt Change</td>
<td>02/02/2009 09:27:57</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Admin State</td>
<td>Up</td>
<td>Oper State</td>
<td>Down</td>
</tr>
<tr>
<td>MTU</td>
<td>1514</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vc Switching</td>
<td>False</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SAP Count</td>
<td>1</td>
<td>SDP Bind Count</td>
<td>1</td>
</tr>
</tbody>
</table>

Service Access & Destination Points

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Type</th>
<th>AdmMTU</th>
<th>OprMTU</th>
<th>Adm</th>
<th>Opr</th>
</tr>
</thead>
<tbody>
<tr>
<td>sap:1/2/9:0</td>
<td>q-tag</td>
<td>1518</td>
<td>1518</td>
<td>Up</td>
<td>Down</td>
</tr>
<tr>
<td>sdp:2:6 S(10.10.10.104)</td>
<td>n/a</td>
<td>0</td>
<td>0</td>
<td>Up</td>
<td>Down</td>
</tr>
</tbody>
</table>
```

bgp-vpws

**Syntax**

```
bgp-vpws
```

**Context**

```
show>service>id
```

**Description**

This command displays BGP VPWS related information for the service.

**Sample Output**

```
*A:cses-E11>config>service>epipe>bgp-vpws# show service id 2 bgp-vpws

BGP VPWS Information

<table>
<thead>
<tr>
<th>Admin State</th>
<th>Enabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>VE Name</td>
<td>PE1</td>
</tr>
<tr>
<td>PW Template</td>
<td>2</td>
</tr>
<tr>
<td>Route Dist</td>
<td>65536:3</td>
</tr>
<tr>
<td>Rte-Target Import</td>
<td>65536:2</td>
</tr>
<tr>
<td>PW-Template Id</td>
<td>2</td>
</tr>
<tr>
<td>Import Rte-Tgt</td>
<td>None</td>
</tr>
</tbody>
</table>
```

**Label**

<table>
<thead>
<tr>
<th>Label</th>
<th>Description (Continued)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISID</td>
<td>The 24 bit field carrying the service instance identifier associated with the frame. It is used at the destination PE as a demultiplexor field.</td>
</tr>
</tbody>
</table>
Show, Clear, Debug Commands

Remote-Ve Information
-----------------------------------------------
Remote VE Name       : PE2               Remote VE Id     : 2
-----------------------------------------------
*A:cses-E11>config>service>epipe>bgp-vpws#

endpoint

Syntax    endpoint [endpoint-name]
Context    show>service>id
Description This command displays service endpoint information.
Parameters  endpoint-name — Specifies the name of an existing endpoint for the service.

Sample Output

*A:ALA-48>config>service>epipe# show service id 6 endpoint
-----------------------------------------------
Service 6 endpoints
-----------------------------------------------
Endpoint name      : x
Revert time        : 0
Act Hold Delay     : 0
Tx Active          : none
-----------------------------------------------
Members
No members found.
-----------------------------------------------
Endpoint name      : y
Revert time        : 0
Act Hold Delay     : 0
Tx Active          : none
-----------------------------------------------
Members
No members found.
-----------------------------------------------
*A:ALA-48>config>service>epipe#

labels

Syntax    labels
Context    show>service>id
Description Displays the labels being used by the service.
**Output**  
Show Service-ID Labels — The following table describes show service-id labels output fields:

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Svc Id</td>
<td>The service identifier.</td>
</tr>
<tr>
<td>Sdp Id</td>
<td>The SDP identifier.</td>
</tr>
<tr>
<td>Type</td>
<td>Indicates whether the SDP is a spoke or a mesh.</td>
</tr>
<tr>
<td>I. Lbl</td>
<td>The VC label used by the far-end device to send packets to this device in this service by the SDP.</td>
</tr>
<tr>
<td>E. Lbl</td>
<td>The VC label used by this device to send packets to the far-end device in this service by the SDP.</td>
</tr>
</tbody>
</table>

**Sample Output**

```
*A:ALA-12# show service id 1 labels
==============================================================================
Martini Service Labels
==============================================================================
Svc Id    Sdp Id     Type ILbl     ELbl
------------------------------------------------------------------------------
1         10:1       Mesh 0      0
1         20:1       Mesh 0      0
1         30:1       Mesh 0      0
1         40:1       Mesh 130081 131061
1         60:1       Mesh 131019 131016
1         100:1      Mesh 0      0
------------------------------------------------------------------------------
Number of Bound SDPs : 6
------------------------------------------------------------------------------
*A:ALA-12#```

7950 SR OS Services Guide
**sap**

**Syntax**

```
sap sap-id [detail]
```

**Context**

```
show>service>id
```

**Description**

This command displays information for the SAPs associated with the service. If no optional parameters are specified, a summary of all associated SAPs is displayed.

**Parameters**

- `sap-id` — The ID that displays SAPs for the service in the form `slot/mda/port`. See Common CLI Command Descriptions on page 1783 for command syntax.
- `interface interface-name` — Displays information for the specified IP interface.
- `ip-address ip-address` — Displays information associated with the specified IP address.
- `detail` — Displays detailed information.
- `detail` — Displays detailed information for the SAP.

**Output**

**Show Service-ID SAP** — The following table describes show service SAP fields:

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Id</td>
<td>The service identifier.</td>
</tr>
<tr>
<td>SAP</td>
<td>The SAP and qtag.</td>
</tr>
<tr>
<td>Encap</td>
<td>The encapsulation type of the SAP.</td>
</tr>
<tr>
<td>Ethertype</td>
<td>Specifies an Ethernet type II Ethertype value.</td>
</tr>
<tr>
<td>Admin State</td>
<td>The administrative state of the SAP.</td>
</tr>
<tr>
<td>Oper State</td>
<td>The operating state of the SAP.</td>
</tr>
<tr>
<td>Flags</td>
<td>Specifies the conditions that affect the operating status of this SAP.</td>
</tr>
<tr>
<td></td>
<td>Display output includes: ServiceAdminDown, SapAdminDown,</td>
</tr>
<tr>
<td></td>
<td>InterfaceAdminDown, PortOperDown, PortMTUTooSmall,</td>
</tr>
<tr>
<td></td>
<td>L2OperDown, SapEgressQoSMismatch, RelearnLimitExceeded,</td>
</tr>
<tr>
<td></td>
<td>RxProtSrcMac, ParentIfAdminDown, NoSapIpipeCelpAddr, TodResourceUnavail,</td>
</tr>
<tr>
<td></td>
<td>TodMssResourceUnavail, SapParamMismatch, ServiceMTUTooSmall, SapIngressNamedPoolMismatch,</td>
</tr>
<tr>
<td></td>
<td>SapEgressNamedPoolMismatch, NoSapEpipeRingNode.</td>
</tr>
<tr>
<td>Last Status Change</td>
<td>The time of the most recent operating status change to this SAP.</td>
</tr>
<tr>
<td>Last Mgmt Change</td>
<td>The time of the most recent management-initiated change to this SAP.</td>
</tr>
<tr>
<td>Admin MTU</td>
<td>The desired largest service frame size (in octets) that can be transmitted</td>
</tr>
<tr>
<td>Oper MTU</td>
<td>The actual largest service frame size (in octets) that can be transmitted</td>
</tr>
</tbody>
</table>
### Sample Output

```
*B: Dut-A# show service id 10 sap 2/1/4:cp.10
========================================================================
Service Access Points (SAP)
========================================================================
Service Id         : 10
SAP                : 2/1/4:cp.10              Encap             : atm
Description        : Default sap description for service id 10
Admin State        : Up                       Oper State        : Up
Flags              : None
Multi Svc Site     : None
Last Status Change : 11/01/2010 11:33:16
Last Mgmt Change   : 11/01/2010 13:46:15
========================================================================
```

```
A:SR12# configure service apipe 1 sap
- no sap <sap-id>
- sap <sap-id> [create] [no-endpoint]
- sap <sap-id> [create] endpoint <endpoint-name>

<sap-id>             : null           - <port-id|bundle-id|bpgrp-id|lag-id|
aps-id>
...
  atm            - <port-id|aps-id>[vpi/vci|vpi|vpi1.vpi2]  
...
  ima-grp        - <bundle-id>[vpi/vci|vpi|vpi1.vpi2]

A:ALA-48>config>service>epipe# show service id 8 sap 881/1/2:4094
========================================================================
Service Access Points (SAP)
========================================================================
Service Id         : 8
Admin State        : Up                       Oper State        : Down
Flags              : ServiceAdminDown
Collect Stats      : ServiceAdminDown
Ingress qos-policy : The ingress QoS policy ID assigned to the SAP.
Ingress Filter-Id  : The ingress filter policy ID assigned to the SAP.
Egress qos-policy  : The egress QoS policy ID assigned to the SAP.
Egress Filter-Id   : The egress filter policy ID assigned to the SAP.
Acct. Pol          : The accounting policy ID assigned to the SAP.
Collect Stats      : Specifies whether collect stats is enabled.
LLF Admin State    : Displays the Link Loss Forwarding administrative state.
LLF Oper State     : Displays the Link Loss Forwarding operational state.
pw-port            : pw-id[drag1[.qtag2]]  pw-id[drag1[.qtag2]]  pw-2:1.1
```

### Ingress qos-policy
- The ingress QoS policy ID assigned to the SAP.

### Egress qos-policy
- The egress QoS policy ID assigned to the SAP.

### Ingress Filter-Id
- The ingress filter policy ID assigned to the SAP.

### Egress Filter-Id
- The egress filter policy ID assigned to the SAP.

### Acct. Pol
- The accounting policy ID assigned to the SAP.

### Collect Stats
- Specifies whether collect stats is enabled.

### LLF Admin State
- Displays the Link Loss Forwarding administrative state.

### LLF Oper State
- Displays the Link Loss Forwarding operational state.

### pw-port
- pw-id[drag1[.qtag2]]  pw-id[drag1[.qtag2]]  pw-2:1.1
Show, Clear, Debug Commands

Last Status Change : 02/06/2007 12:01:14
Last Mgmt Change : 02/06/2007 12:01:17
Admin MTU : 1522 Oper MTU : 1522
Ingress qos-policy : 1 Egress qos-policy : 1
Shared Q plcy : n/a Multipoint shared : Disabled
Ingress Filter-Id : n/a Egress Filter-Id : n/a
tod-suite : None

Multi Svc Site : None
Acct. Pol : None
Collect Stats : Disabled

A:ALA-48>config>service>epipe#
A:ALA-48>config>service>epipe# show service id 8 sap 881/1/2:4094 detail

Service Access Points(SAP)

Service Id : 8
Admin State : Up Oper State : Down
Flags : ServiceAdminDown PortOperDown

Last Status Change : 02/06/2007 12:01:14
Last Mgmt Change : 02/06/2007 12:01:17
Admin MTU : 1522 Oper MTU : 1522
Ingress qos-policy : 1 Egress qos-policy : 1
Shared Q plcy : n/a Multipoint shared : Disabled
Ingress Filter-Id : n/a Egress Filter-Id : n/a
tod-suite : None

Multi Svc Site : None
Acct. Pol : None
Collect Stats : Disabled

Sap Statistics

Packets Octets
Forwarding Engine Stats
Dropped : 0
Off. HiPrio : 0
Off. LoPrio : 0
Off. Uncolor : 0

Queueing Stats(Ingress QoS Policy 1)
Dro. HiPrio : 0
Dro. LoPrio : 0
For. InProf : 0
For. OutProf : 0

Queueing Stats(Egress QoS Policy 1)
Dro. InProf : 0
Dro. OutProf : 0
For. InProf : 0
For. OutProf : 0

Sap per Queue stats

Ingress Queue 1 (Unicast) (Priority)
Packets Octets
Off. HiPrio : 0
Off. LoPrio : 0
Dro. HiPrio : 0
Dro. LoPrio : 0
For. InProf : 0
For. OutProf : 0
Egress Queue 1

---

Page 1560  7950 SR  OS Services Guide
If a TOD Suite is configured on a SAP, the name of the suite is shown in the show command output. The values of the policies may be different from those configured on the SAP, because the configured policy assignments may have been overruled by policy assignments of the TOD Suite.

**Sample Output**

```
A:ALA-48# show service id 1 sap 1/1/1:2
```

```
Service Access Points(SAP)

<table>
<thead>
<tr>
<th>Service Id</th>
<th>SAP</th>
<th>Encap</th>
<th>Dot1Q Ethertype</th>
<th>QinQ Ethertype</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1/1/1:5</td>
<td>q-tag</td>
<td>0x8100</td>
<td>0x8100</td>
</tr>
</tbody>
</table>

Flags: None

```

```
A:ALA-48# show service id 1 sap 1/1/1:6
```

```
Service Access Points(SAP)

<table>
<thead>
<tr>
<th>Service Id</th>
<th>SAP</th>
<th>Encap</th>
<th>Dot1Q Ethertype</th>
<th>QinQ Ethertype</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1/1/1:6</td>
<td>q-tag</td>
<td>0x8100</td>
<td>0x8100</td>
</tr>
</tbody>
</table>

Flags: TodResourceUnavail

Last Status Change: 12/01/2006 09:59:42
Last Mgmt Change: 12/01/2006 09:59:45
...
sdp

Syntax  
```
  sdp [sdp-id:vc-id] [far-end ip-address] [detail]
sdp sdp-id:vc-id mrp
```

Context  
`show>service>`

Description  
This command displays information for the SDPs associated with the service. If no optional parameters are specified, a summary of all associated SDPs is displayed.

Parameters  
- **sdp-id** — Displays only information for the specified SDP ID.
  - Default: All SDPs.
  - Values: `1 — 17407`
- **far-end ip-address** — Displays only SDPs matching the specified far-end IP address.
  - Default: SDPs with any far-end IP address.
- **detail** — Displays detailed SDP information.

Output  
**Show Service-ID SDP** — The following table describes show service-id SDP output fields.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sdp Id</td>
<td>The SDP identifier.</td>
</tr>
<tr>
<td>Type</td>
<td>Indicates whether the SDP is a spoke or a mesh.</td>
</tr>
<tr>
<td>Split Horizon Group</td>
<td>Name of the split horizon group that the SDP belongs to.</td>
</tr>
<tr>
<td>VC Type</td>
<td>The VC type, ether, vlan, or vpls.</td>
</tr>
<tr>
<td>VC Tag</td>
<td>The explicit dot1Q value used when encapsulating to the SDP far end.</td>
</tr>
<tr>
<td>I. Lbl</td>
<td>The VC label used by the far-end device to send packets to this device in this service by the SDP.</td>
</tr>
<tr>
<td>Admin Path MTU</td>
<td>The operating path MTU of the SDP is equal to the admin path MTU (when one is set) or the dynamically computed tunnel MTU, when no admin path MTU is set (the default case).</td>
</tr>
<tr>
<td>Oper Path MTU</td>
<td>The actual largest service frame size (in octets) that can be transmitted through this SDP to the far-end router, without requiring the packet to be fragmented.</td>
</tr>
<tr>
<td>Far End</td>
<td>Specifies the IP address of the remote end of the GRE or MPLS tunnel defined by this SDP.</td>
</tr>
<tr>
<td>Delivery</td>
<td>Specifies the type of delivery used by the SDP: GRE or MPLS.</td>
</tr>
<tr>
<td>Admin State</td>
<td>The administrative state of this SDP.</td>
</tr>
<tr>
<td>Oper State</td>
<td>The current state of this SDP.</td>
</tr>
</tbody>
</table>
### Sample Output

A:Dut-A# show service id 1 sdp detail

<table>
<thead>
<tr>
<th>Description</th>
<th>Label</th>
<th>Description (Continued)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ingress Label</td>
<td>The label used by the far-end device to send packets to this device in this service by this SDP.</td>
<td></td>
</tr>
<tr>
<td>Egress Label</td>
<td>The label used by this device to send packets to the far-end device in this service by the SDP.</td>
<td></td>
</tr>
<tr>
<td>Last Changed</td>
<td>The date and time of the most recent change to the SDP.</td>
<td></td>
</tr>
<tr>
<td>Signaling</td>
<td>Specifies the signaling protocol used to obtain the ingress and egress labels used in frames transmitted and received on this SDP.</td>
<td></td>
</tr>
<tr>
<td>Admin State</td>
<td>The administrative state of the Keepalive process.</td>
<td></td>
</tr>
<tr>
<td>Oper State</td>
<td>The operational state of the Keepalive process.</td>
<td></td>
</tr>
<tr>
<td>Hello Time</td>
<td>Transmission frequency of the SDP echo request messages.</td>
<td></td>
</tr>
<tr>
<td>Max Drop Count</td>
<td>Specifies the maximum number of consecutive SDP echo request messages that can be unacknowledged before the keepalive protocol reports a fault.</td>
<td></td>
</tr>
<tr>
<td>Hello Msg Len</td>
<td>The length of the SDP echo request messages transmitted on this SDP.</td>
<td></td>
</tr>
<tr>
<td>Hold Down Time</td>
<td>Specifies the amount of time to wait before the keepalive operating status is eligible to enter the alive state.</td>
<td></td>
</tr>
<tr>
<td>I. Fwd. Pkts.</td>
<td>Specifies the number of forwarded ingress packets.</td>
<td></td>
</tr>
<tr>
<td>I. Dro. Pkts</td>
<td>Specifies the number of dropped ingress packets.</td>
<td></td>
</tr>
<tr>
<td>E. Fwd. Pkts.</td>
<td>Specifies the number of forwarded egress packets.</td>
<td></td>
</tr>
<tr>
<td>Associated LSP List</td>
<td>When the SDP type is MPLS, a list of LSPs used to reach the far-end router displays. All the LSPs in the list must terminate at the IP address specified in the Far End field.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>If the SDP type is GRE, then the following message displays: SDP delivery mechanism is not MPLS.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Description</th>
<th>Label</th>
<th>Description (Continued)</th>
</tr>
</thead>
<tbody>
<tr>
<td>SDP Id : 1:1</td>
<td>Type : Spoke</td>
<td></td>
</tr>
<tr>
<td>VC Type : Ether</td>
<td>VC Tag : n/a</td>
<td></td>
</tr>
<tr>
<td>Admin Path MTU : 0</td>
<td>Oper Path MTU : 9186</td>
<td></td>
</tr>
<tr>
<td>Far End : 10.20.1.2</td>
<td>Delivery : MPLS</td>
<td></td>
</tr>
<tr>
<td>Admin State : Up</td>
<td>Oper State : Up</td>
<td></td>
</tr>
<tr>
<td>Acct. Pol : None</td>
<td>Collect Stats : Disabled</td>
<td></td>
</tr>
<tr>
<td>Ingress Label : 2048</td>
<td>Egress Label : 2048</td>
<td></td>
</tr>
</tbody>
</table>
Ing mac Fltr       : n/a                      Egr mac Fltr      : n/a
Ing ip Fltr        : n/a                      Egr ip Fltr       : n/a
Ing ipv6 Fltr      : n/a                      Egr ipv6 Fltr     : n/a
Admin ControlWord  : Not Preferred            Oper ControlWord  : False
Last Status Change : 05/31/2007 00:45:43      Signaling         : None
Last Mgmt Change   : 05/31/2007 00:45:43
Class Fwding State : Up
Flags              : None
Peer Pw Bits       : None
Peer Fault Ip      : None
Peer Vccv CV Bits  : None
Peer Vccv CC Bits  : None
Max Nbr of MAC Addr: No Limit                 Total MAC Addr : 0
Learned MAC Addr   : 0                        Static MAC Addr : 0
MAC Learning       : Enabled                  Discard Unkwn Srce: Disabled
MAC Aging          : Enabled
L2PT Termination   : Disabled                 BPDU Translation : Disabled
MAC Pinning        : Disabled
KeepAlive Information :
Admin State        : Disabled                 Oper State        : Disabled
Hello Time         : 10                       Hello Msg Len     : 0
Max Drop Count     : 3                        Hold Down Time    : 10
Statistics :
I. Fwd. Pkts.      : 0                        I. Dro. Pkts.     : 0
I. Fwd. Octs.      : 0                        I. Dro. Octs.     : 0
E. Fwd. Pkts.      : 0                        E. Fwd. Octets    : 0
MCAC Policy Name   :
MCAC Max Unconst BW: no limit                 MCAC Max Mand BW : no limit
MCAC In use Mand BW: 0                          MCAC Avail Mand BW: unlimited
MCAC In use Opnl BW: 0                          MCAC Avail Opnl BW: unlimited
Associated LSP LIST :
Lsp Name           : A_B_1
Admin State        : Up                       Oper State        : Up
Time Since Last Tr*: 00h26m35s
Lsp Name           : A_B_2
Admin State        : Up                       Oper State        : Up
Time Since Last Tr*: 00h26m35s
Lsp Name           : A_B_3
Admin State        : Up                       Oper State        : Up
Time Since Last Tr*: 00h26m34s
Lsp Name           : A_B_4
Admin State        : Up                       Oper State        : Up
Time Since Last Tr*: 00h26m34s
Lsp Name           : A_B_5
Admin State        : Up                       Oper State        : Up
Time Since Last Tr*: 00h26m34s
Lsp Name           : A_B_6
Admin State        : Up                       Oper State        : Up
Time Since Last Tr*: 00h26m34s
Lsp Name           : A_B_7
Admin State        : Up                       Oper State        : Up
Time Since Last Tr*: 00h26m34s
<table>
<thead>
<tr>
<th>Lsp Name</th>
<th>Admin State</th>
<th>Oper State</th>
<th>Time Since Last Tr*</th>
</tr>
</thead>
<tbody>
<tr>
<td>A_B_8</td>
<td>Up</td>
<td>Up</td>
<td>00h26m35s</td>
</tr>
<tr>
<td>A_B_9</td>
<td>Up</td>
<td>Up</td>
<td>00h26m34s</td>
</tr>
<tr>
<td>A_B_10</td>
<td>Up</td>
<td>Up</td>
<td>00h26m34s</td>
</tr>
</tbody>
</table>

Class-based forwarding:

- Class forwarding: enabled
- Default LSP: A_B_10
- Multicast LSP: A_B_9

FC Mapping Table

<table>
<thead>
<tr>
<th>FC Name</th>
<th>LSP Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>af</td>
<td>A_B_3</td>
</tr>
<tr>
<td>be</td>
<td>A_B_1</td>
</tr>
<tr>
<td>ef</td>
<td>A_B_6</td>
</tr>
<tr>
<td>h1</td>
<td>A_B_7</td>
</tr>
<tr>
<td>h2</td>
<td>A_B_5</td>
</tr>
<tr>
<td>l1</td>
<td>A_B_4</td>
</tr>
<tr>
<td>l2</td>
<td>A_B_2</td>
</tr>
<tr>
<td>nc</td>
<td>A_B_8</td>
</tr>
</tbody>
</table>

Stp Service Destination Point specifics

- Mac Move: Blockable
- Stp Admin State: Up
- Stp Oper State: Down
- Core Connectivity: Down
- Port Role: N/A
- Port Number: 2049
- Port Priority: 128
- Port Path Cost: 10
- Auto Edge: Enabled
- Admin Edge: Disabled
- Oper Edge: N/A
- Link Type: Pt-pt
- BPDU Encap: Dot1d
- Root Guard: Disabled
- Active Protocol: N/A
- Last BFDU from: N/A
- Designated Bridge: N/A
- Designated Port Id: 0
- Fwd Transitions: 0
- Bad BPDUs rcvd: 0
- Cfg BPDUs tx: 0
- Cfg BPDUs rcvd: 0
- TCN BPDUs tx: 0
- TCN BPDUs rcvd: 0
- RST BPDUs tx: 0
- RST BPDUs rcvd: 0

Number of SDPs: 1

* indicates that the corresponding row element may have been truncated.

A:Dut-A#

The following examples show both sides (PE nodes) when control word is enabled:

*A:ALA-Dut-B>config>service>epipe# show service id 2100 sdp detail

Services: Service Destination Points Details

Page 1566
### VLL Show Commands

<table>
<thead>
<tr>
<th>Description</th>
<th>Default sdp description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SDP Id</td>
<td>1:2001</td>
</tr>
<tr>
<td>Type</td>
<td>Spoke</td>
</tr>
<tr>
<td>VC Type</td>
<td>Ether</td>
</tr>
<tr>
<td>VC Tag</td>
<td>n/a</td>
</tr>
<tr>
<td>Admin Path MTU</td>
<td>1600</td>
</tr>
<tr>
<td>Oper Path MTU</td>
<td>1600</td>
</tr>
<tr>
<td>Far End</td>
<td>1.1.1.1</td>
</tr>
<tr>
<td>Delivery</td>
<td>GRE</td>
</tr>
<tr>
<td>Admin State</td>
<td>Up</td>
</tr>
<tr>
<td>Oper State</td>
<td>Up</td>
</tr>
<tr>
<td>Acct. Pol</td>
<td>None</td>
</tr>
<tr>
<td>Collect Stats</td>
<td>Disabled</td>
</tr>
<tr>
<td>Ingress Label</td>
<td>115066</td>
</tr>
<tr>
<td>Egress Label</td>
<td>119068</td>
</tr>
<tr>
<td>Ingress mac Fltr</td>
<td>n/a</td>
</tr>
<tr>
<td>Egress mac Fltr</td>
<td>n/a</td>
</tr>
<tr>
<td>Ingress ip Fltr</td>
<td>n/a</td>
</tr>
<tr>
<td>Egress ip Fltr</td>
<td>n/a</td>
</tr>
<tr>
<td>Ingress ipv6 Fltr</td>
<td>n/a</td>
</tr>
<tr>
<td>Egress ipv6 Fltr</td>
<td>n/a</td>
</tr>
<tr>
<td>Admin ControlWord</td>
<td>Preferred</td>
</tr>
<tr>
<td>Oper ControlWord</td>
<td>True</td>
</tr>
<tr>
<td>Last Status Change</td>
<td>02/05/2007 16:39:22</td>
</tr>
<tr>
<td>Signaling</td>
<td>TLDP</td>
</tr>
<tr>
<td>Last Mgmt Change</td>
<td>02/05/2007 16:39:22</td>
</tr>
<tr>
<td>Class Fwding State</td>
<td>Up</td>
</tr>
<tr>
<td>Precedence</td>
<td>4</td>
</tr>
<tr>
<td>Flags</td>
<td>None</td>
</tr>
<tr>
<td>Peer Pw Bits</td>
<td>None</td>
</tr>
<tr>
<td>Peer Fault Ip</td>
<td>None</td>
</tr>
<tr>
<td>Peer Vccv CV Bits</td>
<td>None</td>
</tr>
<tr>
<td>Peer Vccv CC Bits</td>
<td>None</td>
</tr>
<tr>
<td>Max Mbr of MAC Addr</td>
<td>No Limit</td>
</tr>
<tr>
<td>Total MAC Addr</td>
<td>0</td>
</tr>
<tr>
<td>Learned MAC Addr</td>
<td>0</td>
</tr>
<tr>
<td>Static MAC Addr</td>
<td>0</td>
</tr>
<tr>
<td>MAC Learning</td>
<td>Enabled</td>
</tr>
<tr>
<td>MAC Aging</td>
<td>Enabled</td>
</tr>
<tr>
<td>L2PT Termination</td>
<td>Disabled</td>
</tr>
<tr>
<td>BPDU Translation</td>
<td>Disabled</td>
</tr>
<tr>
<td>MAC Pinning</td>
<td>Disabled</td>
</tr>
<tr>
<td>KeepAlive Information:</td>
<td></td>
</tr>
<tr>
<td>Admin State</td>
<td>Disabled</td>
</tr>
<tr>
<td>Oper State</td>
<td>Disabled</td>
</tr>
<tr>
<td>Hello Time</td>
<td>10</td>
</tr>
<tr>
<td>Hello Msg Len</td>
<td>0</td>
</tr>
<tr>
<td>Max Drop Count</td>
<td>3</td>
</tr>
<tr>
<td>Hold Down Time</td>
<td>10</td>
</tr>
<tr>
<td>I. Fwd. Pkts.</td>
<td>0</td>
</tr>
<tr>
<td>I. Dro. Pkts.</td>
<td>0</td>
</tr>
<tr>
<td>E. Fwd. Pkts.</td>
<td>0</td>
</tr>
<tr>
<td>E. Fwd. Octets</td>
<td>0</td>
</tr>
</tbody>
</table>

**Associated LSP LIST:**
- SDP Delivery Mechanism is not MPLS

---

```
*A:ALA-Dut-B>config>service>epipe#
```
The following is an example when one side (PE) has the control word enabled (the pipe will be down):

This is the side with control word disabled:

*A:ALA-Dut-B>config>service>epipe# show service id 2100 sdp detail
===============================================================================
Services: Service Destination Points Details
===============================================================================
Sdp Id 1:2001  -(1.1.1.1)
Description : Default sdp description
SDP Id : 1:2001 Type : Spoke
VC Type : Ether VC Tag : n/a
Admin Path MTU : 1600 Oper Path MTU : 1600
Far End : 1.1.1.1 Delivery : GRE
Admin State : Up Oper State : Down
Acct. Pol : None Collect Stats : Disabled
Ingress Label : 115066 Egress Label : 119068
Ing mac Fltr : n/a Egr mac Fltr : n/a
Ing ip Fltr : n/a Egr ip Fltr : n/a
Ing ipv6 Fltr : n/a Egr ipv6 Fltr : n/a
Admin ControlWord : Not Preferred Oper ControlWord : False
Last Status Change : 02/05/2007 16:47:54 Signaling : TLDP
Last Mgmt Change : 02/05/2007 16:47:54
Flags : None Peer Pw Bits : None
Peer Fault Ip : None Peer Vccv CV Bits : None
Peer Vccv CC Bits : None
Max Nbr of MAC Addr: No Limit Total MAC Addr : 0
Learned MAC Addr : 0 Static MAC Addr : 0
MAC Learning : Enabled Discard Unkwn Srce: Disabled
MAC Aging : Enabled BPDU Translation : Disabled
L2PT Termination : Disabled
MAC Pinning : Disabled
KeepAlive Information :
Admin State : Disabled Oper State : Disabled
Hello Time : 10 Hello Msg Len : 0
Max Drop Count : 3 Hold Down Time : 10
Statistics :
I. Fwd. Pkts. : 0 I. Dro. Pkts. : 0
E. Fwd. Pkts. : 0 E. Fwd. Octets : 0
Associated LSP LIST :
SDP Delivery Mechanism is not MPLS
Number of SDPs : 1
SDP Id 1:2001

This is the side with control word enabled:

*A:ALA-Dut-B>config>service>epipe#

A:ALA-Dut-B>config>service>epipe# show service id 2100 sdp detail
===============================================================================
Services: Service Destination Points Details
===============================================================================
Sdp Id 1:12000  -(3.3.3.3)

*A:ALA-Dut-B>config>service>epipe#
VLL Show Commands

Description     : Default sdp description
SDP Id           : 1:12000                   Type              : Spoke
VC Type          : Ether                    VC Tag             : n/a
Admin Path MTU  : 1600                     Oper Path MTU      : 1600
Far End          : 3.3.3.3                  Delivery           : GRE
Admin State      : Up                       Oper State        : Down
Acct. Pol        : None                     Collect Stats     : Disabled
Ingress Label    : 119066                   Egress Label      : 0
Ing mac Fltr     : n/a                      Egr mac Fltr      : n/a
Ing ip Fltr      : n/a                      Egr ip Fltr       : n/a
Ing ipv6 Fltr    : n/a                      Egr ipv6 Fltr     : n/a
Admin ControlWord : Preferred                Oper ControlWord  : True
Last Status Change : 02/04/2007 22:52:43      Signaling         : TLDP
Last Mgmt Change : 02/04/2007 02:06:08
Flags            : None
Peer Pw Bits     : None
Peer Fault Ip    : None
Peer Vccv CV Bits: None
Peer Vccv CC Bits: None
Max Nbr of MAC Addr: No Limit                 Total MAC Addr    : 0
Learned MAC Addr : 0                           Static MAC Addr   : 0
MAC Learning     : Enabled                   Discard Unkw Srce: Disabled
MAC Aging        : Enabled                   L2PT Termination  : Disabled
MAC Pinning      : Disabled                   MAC Aging         : Disabled
KeepAlive Information :
Admin State      : Disabled                 Oper State        : Disabled
Hello Time       : 10                       Hello Msg Len     : 0
Max Drop Count   : 3                        Hold Down Time    : 10
Statistics       :
I. Fwd. Pkts.    : 0                        I. Dro. Pkts.      : 0
E. Fwd. Pkts.    : 0                        E. Fwd. Octets    : 0
Associated LSP LIST :
SDP Delivery Mechanism is not MPLS
Number of SDPs : 1

The following is an example when both sides have control word disabled:
*A:ALA-Dut-B>config>service>epipe# show service id 2100 sdp detail

Services: Service Destination Points Details
Sdp Id 1:2001 - (1.1.1.1)
Description     : Default sdp description
SDP Id           : 1:2001                   Type              : Spoke
VC Type          : Ether                    VC Tag             : n/a
Admin Path MTU  : 1600                     Oper Path MTU      : 1600
Far End          : 1.1.1.1                  Delivery           : GRE
Admin State      : Up                       Oper State        : Up
Acct. Pol        : None                     Collect Stats     : Disabled
Ingress Label    : 115066                   Egress Label      : 119068
Ing mac Fltr     : n/a                      Egr mac Fltr      : n/a
Ing ip Fltr      : n/a                      Egr ip Fltr       : n/a
Ing ipv6 Fltr    : n/a                      Egr ipv6 Fltr     : n/a
Admin ControlWord : Not Preferred          Oper ControlWord  : False
Last Status Change : 02/05/2007 16:49:05      Signaling : TLDP
Last Mgmt Change  : 02/05/2007 16:47:54
Flags              : None
Peer Pw Bits       : None
Peer Fault Ip      : None
Peer Vccv CV Bits  : None
Peer Vccv CC Bits  : None
Max Nbr of MAC Addr: No Limit                 Total MAC Addr    : 0
Learned MAC Addr   : 0                        Static MAC Addr   : 0
MAC Learning       : Enabled                   Discard Unkwn Srce: Disabled
MAC Aging          : Enabled                   BPDU Translation  : Disabled
L2PT Termination   : Disabled                 MAC Pinning       : Disabled
KeepAlive Information :
Admin State        : Disabled                 Oper State        : Disabled
Hello Time         : 10                       Hello Msg Len     : 0
Max Drop Count     : 3                        Hold Down Time    : 10
Statistics            :
I. Fwd. Pkts.      : 0                        I. Dro. Pkts.     : 0
E. Fwd. Pkts.      : 0                        E. Fwd. Octets    : 0
Associated LSP LIST :
SDP Delivery Mechanism is not MPLS
Number of SDPs : 1
-------------------------------------------------------------------------------
Number of SDPs : 1
-------------------------------------------------------------------------------
Service Destination Point (Sdp Id : 2000:1) Details
-------------------------------------------------------------------------------
Sdp Id 2000:1  -(101.101.101.101)
-------------------------------------------------------------------------------
Description     : (Not Specified)
SDP Id           : 2000:1                   Type              : Spoke
Spoke Descr      : (Not Specified)
VC Type          : Ether                    VC Tag             : n/a
Admin Path MTU   : 1500                     Oper Path MTU     : 1500
Hash Label       : Enabled
Admin State      : Up                       Oper State        : Down
Acct. Pol        : None                     Collect Stats     : Disabled
Ingress Label    : 0                        Egress Label      : 0
Ingr IPv6 Fltr-Id: n/a                      Egr IPv6 Fltr-Id  : n/a
Admin ControlWord: Not Preferred            Oper ControlWord  : False
Admin BW(Kbps)   : 0                        Oper BW(Kbps)     : 0
Last Status Change : 10/08/2009 06:55:54      Signaling : TLDP
Last Mgmt Change : 10/08/2009 07:04:27      Force Vlan-Vc : Disabled
Endpoint         : N/A                      Precedence        : 4
Class Fwding State : Down
Flags            : SvcAdminDown SdpOperDown
                  NoIngrVCLabel NoEgrVCLabel
                  PathMTUTooSmall
Peer Pw Bits     : None
Peer Fault Ip    : None
Peer Vccv CV Bits: None
Peer Vccv CC Bits: None

*A:ALA-Dut-B>config>service>epipe#
Application Profile: None

KeepAlive Information:
 Admin State       : Enabled                  Oper State       : No response
 Hello Time       : 600                      Hello Msg Len    : 1500
 Max Drop Count   : 3                        Hold Down Time   : 10

Statistics:
 I. Fwd. Pkts.    : 0                        I. Dro. Pkts.     : 0
 E. Fwd. Pkts.    : 0                        E. Fwd. Octets    : 0

RSVP/Static LSPs
 Associated LSP LIST:
 No LSPs Associated

Class-based forwarding:
 Class forwarding  : Disabled                 EnforceDSTELspFc : Disabled
 Default LSP       : Uknwn                    Multicast LSP     : None

FC Mapping Table

<table>
<thead>
<tr>
<th>FC Name</th>
<th>LSP Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>No FC Mappings</td>
<td></td>
</tr>
</tbody>
</table>

Number of SDPs: 1

*A:SetupCLI>config>service>epipe>spoke-sdp#

---

**spoke-sdp-fec**

**Syntax**  
```
spoke-sdp-fec [[1..4294967295]
```

**Context**  
```
show>service>id
```

**Description**  
This command displays spoke-SDP FEC information.

**Parameters**  
- `detail` — Displays detailed information.

**Sample Output**

<table>
<thead>
<tr>
<th>Spoke-Sdp-Fec-Id</th>
<th>Admin State</th>
<th>FEC Type</th>
<th>AII Type</th>
<th>Standby Sig Slave</th>
<th>ICB</th>
<th>Auto Config</th>
<th>Precedence</th>
<th>Retry Timer</th>
<th>Retry Count</th>
<th>SAI1 Type2</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>enabled</td>
<td>129</td>
<td>2</td>
<td>disabled</td>
<td></td>
<td></td>
<td>4</td>
<td>10 secs</td>
<td>10</td>
<td>3:10.20.1.3:1</td>
</tr>
</tbody>
</table>
Show, Clear, Debug Commands

TAII Type2 : 6:10.20.1.6:1
Path : n/a
Endpoint : n/a
Oper SDP-Bind : 17407:4294967246
Last Error : <none>

Entries found: 1

---

stp

**Syntax**  
stp [detail]

**Context**  
show>service>id

**Description**  
This command displays information for the spanning tree protocol instance for the service.

**Parameters**  
detail — Displays detailed information.

spoke-sdp-fec

**Syntax**  
spoke-sdp-fec [[1..4294967295]

**Context**  
show>service>id

**Description**  
This command displays the details of a spoke-sdp-fec spoke-sdp.

**Sample Output**

---

Service Spoke-SDP FEC Information

<table>
<thead>
<tr>
<th>Spoke-Sdp-Fec-Id</th>
<th>Admin State</th>
<th>FEc Type</th>
<th>AIi Type</th>
<th>Standby Sig Slave</th>
<th>ICB</th>
<th>Auto Config</th>
<th>PW Template Id</th>
<th>Precedence</th>
<th>Retry Timer</th>
<th>Retry Count</th>
<th>Retries Remaining</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>enabled</td>
<td>129</td>
<td>2</td>
<td>disabled</td>
<td>disabled</td>
<td>disabled</td>
<td>(none)</td>
<td>4</td>
<td>10 secs</td>
<td>10</td>
<td>0</td>
</tr>
</tbody>
</table>

Entries found: 1

---
VLL Clear Commands

id

Syntax  id service-id
Context  clear>service
clear>service>statistics
Description  This command clears commands for a specific service.
Parameters  service-id — The ID that uniquely identifies a service.
           Values  service-id: 1 — 214748364
                    svc-name: A string up to 64 characters in length.

mesh-sdp

Syntax  mesh-sdp sd-id[:vc-id] ingress-vc-label
Context  clear>service>id
Description  This command clears and resets the mesh SDP binding.
Parameters  sd-id — The spoke SDP ID for which to clear statistics.
           Values  1 — 17407
vc-id — The virtual circuit ID on the SDP ID to be reset.
           Values  1 — 4294967295
ingress-vc-label — Specifies to clear the ingress VC label.

spoke-sdp

Syntax  spoke-sdp sd-id:vc-id ingress-vc-label
Context  clear>service>id
Description  This command clears and resets the spoke SDP bindings for the service.
Parameters  sd-id — The spoke SDP ID to be reset.
           Values  1 — 17407
vc-id — The virtual circuit ID on the SDP ID to be reset.
           Values  1 — 4294967295
ingress-vc-label — Specifies to clear the ingress VC label.
Show, Clear, Debug Commands

sap

Syntax  sap sap-id {all | counters | stp}
Context  clear>service>statistics
Description  This command clears SAP statistics for a SAP.
Parameters  sap-id — Specifies the physical port identifier portion of the SAP definition. See Common CLI Command Descriptions on page 1783 for command syntax.
  all — Clears all SAP queue statistics and STP statistics.
  counters — Clears all queue statistics associated with the SAP.
  stp — Clears all STP statistics associated with the SAP.

sdp

Syntax  sdp sdp-id keep-alive
Context  clear>service>statistics
Description  This command clears keepalive statistics associated with the SDP ID.
Parameters  sdp-id — The SDP ID for which to clear keepalive statistics.
  Values  1 — 17407

counters

Syntax  counters
Context  clear>service>statistics>id
Description  This command clears all traffic queue counters associated with the service ID.

spoke-sdp

Syntax  spoke-sdp sdp-id[:vc-id] {all | counters | stp}
Context  clear>service>statistics>id
Description  This command clears statistics for the spoke SDP bound to the service.
Parameters  sdp-id — The spoke SDP ID for which to clear statistics.
  Values  1 — 17407
  vc-id — The virtual circuit ID on the SDP ID to be reset.
  Values  1 — 4294967295
all — Clears all queue statistics and STP statistics associated with the SDP.
counters — Clears all queue statistics associated with the SDP.
stp — Clears all STP statistics associated with the SDP.

stp

**Syntax**

```plaintext
stp
```

**Context**

```plaintext
clear>service>statistics>id
```

**Description**

Clears all spanning tree statistics for the service ID.
VLL Debug Commands

id

**Syntax**

```plaintext
id service-id
```

**Context**

debug>service

**Description**

This command debugs commands for a specific service.

**Parameters**

`service-id` — The ID that uniquely identifies a service.

---

sap

**Syntax**

```plaintext
[no] sap sap-id
```

**Context**

debug>service>id

**Description**

This command enables debugging for a particular SAP.

**Parameters**

`sap-id` — Specifies the SAP ID.

---

event-type

**Syntax**

```plaintext
[no] event-type {arp | config-change | |oper-status-change}
```

**Context**

debug>service>id

**Description**

This command enables a particular debugging event type. The **no** form of the command disables the event type debugging.

**Parameters**

`arp` — Displays ARP events.
`config-change` — Debugs configuration change events.
`svc-oper-status-change` — Debugs service operational status changes.

---

**Sample Output**

```
A:bksim180# debug service id 1000 sap 1/7/1 event-type arp
DEBUG OUTPUT show on CLI is as follows:
3 2008/11/17 18:13:24.35 UTC MINOR: DEBUG #2001 Base Service 1000 SAP 1/7/1 "Service 1000 SAP 1/7/1:
RX: ARP_REQUEST (0x0001)
hwType : 0x0001
prType : 0x0800
hwLength : 0x06
```
VLL Show Commands

```
prLength : 0x04
srcMac   : 8c:c7:01:07:00:03
destMac  : 00:00:00:00:00:00
srcIp    : 200.1.1.2
destIp   : 200.1.1.1
```

4 2008/11/17 18:13:24.35 UTC MINOR: DEBUG #2001 Base Service 1000 SAP 1/7/1 "Service 1000 SAP 1/7/1:
TX: ARP_RESPONSE (0x0002)
hwType : 0x0001
prType : 0x0800
hwLength: 0x06
prLength: 0x04
srcMac : 00:03:0a:0a:0a:0a
destMac: 8c:c7:01:07:00:03
srcIp  : 200.1.1.1
destIp : 200.1.1.2
```

sdp

**Syntax**  
[no] sdp sdp-id:vc-id

**Context**  
debug>service>id

**Description**  
This command enables debugging for a particular SDP.

**Parameters**  
sdp-id — Specifies the SDP ID.
VPLS Show Commands

egress-label

Syntax  
```plaintext
egress-label egress-label1 [egress-label2]
```

Context  
show>service

Description  
This command displays service information using the range of egress labels.

If only the mandatory `egress-label1` parameter is specified, only services using the specified label are displayed.

If both `egress-label1` and `egress-label2` parameters are specified, the services using the range of labels X where `egress-label1 <= X <= egress-label2` are displayed.

Use the `show router ldp bindings` command to display dynamic labels.

Parameters  
- **egress-label1** — The starting egress label value for which to display services using the label range. If only `egress-label1` is specified, services only using `egress-label1` are displayed.
  - **Values**  
    - 0, 2049 — 131071

- **egress-label2** — The ending egress label value for which to display services using the label range.
  - **Default**  
    - `egress-label1` value.
  - **Values**  
    - 2049 — 131071

fdb-info

Syntax  
```plaintext
fdb-info
```

Context  
show>service

Description  
Displays global FDB usage information.

Output  
**Show FDB-Info Command Output** — The following table describes show FDB-Info command output.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service ID</td>
<td>The value that identifies a service.</td>
</tr>
<tr>
<td>Mac Move</td>
<td>Indicates the administrative state of the MAC movement feature associated with the service.</td>
</tr>
<tr>
<td>Label</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Mac Move Rate</td>
<td>The maximum rate at which MAC’s can be re-learned in this TLS service, before the SAP where the moving MAC was last seen is automatically disabled in order to protect the system against undetected loops or duplicate MAC’s. The rate is computed as the maximum number of re-learns allowed in a 5 second interval. The default rate of 10 re-learns per second corresponds to 50 re-learns in a 5 second period.</td>
</tr>
<tr>
<td>Mac Move Timeout</td>
<td>Indicates the time in seconds to wait before a SAP that has been disabled after exceeding the maximum re-learn rate is re-enabled. A value of zero indicates that the SAP will not be automatically re-enabled after being disabled. If after the SAP is re-enabled it is disabled again, the effective retry timeout is doubled in order to avoid thrashing.</td>
</tr>
<tr>
<td>Table Size</td>
<td>The maximum number of learned and static entries allowed in the FDB.</td>
</tr>
<tr>
<td>Total Count</td>
<td>The current number of entries (both learned and static) in the FDB of this service.</td>
</tr>
<tr>
<td>Learned Count</td>
<td>The current number of learned entries in the FDB of this service.</td>
</tr>
<tr>
<td>Static Count</td>
<td>The current number of static entries in the FDB of this service.</td>
</tr>
<tr>
<td>Local Age</td>
<td>The seconds used to age out FDB entries learned on local SAPs.</td>
</tr>
<tr>
<td>High WaterMark</td>
<td>The utilization of the FDB table of this service at which a ‘table full’ alarm is raised by the agent.</td>
</tr>
<tr>
<td>Low WaterMark</td>
<td>The utilization of the FDB table of this service at which a ‘table full’ alarm is cleared by the agent.</td>
</tr>
<tr>
<td>Mac Learning</td>
<td>Specifies whether the MAC learning process is enabled in this service.</td>
</tr>
<tr>
<td>Discard Unknown</td>
<td>Specifies whether frames received with an unknown destination MAC are discarded in this service.</td>
</tr>
<tr>
<td>MAC Aging</td>
<td>Specifies whether the MAC aging process is enabled in this service.</td>
</tr>
<tr>
<td>Relearn Only</td>
<td>When enabled, indicates that either the FDB table of this service is full or that the maximum system-wide number of MAC’s supported by the agent has been reached, and thus MAC learning is temporary disabled, and only MAC re-learns can take place.</td>
</tr>
<tr>
<td>Total Service FDB</td>
<td>The current number of service FDBs configured on this node.</td>
</tr>
<tr>
<td>Total FDB Configured Size</td>
<td>The sum of configured FDBs.</td>
</tr>
<tr>
<td>Total FDB Entries In Use</td>
<td>The total number of entries (both learned and static) in use.</td>
</tr>
</tbody>
</table>
VPLS Show Commands

fdb-mac

Syntax

fdb-mac ieee-address [expiry]

Context

show>service

Description

This command displays the FDB entry for a given MAC address.

Parameters

ieee-address — The 48-bit MAC address for which to display the FDB entry in the form

aa:bb:cc:dd:ee:ff or aa-bb-cc-dd-ee-ff where aa, bb, cc, dd, ee and ff are hexadecimal numbers.

expiry — Shows the time until the MAC is aged out.

Output

Show FDB-MAC Command Output — The following table describes the show FDB MAC command output fields:

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service ID</td>
<td>The service ID number.</td>
</tr>
<tr>
<td>MAC</td>
<td>The specified MAC address</td>
</tr>
<tr>
<td>Source-Identifier</td>
<td>The location where the MAC is defined.</td>
</tr>
<tr>
<td>Type/Age</td>
<td>Static — FDB entries created by management.</td>
</tr>
<tr>
<td></td>
<td>Learned — Dynamic entries created by the learning process.</td>
</tr>
<tr>
<td></td>
<td>P — Indicates the MAC is protected by the MAC protection feature.</td>
</tr>
</tbody>
</table>

Sample Output

*A:ian2# show service fdb-mac

Service Forwarding Database

<table>
<thead>
<tr>
<th>ServId</th>
<th>MAC</th>
<th>Source-Identifier</th>
<th>Type</th>
<th>Age</th>
<th>Last Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>00:00:00:00:00:01</td>
<td>sap:1/1/1</td>
<td>LP/0</td>
<td>01/07/2011</td>
<td>20:25:34</td>
</tr>
<tr>
<td>1</td>
<td>00:00:00:00:00:02</td>
<td>sap:1/1/2</td>
<td>L/0</td>
<td>01/07/2011</td>
<td>20:26:25</td>
</tr>
<tr>
<td>1</td>
<td>00:00:00:00:00:03</td>
<td>sap:1/1/1</td>
<td>A/0</td>
<td>01/07/2011</td>
<td>20:25:34</td>
</tr>
</tbody>
</table>

No. of Entries: 2

Legend: L-Learned; P-MAC is protected; A-Auto learn protected

*A:ian2#

The following shows the protected MACs in the FDB.

A:term17>config>service>vpls>sap>arp-host# show service id 12 fdb detail

Forwarding Database, Service 12

<table>
<thead>
<tr>
<th>ServId</th>
<th>MAC</th>
<th>Source-Identifier</th>
<th>Type</th>
<th>Age</th>
<th>Last Change</th>
</tr>
</thead>
</table>

7950 SR OS Services Guide
The following shows whether restrict-protected-src or restrict-unprotected-dst are enabled on SDPs.

*Arian1# show service id 1 sdp 1:1 detail

-------------------------------------------------------------------------------
| Sdp Id 1:1  -(1.1.1.2) |
-------------------------------------------------------------------------------

Flags              : RxProtSrcMac
Restr MacProt Src  : Enabled                  Restr MacUnpr Dst : Disabled

**ingress-label**

**Syntax**

**ingress-label start-label [end-label]**

**Context**

show>service

**Description**

Display services using the range of ingress labels.

If only the mandatory *start-label* parameter is specified, only services using the specified label are displayed.

If both *start-label* and *end-label* parameters are specified, the services using the range of labels X where *start-label* <= X <= *end-label* are displayed.

Use the show router ldp bindings command to display dynamic labels.

**Parameters**

*start-label* — The starting ingress label value for which to display services using the label range. If only *start-label* is specified, services only using *start-label* are displayed.

**Values**

0, 2048 — 131071

*end-label* — The ending ingress label value for which to display services using the label range.

**Default**

The *start-label* value.

**Values**

2049 — 131071
Show Service Ingress-Label — The following table describes show service ingress-label output fields.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Svc ID</td>
<td>The service identifier.</td>
</tr>
<tr>
<td>SDP Id</td>
<td>The SDP identifier.</td>
</tr>
<tr>
<td>Type</td>
<td>Indicates whether the SDP is spoke.</td>
</tr>
<tr>
<td>I.Lbl</td>
<td>The ingress label used by the far-end device to send packets to this device in this service by the SDP.</td>
</tr>
<tr>
<td>E.Lbl</td>
<td>The egress label used by this device to send packets to the far-end device in this service by the SDP.</td>
</tr>
<tr>
<td>Number of Bindings Found</td>
<td>The number of SDP bindings within the label range specified.</td>
</tr>
</tbody>
</table>
Show, Clear, Debug Commands

sap-using

Syntax

```
sap-using [msap] [dyn-script] [description]
sap-using [sap sap-id] [vlan-translation | anti-spoof] [description]
sap-using interface [ip-address | ip-int-name]
sap-using [ingress | egress] filter filter-id
sap-using [sap sap-id]
sap-using [ingress] qos-policy qos-policy-id
```

Context

```
show>service
```

Description

This command displays SAP information.

If no optional parameters are specified, the command displays a summary of all defined SAPs. The optional parameters restrict output to only SAPs matching the specified properties.

Parameters

- `ingress` — Specifies matching an ingress policy.
- `egress` — Specifies matching an egress policy.
- `filter filter-id` — The ingress or egress filter policy ID for which to display matching SAPs.

  **Values**

  - `1 — 65535`

- `dyn-script` — Displays dynamic service SAPs information.

- `sap-id` — Specifies the physical port identifier portion of the SAP definition. See Common CLI Command Descriptions on page 1783 for command syntax.

Output

**Show Service SAP** — The following table describes show service SAP output fields:

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port ID</td>
<td>The ID of the access port where the SAP is defined.</td>
</tr>
<tr>
<td>Svc ID</td>
<td>The service identifier.</td>
</tr>
<tr>
<td>I.QoS</td>
<td>The SAP ingress QoS policy number specified on the ingress SAP.</td>
</tr>
<tr>
<td>I.MAC/IP</td>
<td>The MAC or IP filter policy ID applied to the ingress SAP.</td>
</tr>
<tr>
<td>Egr. Fltr</td>
<td>The filter policy ID applied to the egress SAP.</td>
</tr>
<tr>
<td>A.Pol</td>
<td>The accounting policy ID assigned to the SAP.</td>
</tr>
<tr>
<td>Adm</td>
<td>The administrative state of the SAP.</td>
</tr>
<tr>
<td>Opr</td>
<td>The actual state of the SAP.</td>
</tr>
</tbody>
</table>

Sample Output
sdp

Syntax
sdp [sdp-id | far-end ip-addr] [detail | keep-alive-history]

Context
show>service>id

Description
This command displays information for the SDPs associated with the service.
If no optional parameters are specified, a summary of all associated SDPs is displayed.

Parameters
sdp-id — Displays only information for the specified SDP ID. An SDP is a logical mechanism that
ties a far-end to a particular service without having to specifically define far end SAPs. Each
SDP represents a method to reach a router.

Default All SDPs.

Values 1 — 17407

far-end ip-addr — Displays only SDPs matching with the specified system IP address of the far-end
destination router for the Service Distribution Point (SDP) that is the termination point for a
service.

Default SDPs with any far-end IP address.

detail — Displays detailed SDP information.

Output
Show Service SDP — The following table describes show service-id SDP output fields.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sdp Id</td>
<td>The SDP identifier.</td>
</tr>
<tr>
<td>Type</td>
<td>Indicates whether the SDP is a spoke</td>
</tr>
<tr>
<td>VC Type</td>
<td>Displays the VC type, ether or vlan.</td>
</tr>
<tr>
<td>VC Tag</td>
<td>Displays the explicit dot1Q value used when encapsulating to the SDP far end.</td>
</tr>
<tr>
<td>I. Lbl</td>
<td>The VC label used by the far-end device to send packets to this device in this service by the SDP.</td>
</tr>
<tr>
<td>Admin Path MTU</td>
<td>The operating path MTU of the SDP is equal to the admin path MTU (when one is set) or the dynamically computed tunnel MTU, when no admin path MTU is set (the default case.)</td>
</tr>
<tr>
<td>Oper Path MTU</td>
<td>The actual largest service frame size (in octets) that can be transmitted through this SDP to the far-end router, without requiring the packet to be fragmented.</td>
</tr>
<tr>
<td>Far End</td>
<td>Specifies the IP address of the remote end of the MPLS tunnel defined by this SDP.</td>
</tr>
<tr>
<td>Delivery</td>
<td>Specifies the type of delivery used by the SDP: MPLS.</td>
</tr>
<tr>
<td>Admin State</td>
<td>The administrative state of this SDP.</td>
</tr>
<tr>
<td>Oper State</td>
<td>The operational state of this SDP.</td>
</tr>
</tbody>
</table>
**Sample Output**

```
A:ALA-48# show service id <service-id> mac-protect

Mac Protection

ServId    MAC
1         aa:aa:aa:aa:aa:ab

No. of MAC Entries: 1
```

**Label** | **Description (Continued)**
---|---
Ingress Label | The label used by the far-end device to send packets to this device in this service by this SDP.
Egress Label | The label used by this device to send packets to the far-end device in this service by the SDP.
Last Changed | The date and time of the most recent change to the SDP.
Signaling | Specifies the signaling protocol used to obtain the ingress and egress labels used in frames transmitted and received on this SDP.
Admin State | The administrative state of the Keepalive process.
Oper State | The operational state of the Keepalive process.
Hello Time | Specifies how often the SDP echo request messages are transmitted on this SDP.
Max Drop Count | Specifies the maximum number of consecutive SDP echo request messages that can be unacknowledged before the keepalive protocol reports a fault.
Hello Msg Len | Specifies the length of the SDP echo request messages transmitted on this SDP.
Hold Down Time | Specifies the amount of time to wait before the keepalive operating status is eligible to enter the alive state.
I. Fwd. Pkts. | Specifies the number of forwarded ingress packets.
I. Dro. Pkts | Specifies the number of dropped ingress packets.
E. Fwd. Pkts. | Specifies the number of forwarded egress packets.
E. Fwd. Octets | Specifies the number of forwarded egress octets.
Associated LSP List | When the SDP type is MPLS, a list of LSPs used to reach the far-end router displays. All the LSPs in the list must terminate at the IP address specified in the Far End field. If the SDP type is GRE, then the following message displays: SDP Delivery Mechanism is not MPLS.
**sdp-using**

**Syntax**

sdp-using [sdp-id:vc-id] | far-end ip-address

**Context**

show>service

**Description**

This command displays services using SDP or far-end address options.

**Parameters**

- **sdp-id** — Displays only services bound to the specified SDP ID.
  
  **Values**
  
  1 — 17407

- **vc-id** — The virtual circuit identifier.
  
  **Values**
  
  1 — 4294967295

- **far-end ip-address** — Displays only services matching with the specified far-end IP address.
  
  **Default**
  
  Services with any far-end IP address.

**Output**

**Show Service SDP Using** — The following table describes service-using output fields.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Svc ID</td>
<td>The service identifier.</td>
</tr>
<tr>
<td>Sdp ID</td>
<td>The SDP identifier.</td>
</tr>
<tr>
<td>Type</td>
<td>Specifies the type of SDP: Spoke</td>
</tr>
<tr>
<td>Far End</td>
<td>The far-end address of the SDP.</td>
</tr>
<tr>
<td>Oper State</td>
<td>The operational state of the service.</td>
</tr>
<tr>
<td>Ingress Label</td>
<td>The label used by the far-end device to send packets to this device in this service by this SDP.</td>
</tr>
<tr>
<td>Egress Label</td>
<td>The label used by this device to send packets to the far-end device in this service by this SDP.</td>
</tr>
</tbody>
</table>

**Sample Output**

*ALA-1#* show service sdp-using 300

```
Service Destination Point (Sdp Id : 300)

<table>
<thead>
<tr>
<th>SvcId</th>
<th>SdpId</th>
<th>Type</th>
<th>Far End</th>
<th>Opr State</th>
<th>I.Label</th>
<th>E.Label</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>300:2</td>
<td>Spok</td>
<td>10.0.0.13</td>
<td>Up</td>
<td>131070</td>
<td>131070</td>
</tr>
</tbody>
</table>
```

Number of SDPs : 

*A:ALA-1#*
service-using

Syntax  service-using [epipe] [vpls] [mirror] [customer customer-id]

Context  show>service

Description  This command displays the services matching certain usage properties. If no optional parameters are specified, all services defined on the system are displayed.

Parameters  
- **epipe** — Displays matching Epipe services.
- **vpls** — Displays matching VPLS instances.
- **mirror** — Displays matching mirror services.
- **customer customer-id** — Displays services only associated with the specified customer ID.

Default  Services associated with a customer.

Values  1 — 2147483647

Output  

**Show Service Service-Using** — The following table describes show service service-using output fields:

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Id</td>
<td>The service identifier.</td>
</tr>
<tr>
<td>Type</td>
<td>Specifies the service type configured for the service ID.</td>
</tr>
<tr>
<td>Adm</td>
<td>The administrative state of the service.</td>
</tr>
<tr>
<td>Opr</td>
<td>The operating state of the service.</td>
</tr>
<tr>
<td>CustomerID</td>
<td>The ID of the customer who owns this service.</td>
</tr>
<tr>
<td>Last Mgmt Change</td>
<td>The date and time of the most recent management-initiated change to this service.</td>
</tr>
</tbody>
</table>

Sample Output

*A:ALA-12# show service service-using customer 10

Services

<table>
<thead>
<tr>
<th>ServiceId</th>
<th>Type</th>
<th>Adm</th>
<th>Opr</th>
<th>CustomerId</th>
<th>Last Mgmt Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>VPLS</td>
<td>Up</td>
<td>Up</td>
<td>10</td>
<td>09/05/2006 13:24:15</td>
</tr>
<tr>
<td>100</td>
<td>IES</td>
<td>Up</td>
<td>Up</td>
<td>10</td>
<td>09/05/2006 13:24:15</td>
</tr>
<tr>
<td>300</td>
<td>Epipe</td>
<td>Up</td>
<td>Up</td>
<td>10</td>
<td>09/05/2006 13:24:15</td>
</tr>
</tbody>
</table>

Matching Services : 3

*A:ALA-12#

*A:ALA-12# show service service-using epipe

Services [epipe]
### ServiceId | Type | Adm | Opr | CustomerId | Last Mgmt Change
---|---|---|---|---|---
6 | Epipe | Up | Up | 6 | 09/22/2006 23:05:58
7 | Epipe | Up | Up | 6 | 09/22/2006 23:05:58
8 | Epipe | Up | Up | 3 | 09/22/2006 23:05:58
103 | Epipe | Up | Up | 6 | 09/22/2006 23:05:58

Matching Services : 4

### ServiceId | Type | Adm | Opr | CustomerId | Last Mgmt Change
---|---|---|---|---|---
10 | mVPLS | Down | Down | 1 | 10/26/2006 15:44:57
11 | mVPLS | Down | Down | 1 | 10/26/2006 15:44:57
100 | mVPLS | Up | Up | 1 | 10/26/2006 15:44:57
101 | mVPLS | Up | Up | 1 | 10/26/2006 15:44:57
102 | mVPLS | Up | Up | 1 | 10/26/2006 15:44:57

Matching Services : 5
id

**Syntax**

`id service-id`

**Context**

`show>service`

**Description**

This command displays information for a particular service-id.

**Parameters**

`service-id` — The unique service identification number that identifies the service in the service domain.

**Values**

- `service-id`: 1 — 214748364
- `svc-name`: A string up to 64 characters in length.

**Parameters**

- `all` — Display detailed information about the service.
- `base` — Display basic service information.
- `endpoint` — Display service endpoint information.
- `fdb` — Display FDB entries.
- `labels` — Display labels being used by this service.
- `sap` — Display SAPs associated to the service.
- `sdp` — Display SDPs associated with the service.
- `stp` — Display STP information.
Syntax: `all`

Context: `show>service>id`

Description: This command displays detailed information for all aspects of the service.

Output: Show service ID all output — The following table describes the command output fields.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Id</td>
<td>The service identifier.</td>
</tr>
<tr>
<td>VPN Id</td>
<td>The number which identifies the VPN.</td>
</tr>
<tr>
<td>Service Type</td>
<td>Specifies the type of service.</td>
</tr>
<tr>
<td>Description</td>
<td>Generic information about the service.</td>
</tr>
<tr>
<td>Customer Id</td>
<td>The customer identifier.</td>
</tr>
<tr>
<td>Last Mgmt Change</td>
<td>The date and time of the most recent management-initiated change to this customer.</td>
</tr>
<tr>
<td>SAP Count</td>
<td>The number of SAPs specified for this service.</td>
</tr>
<tr>
<td>Admin State</td>
<td>The administrative state of this SDP.</td>
</tr>
<tr>
<td>Oper State</td>
<td>The operational state of this SDP.</td>
</tr>
<tr>
<td>Ingress Filter</td>
<td>The ID of the ingress filter policy.</td>
</tr>
<tr>
<td>Egress Filter</td>
<td>The ID of the egress filter policy.</td>
</tr>
<tr>
<td>Last Changed</td>
<td>The date and time of the most recent change to this customer.</td>
</tr>
<tr>
<td>Service Id</td>
<td>The service identifier.</td>
</tr>
<tr>
<td>Port Id</td>
<td>The ID of the access port where this SAP is defined.</td>
</tr>
<tr>
<td>Description</td>
<td>Generic information about the SAP.</td>
</tr>
<tr>
<td>Encap Value</td>
<td>The value of the label used to identify this SAP on the access port.</td>
</tr>
<tr>
<td>Admin State</td>
<td>The administrative state of the SAP.</td>
</tr>
<tr>
<td>Oper State</td>
<td>The operating state of the SAP.</td>
</tr>
<tr>
<td>Last Changed</td>
<td>The date and time of the last change.</td>
</tr>
<tr>
<td>Ingress qos-policy</td>
<td>The SAP ingress QoS policy ID.</td>
</tr>
<tr>
<td>Ingress Filter-Id</td>
<td>The SAP ingress filter policy ID.</td>
</tr>
<tr>
<td>Egress Filter-Id</td>
<td>The SAP egress filter policy ID.</td>
</tr>
<tr>
<td>Acct. Pol</td>
<td>Indicates the accounting policy applied to the SAP.</td>
</tr>
<tr>
<td>Collect Stats</td>
<td>Specifies whether accounting statistics are collected on the SAP.</td>
</tr>
</tbody>
</table>
Show, Clear, Debug Commands

**show service id arp**

**Syntax:** ` arp [ip-address] | [mac ieee-address] | [sap sap-id] | [interface ip-int-name]`

**Context:** `show>service>id`

**Description:** This command displays the ARP table for the VPLS instance. The ARP entries for a subscriber interface are displayed uniquely. Each MAC associated with the subscriber interface child group-interfaces is displayed with each subscriber interface ARP entry for easy lookup.

**Parameters**

- `ip-address` — All IP addresses.
- `mac ieee-address` — Displays only ARP entries in the ARP table with the specified 48-bit MAC address. The MAC address is in the form aa:bb:cc:dd:ee:ff or aa-bb-cc-dd-ee-ff, where aa, bb, cc, dd, ee and ff are hexadecimal numbers.
- `Default` — All MAC addresses.
- `sap sap-id` — Displays SAP information for the specified SAP ID.
- `interface` — Specifies matching service ARP entries associated with the IP interface.
- `ip-address` — The IP address of the interface for which to display matching ARP entries.
- `Values` — `1.0.0.0 — 223.255.255.255`
- `ip-int-name` — The IP interface name for which to display matching ARPs.

**Output**

**Show Service-ID ARP** — The following table describes show service-id ARP output fields.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>The IP address.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>The specified MAC address.</td>
</tr>
<tr>
<td></td>
<td>Type Static — FDB entries created by management.</td>
</tr>
</tbody>
</table>
## VPLS Show Commands

### Syntax

```
base
```

### Context

```
show>service>id
show>service>id>igmp-snooping
```

### Description

This command displays basic information about the service ID including service type, description, SAPs and SDPs.

### Output

**Show Service-ID Base** — The following table describes show service-id base output fields:

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Id</td>
<td>The service identifier.</td>
</tr>
<tr>
<td>Vpn Id</td>
<td>Specifies the VPN ID assigned to the service.</td>
</tr>
<tr>
<td>Service Type</td>
<td>Displays the type of service.</td>
</tr>
<tr>
<td>Description</td>
<td>Generic information about the service.</td>
</tr>
<tr>
<td>Customer Id</td>
<td>The customer identifier.</td>
</tr>
<tr>
<td>Last Mgmt Change</td>
<td>The date and time of the most recent management-initiated change to this customer.</td>
</tr>
<tr>
<td>Adm</td>
<td>The administrative state of the service.</td>
</tr>
<tr>
<td>Oper</td>
<td>The operational state of the service.</td>
</tr>
<tr>
<td>Mtu</td>
<td>The largest frame size (in octets) that the service can handle.</td>
</tr>
<tr>
<td>Def. Mesh VC Id</td>
<td>This object is only valid in services that accept mesh SDP bindings. It is used to validate the VC ID portion of each mesh SDP binding defined in the service.</td>
</tr>
<tr>
<td>SAP Count</td>
<td>The number of SAPs defined on the service.</td>
</tr>
<tr>
<td>SDP Bind Count</td>
<td>The number of SDPs bound to the service.</td>
</tr>
<tr>
<td>Label</td>
<td>Description (Continued)</td>
</tr>
<tr>
<td>-----------</td>
<td>----------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Identifier</td>
<td>Specifies the service access (SAP) and destination (SDP) points.</td>
</tr>
<tr>
<td>Type</td>
<td>Specifies the signaling protocol used to obtain the ingress and egress labels used in frames transmitted and received on the SDP.</td>
</tr>
<tr>
<td>AdmMTU</td>
<td>Specifies the largest service frame size (in octets) that can be transmitted through this SDP to the far-end ESR, without requiring the packet to be fragmented.</td>
</tr>
<tr>
<td>OprMTU</td>
<td>Specifies the actual largest service frame size (in octets) that can be transmitted through this service to the far-end ESR, without requiring the packet to be fragmented.</td>
</tr>
<tr>
<td>Opr</td>
<td>The operating state of the SAP</td>
</tr>
</tbody>
</table>

**Sample Output**
VPLS Show Commands

**fdb**

**Syntax**

```
fdb [sap sap-id [expiry]] | [mac ieee-address [expiry]] | [detail] [expiry]
```

**Context**

- `show>service>id`
- `show>service>fdb-mac`

**Description**

This command displays FDB entries for a given MAC address.

**Parameters**

- `sap sap-id` — Specifies the physical port identifier portion of the SAP. See Common CLI Command Descriptions on page 1783 for command syntax.
- `detail` — Displays detailed information.
- `expiry` — Displays time until MAC is aged out.

**Show FDB Information** — The following table describes service FDB output fields.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ServID</td>
<td>Displays the service ID.</td>
</tr>
<tr>
<td>MAC</td>
<td>Displays the associated MAC address.</td>
</tr>
<tr>
<td>Mac Move</td>
<td>Displays the administrative state of the MAC movement feature associated with this service.</td>
</tr>
<tr>
<td>Primary Factor</td>
<td>Displays a factor for the primary ports defining how many MAC-relearn periods should be used to measure the MAC-relearn rate.</td>
</tr>
<tr>
<td>Secondary Factor</td>
<td>Displays a factor for the secondary ports defining how many MAC-relearn periods should be used to measure the MAC-relearn rate.</td>
</tr>
<tr>
<td>Mac Move Rate</td>
<td>Displays the maximum rate at which MAC's can be re-learned in this service, before the SAP where the moving MAC was last seen is automatically disabled in order to protect the system against undetected loops or duplicate MAs. The rate is computed as the maximum number of re-learns allowed in a 5 second interval: for example, the default rate of 2 re-learns per second corresponds to 10 re-learns in a 5 second period.</td>
</tr>
<tr>
<td>Mac Move Timeout</td>
<td>Displays the time in seconds to wait before a SAP that has been disabled after exceeding the maximum re-learn rate is re-enabled. A value of zero indicates that the SAP will not be automatically re-enabled after being disabled. If after the SAP is re-enabled it is disabled again, the effective retry timeout is doubled in order to avoid thrashing.</td>
</tr>
<tr>
<td>Mac Move Retries</td>
<td>Displays the number of times retries are performed for reenabling the SAP/SDP.</td>
</tr>
<tr>
<td>Table Size</td>
<td>Specifies the maximum number of learned and static entries allowed in the FDB of this service.</td>
</tr>
<tr>
<td>Total Count</td>
<td>Displays the total number of learned entries in the FDB of this service.</td>
</tr>
<tr>
<td>Label</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Learned Count</td>
<td>Displays the current number of learned entries in the FDB of this service.</td>
</tr>
<tr>
<td>Static Count</td>
<td>Displays the current number of static entries in the FDB of this service.</td>
</tr>
<tr>
<td>OAM-learned Count</td>
<td>Displays the current number of OAM entries in the FDB of this service.</td>
</tr>
<tr>
<td>Remote Age</td>
<td>Displays the number of seconds used to age out FDB entries learned on an SDP.</td>
</tr>
<tr>
<td>Local Age</td>
<td>Displays the number of seconds used to age out FDB entries learned on local SAPs.</td>
</tr>
<tr>
<td>High Watermark</td>
<td>Displays the utilization of the FDB table of this service at which a table full alarm will be raised by the agent.</td>
</tr>
<tr>
<td>Low Watermark</td>
<td>Displays the utilization of the FDB table of this service at which a table full alarm will be cleared by the agent.</td>
</tr>
<tr>
<td>Mac Learning</td>
<td>Specifies whether the MAC learning process is enabled.</td>
</tr>
<tr>
<td>Discard Unknown</td>
<td>Specifies whether frames received with an unknown destination MAC are discarded.</td>
</tr>
<tr>
<td>Mac Aging</td>
<td>Indicates whether the MAC aging process is enabled.</td>
</tr>
<tr>
<td>Relearn Only</td>
<td>Displays, that when enabled, either the FDB table of this service is full, or that the maximum system-wide number of MA's supported by the agent has been reached, and thus MAC learning is temporary disabled, and only MAC re-learns can take place.</td>
</tr>
<tr>
<td>Mac Subnet Len</td>
<td>Displays the number of bits to be considered when performing MAC-learning or MAC-switching.</td>
</tr>
<tr>
<td>Source-Identifier</td>
<td>The location where the MAC is defined.</td>
</tr>
<tr>
<td>Type/Age</td>
<td>Type — Specifies the number of seconds used to age out TLS FDB entries learned on local SAPs.</td>
</tr>
<tr>
<td></td>
<td>L — Learned - Dynamic entries created by the learning process.</td>
</tr>
<tr>
<td></td>
<td>OAM — Entries created by the OAM process.</td>
</tr>
<tr>
<td></td>
<td>Static — Statically configured.</td>
</tr>
<tr>
<td>Last Change</td>
<td>Indicates the time of the most recent state changes.</td>
</tr>
</tbody>
</table>

Sample Output
### isid-using

**Syntax**  
isid-using [ISID]

**Context**  
show>service

**Description**  
This command displays services using an ISID.

**Parameters**  
ISID — Specifies a 24 bit (0..16777215) service instance identifier for this service. As part of the Provider Backbone Bridging frames, it is used at the destination PE as a demultiplexor field.

**Values**  
0 — 16777215

**Output**  
*A:SetupCLI# show service isid-using

=================================================================
Services

<table>
<thead>
<tr>
<th>SvcId</th>
<th>ISID</th>
<th>Type</th>
<th>b-Vpls</th>
<th>Adm</th>
<th>Opr</th>
<th>SvcMtu</th>
<th>CustId</th>
</tr>
</thead>
<tbody>
<tr>
<td>2001</td>
<td>122</td>
<td>i-VPLS</td>
<td>2002</td>
<td>Up</td>
<td>Down</td>
<td>1514</td>
<td>1</td>
</tr>
<tr>
<td>2005</td>
<td>2005</td>
<td>i-mVP*</td>
<td>2004</td>
<td>Down</td>
<td>Down</td>
<td>1500</td>
<td>1</td>
</tr>
</tbody>
</table>

Matching Services : 2

*A:SetupCLI#

A:term17# show service isid-using

=================================================================
Services

<table>
<thead>
<tr>
<th>SvcId</th>
<th>ISID</th>
<th>Type</th>
<th>b-Vpls</th>
<th>Adm</th>
<th>Opr</th>
<th>SvcMtu</th>
<th>CustId</th>
</tr>
</thead>
<tbody>
<tr>
<td>2000</td>
<td>0</td>
<td>b-VPLS</td>
<td>0</td>
<td>Up</td>
<td>Up</td>
<td>1530</td>
<td>1</td>
</tr>
<tr>
<td>2110</td>
<td>123</td>
<td>i-VPLS</td>
<td>2000</td>
<td>Up</td>
<td>Up</td>
<td>1514</td>
<td>1</td>
</tr>
<tr>
<td>2299</td>
<td>0</td>
<td>b-VPLS</td>
<td>0</td>
<td>Down</td>
<td>Down</td>
<td>1514</td>
<td>1</td>
</tr>
</tbody>
</table>

Matching Services : 3

A:term17#

### labels

**Syntax**  
labels

**Context**  
show>service>id

**Description**  
This command displays the labels being used by the service.

**Output**  
**Show Service-ID Labels** — The following table describes show service-id labels output fields:

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Svc Id</td>
<td>The service identifier.</td>
</tr>
<tr>
<td>Sdp Id</td>
<td>The SDP identifier.</td>
</tr>
<tr>
<td>Label</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td>Type</td>
<td>Indicates whether the SDP is spoke.</td>
</tr>
<tr>
<td>I. Lbl</td>
<td>The VC label used by the far-end device to send packets to this device in this service by the SDP.</td>
</tr>
<tr>
<td>E. Lbl</td>
<td>The VC label used by this device to send packets to the far-end device in this service by the SDP.</td>
</tr>
</tbody>
</table>

**Sample Output**

*A:ALA-12# show service id 1 labels*

```
==============================================================================
Martini Service Labels
==============================================================================
Svc Id  Sdp Id     Type I.Lbl    E.Lbl
---------------------------------------------------------------
 1       10:1          Mesh 0       0
 1       20:1          Mesh 0       0
 1       30:1          Mesh 0       0
 1       40:1          Mesh 130081  131061
 1       60:1          Mesh 131019  131016
 1       100:1         Mesh 0       0
---------------------------------------------------------------
Number of Bound SDPs : 6
```

*A:ALA-12#*
l2pt

Syntax
l2pt disabled
l2pt [detail]

Context
show>service>id

Description
This command displays Layer 2 Protocol Tunnel (L2-PT) route information associated with this service.

Parameters
disabled — Displays only entries with termination disabled. This helps identify configuration errors.
detail — Displays detailed information.

Output
Show L2PT Fields — The following table describes show L2PT output fields:

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service id</td>
<td>Displays the 24 bit (0..16777215) service instance identifier for the service.</td>
</tr>
<tr>
<td>L2pt-term enabled</td>
<td>Indicates if L2-PT-termination and/or Bpdu-translation is in use in this service by at least one SAP or spoke SDP binding. If in use, at least one of L2PT-termination or Bpdu-translation is enabled. When enabled it is not possible to enable STP on this service.</td>
</tr>
<tr>
<td>L2pt-term disabled</td>
<td>Indicates that L2-PT-termination is disabled.</td>
</tr>
<tr>
<td>Bpdu-trans auto</td>
<td>Specifies the number of L2-PT PDU's are translated before being sent out on a port or sap.</td>
</tr>
<tr>
<td>Bpdu-trans disabled</td>
<td>Indicates that Bpdu-translation is disabled.</td>
</tr>
<tr>
<td>SAPs</td>
<td>Displays the number of SAPs with L2PT or BPDU translation enabled or disabled.</td>
</tr>
<tr>
<td>SDPs</td>
<td>Displays the number of SDPs with L2PT or BPDU translation enabled or disabled.</td>
</tr>
<tr>
<td>Total</td>
<td>Displays the column totals of L2PT entities.</td>
</tr>
<tr>
<td>SapId</td>
<td>The ID of the access point where this SAP is defined.</td>
</tr>
<tr>
<td>L2pt-termination</td>
<td>Indicates whether L2pt termination is enabled or disabled.</td>
</tr>
<tr>
<td>Admin Bpdu-translation</td>
<td>Specifies whether Bpdu translation is administratively enabled or disabled.</td>
</tr>
<tr>
<td>Oper Bpdu-translation</td>
<td>Specifies whether Bpdu translation is operationally enabled or disabled.</td>
</tr>
<tr>
<td>SdpId</td>
<td>Specifies the SAP ID.</td>
</tr>
</tbody>
</table>

A:ALA-48>show>service>id# l2pt
### L2pt summary, Service id 700

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP’s</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>SDP’s</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Total</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

A:ALA-48>show>service>id#

A:ALA-48>show>service>id# l2pt disabled

L2pt details, Service id 700

Service Access Points

<table>
<thead>
<tr>
<th>SapId</th>
<th>L2pt-termination</th>
<th>Admin Bpdu-translation</th>
<th>Oper Bpdu-translation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1/9:0</td>
<td>disabled</td>
<td>disabled</td>
<td>disabled</td>
</tr>
</tbody>
</table>

Number of SAPs : 1

Service Destination Points

<table>
<thead>
<tr>
<th>SdpId</th>
<th>L2pt-termination</th>
<th>Admin Bpdu-translation</th>
<th>Oper Bpdu-translation</th>
</tr>
</thead>
<tbody>
<tr>
<td>2:222</td>
<td>disabled</td>
<td>disabled</td>
<td>disabled</td>
</tr>
</tbody>
</table>

Number of SDPs : 1

L2pt summary, Service id 700

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP’s</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>SDP’s</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Total</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

A:ALA-48>show>service>id#

A:ALA-48>show>service>id# l2pt detail

L2pt details, Service id 700

Service Access Points

<table>
<thead>
<tr>
<th>SapId</th>
<th>L2pt-termination</th>
<th>Admin Bpdu-translation</th>
<th>Oper Bpdu-translation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1/9:0</td>
<td>disabled</td>
<td>disabled</td>
<td>disabled</td>
</tr>
</tbody>
</table>

Number of SAPs : 1
## VPLS Show Commands

### Service Destination Points

<table>
<thead>
<tr>
<th>SdpId</th>
<th>L2pt-termination</th>
<th>Admin Bpdu-translation</th>
<th>Oper Bpdu-translation</th>
</tr>
</thead>
<tbody>
<tr>
<td>2:222</td>
<td>disabled</td>
<td>disabled</td>
<td>disabled</td>
</tr>
</tbody>
</table>

Number of SDPs: 1

### L2pt summary, Service id 700

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>enabled</td>
<td>disabled</td>
<td>auto</td>
<td>disabled</td>
<td>pvst</td>
<td>stp</td>
</tr>
</tbody>
</table>

| SAP's | 0 | 1 | 0 | 1 | 0 | 0 |
| SDP's | 0 | 1 | 0 | 1 | 0 | 0 |

Total 0 2 0 2 0 0

### mac-move

**Syntax**

`mac-move`

**Context**

`show>service>id`

**Description**

This command displays MAC move related information about the service.

**Sample Output**

```
*A:ALA-2009>config>service>vpls>mac-move# show service id 500 mac-move

Service Id Mac Move Information
-----------------------------------------------
<table>
<thead>
<tr>
<th>Service Id</th>
<th>Mac Move</th>
</tr>
</thead>
<tbody>
<tr>
<td>500</td>
<td>Enabled</td>
</tr>
<tr>
<td>Primary Factor</td>
<td>4</td>
</tr>
<tr>
<td>Secondary Factor</td>
<td>2</td>
</tr>
<tr>
<td>Mac Move Rate</td>
<td>2</td>
</tr>
<tr>
<td>Mac Move Retries</td>
<td>3</td>
</tr>
</tbody>
</table>

SAP Mac Move Information: 2/1/3:501
-----------------------------------------------
<table>
<thead>
<tr>
<th>Admin State</th>
<th>Oper State</th>
<th>Flags</th>
<th>Time to come up</th>
<th>Retries Left</th>
<th>Mac Move</th>
<th>Blockable Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Up</td>
<td>Down</td>
<td>RelearnLimitExceeded</td>
<td>1 seconds</td>
<td>1</td>
<td>Blockable</td>
<td>Tertiary</td>
</tr>
</tbody>
</table>

SDP Mac Move Information: 21:501
-----------------------------------------------
<table>
<thead>
<tr>
<th>Admin State</th>
<th>Oper State</th>
<th>Flags</th>
<th>Time to RetryReset</th>
<th>Retries Left</th>
<th>Mac Move</th>
<th>Blockable Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Up</td>
<td>Up</td>
<td>None</td>
<td>267 seconds</td>
<td>none</td>
<td>Blockable</td>
<td>Tertiary</td>
</tr>
</tbody>
</table>
```

*A:ALA-48>show>service>id#*
Show, Clear, Debug Commands

Flags : None
Time to RetryReset: never Retries Left : 3
Mac Move : Blockable Blockable Level : Secondary
-----------------------------------------------------------------------------------------------
SDP Mac Move Information: 21:502
-----------------------------------------------------------------------------------------------
Admin State : Up Oper State : Down
Flags : RelearnLimitExceeded
Time to come up : never Retries Left : none
Mac Move : Blockable Blockable Level : Tertiary
-----------------------------------------------------------------------------------------------
*A:ALA-2009>config>service>vpls>mac-move#

mac-protect

Syntax  mac-protect
Context  show>service>id
Description  This command displays MAC protect-related information about the service.

Output
*A:ALA-48>show>service>id# mac-protect
Protected MACs, Service 700
ServId  MAC  Source-Identifier  Type/Age  Last Change
-------------------------------------------------------------------------------
700    ff:ff:ff:ff:ff:ff not learned  n/a  n/a
-------------------------------------------------------------------------------
No. of MAC Entries: 1
*A:ALA-48>show>service>id# mac-protect

mroutes

Syntax  mroutes [detail]
Context  show>service>id>mld-snooping
Description  This command displays all multicast routers.

provider-tunnel

Syntax  provider-tunnel
Description  This command displays the service provider tunnel information.

Output
*A:Dut-B# show service id 1 provider-tunnel
Service Provider Tunnel Information
-----------------------------------------------------------------------------------------------
Type : inclusive  Root and Leaf : enabled
-----------------------------------------------------------------------------------------------
VPLS Show Commands

Admin State : inService          Data Delay Intvl : 3 secs
PMSI Type    : ldp                LSP Template       :
Remain Delay Intvl : 0 secs     LSP Name used : 8193

-----------------------------------------------
*A:Dut=B# /tools dump service id 1 provider-tunnels type originating

-----------------------------------------------
VPLS 1 Inclusive Provider Tunnels Originating
-----------------------------------------------
ipmsi (LDP)                                  P2MP-ID Root-Addr
-----------------------------------------------
                      8193    8193    10.20.1.2

-----------------------------------------------
*A:Dut-B# /tools dump service id 1 provider-tunnels type terminating

-----------------------------------------------
VPLS 1 Inclusive Provider Tunnels Terminating
-----------------------------------------------
ipmsi (LDP)                                  P2MP-ID Root-Addr
-----------------------------------------------
                      8193    8193    10.20.1.3
                      8193    8193    10.20.1.4
                      8193    8193    10.20.1.6
                      8193    8193    10.20.1.7

-----------------------------------------------
*A:Dut-B# /tools dump service id 1 provider-tunnels

-----------------------------------------------
VPLS 1 Inclusive Provider Tunnels Originating
-----------------------------------------------
ipmsi (LDP)                                  P2MP-ID Root-Addr
-----------------------------------------------
                      8193    8193    10.20.1.2

-----------------------------------------------
VPLS 1 Inclusive Provider Tunnels Terminating
-----------------------------------------------
ipmsi (LDP)                                  P2MP-ID Root-Addr
-----------------------------------------------
                      8193    8193    10.20.1.3
                      8193    8193    10.20.1.4
                      8193    8193    10.20.1.6
                      8193    8193    10.20.1.7

-----------------------------------------------

Provider-tunnel

Syntax  provider-tunnel
Context  show>service>id
Description  This command displays provider tunnel information.
Sample Output

*A:Dut-B# show service id 1 provider-tunnel

Service Provider Tunnel Information

Type : inclusive  Root and Leaf : enabled
Admin State : inService  Data Delay Intvl : 3 secs
PMSI Type : ldp  LSP Template :
Remain Delay Intvl : 0 secs  LSP Name used : 8193

*A:Dut-B# /tools dump service id 1 provider-tunnels type originating

VPLS 1 Inclusive Provider Tunnels Originating

ipmsi (LDP)
P2MP-ID  Root-Addr
8193  8193  10.20.1.2

*A:Dut-B# /tools dump service id 1 provider-tunnels type terminating

VPLS 1 Inclusive Provider Tunnels Terminating

ipmsi (LDP)
P2MP-ID  Root-Addr
8193  8193  10.20.1.3
8193  10.20.1.4
8193  10.20.1.6
8193  10.20.1.7

*A:Dut-C# show service id 1001 provider-tunnel

Service Provider Tunnel Information

Type : inclusive  Root and Leaf : enabled
Admin State : inService  Data Delay Intvl : 3 secs
PMSI Type : rsvp  LSP Template : ipmsi
Remain Delay Intvl : 0 secs  LSP Name used : ipmsi-1001-73728

proxy-arp

Syntax  proxy-arp [ip-address ip-address]

Context  show>service>id
Description

This command displays the proxy-ARP entries existing for a particular service. This table is populated by the EVPN mac routes containing a MAC and an IP address. A 7x50 receiving an ARP request from a SAP or SDP-binding will perform a lookup in the proxy-arp table for the service. If the 7x50 finds a match, it will reply to the ARP and will not let the ARP be flooded in the VPLS service. If the 7x50 does not find a match, the ARP will be flooded within the service. The command allows for an specific IP addresses to be shown.

Output

Sample Output

*A:DutA# show service id 1 proxy-arp

VPLS Proxy Arp Table

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Mac Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.10.10.69</td>
<td>00:de:fe:ca:da:00</td>
</tr>
<tr>
<td>20.0.0.1</td>
<td>00:de:fe:ca:da:00</td>
</tr>
<tr>
<td>20.0.1.1</td>
<td>00:de:fe:ca:da:00</td>
</tr>
</tbody>
</table>

Number of entries : 3

vxlan

Syntax

vxlan

Context

show>service>id
show>service

Description

This command displays the VXLAN bindings auto-created in a given service. A VXLAN binding is composed of the remote VTEP (VXLAN Termination Endpoint) and the corresponding egress VNI (VXLAN Network Identifier) to identify the service at the egress node. The command shows the number of MACs associated to each binding as well as the operational status if the binding is part of the multicast list. The binding will be operationally down when the VTEP address is not found in the base routing table (the VTEP address cannot be reached). A binding will be part of the multicast list if a valid BGP EVPN inclusive multicast route exists for it.

Output

Sample Output

*A:DutA# show service id 1 vxlan

VPLS VXLAN, Ingress VXLAN Network Id: 1

<table>
<thead>
<tr>
<th>Egress VTEP, VNI</th>
</tr>
</thead>
<tbody>
<tr>
<td>VTEP Address</td>
</tr>
<tr>
<td>------------------</td>
</tr>
<tr>
<td>192.0.0.71</td>
</tr>
<tr>
<td>192.0.0.72</td>
</tr>
<tr>
<td>192.0.0.74</td>
</tr>
</tbody>
</table>
Show, Clear, Debug Commands

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>Yes</th>
<th>Down</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.0.0.76</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>192.168.45.2</td>
<td>1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Number of Egress VTEP, VNI : 5

A:DutB# show service vxlan
<vtep>
  192.0.2.65  192.0.2.66

A:PE63# show service vxlan 192.0.2.65

VXLAN Tunnel Endpoint: 192.0.2.65

Egress VNI        Service Id        Oper State
--------------------------------------------
60                  60                    Up
**sap**

**Syntax**

```
sap sap-id [filter]
```

**Context**

```
show>service>id
```

**Description**

This command displays information for the SAPs associated with the service. If no optional parameters are specified, a summary of all associated SAPs is displayed.

**Parameters**

- `sap sap-id` — The ID that displays SAPs for the service in the `slot/mda/port[.channel]` form. See Common CLI Command Descriptions on page 1783 for command syntax.
- `detail` — Displays detailed information for the SAP.

**Output**

**Show Service-ID SAP** — The following table describes show service SAP fields:

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Id</td>
<td>The service identifier.</td>
</tr>
<tr>
<td>SAP</td>
<td>The SAP and qtag.</td>
</tr>
<tr>
<td>Encap</td>
<td>The encapsulation type of the SAP.</td>
</tr>
<tr>
<td>Ethertype</td>
<td>Specifies an Ethernet type II Ethertype value.</td>
</tr>
<tr>
<td>Admin State</td>
<td>The administrative state of the SAP.</td>
</tr>
<tr>
<td>Oper State</td>
<td>The operational state of the SAP.</td>
</tr>
<tr>
<td>Flags</td>
<td>Specifies the conditions that affect the operating status of this SAP.</td>
</tr>
<tr>
<td></td>
<td>Display output includes: ServiceAdminDown, SapAdminDown, InterfaceAdminDown,</td>
</tr>
<tr>
<td></td>
<td>PortOperDown, L2OperDown, RelearnLimitExceeded, ParentIfAdminDown,</td>
</tr>
<tr>
<td></td>
<td>NoSapIpipeCelpAddr, TodResourceUnavail, TodMssResourceUnavail, SapParamMismatch,</td>
</tr>
<tr>
<td></td>
<td>CemSapNoEcidOrMacAddr, StandByForMcRing, SapIngressNamedPoolMismatch, SapEgressNamedPoolMismatch,</td>
</tr>
<tr>
<td></td>
<td>NoSapEpipeRingNode.</td>
</tr>
<tr>
<td>Last Status Change</td>
<td>Specifies the time of the most recent operating status change to this</td>
</tr>
<tr>
<td></td>
<td>SAP.</td>
</tr>
<tr>
<td>Last Mgmt Change</td>
<td>Specifies the time of the most recent management-initiated change to</td>
</tr>
<tr>
<td></td>
<td>this SAP.</td>
</tr>
<tr>
<td>Oper MTU</td>
<td>The actual largest service frame size (in octets) that can be transmitted</td>
</tr>
<tr>
<td></td>
<td>through the SAP to the far-end router, without requiring the packet to</td>
</tr>
<tr>
<td></td>
<td>be fragmented.</td>
</tr>
<tr>
<td>Ingress qos-policy</td>
<td>The ingress QoS policy ID assigned to the SAP.</td>
</tr>
<tr>
<td>Egress qos-policy</td>
<td>The egress QoS policy ID assigned to the SAP.</td>
</tr>
<tr>
<td>Label</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Ingress Filter-Id</td>
<td>The ingress filter policy ID assigned to the SAP.</td>
</tr>
<tr>
<td>Egress Filter-Id</td>
<td>The egress filter policy ID assigned to the SAP.</td>
</tr>
<tr>
<td>Acct. Pol</td>
<td>The accounting policy ID assigned to the SAP.</td>
</tr>
<tr>
<td>Collect Stats</td>
<td>Specifies whether collect stats is enabled.</td>
</tr>
<tr>
<td>Forwarding Engine Stats</td>
<td></td>
</tr>
<tr>
<td>Dropped</td>
<td>The number of packets and octets dropped due to SAP state, ingress MAC or IP filter, same segment discard, bad checksum, etc.</td>
</tr>
<tr>
<td>Off. HiPrio</td>
<td>The number of high priority packets and octets, as determined by the SAP ingress QoS policy.</td>
</tr>
<tr>
<td>Off. LowPrio</td>
<td>The number of low priority packets and octets, as determined by the SAP ingress QoS policy.</td>
</tr>
<tr>
<td>Off. Uncolor</td>
<td>The number of uncolored packets and octets, as determined by the SAP ingress QoS policy.</td>
</tr>
<tr>
<td>Queueing Stats (Ingress QoS Policy)</td>
<td></td>
</tr>
<tr>
<td>Dro. HiPrio</td>
<td>The number of high priority packets and octets, as determined by the SAP ingress QoS policy, dropped due to: MBS exceeded, buffer pool limit exceeded, etc.</td>
</tr>
<tr>
<td>Dro. LowPrio</td>
<td>The number of low priority packets and octets, as determined by the SAP ingress QoS policy, dropped due to: MBS exceeded, buffer pool limit exceeded, etc.</td>
</tr>
<tr>
<td>For. InProf</td>
<td>The number of in-profile packets and octets (rate below CIR) forwarded.</td>
</tr>
<tr>
<td>For. OutProf</td>
<td>The number of out-of-profile packets and octets discarded due to MBS exceeded, buffer pool limit exceeded, etc.</td>
</tr>
<tr>
<td>Queueing Stats (Egress QoS Policy)</td>
<td></td>
</tr>
<tr>
<td>Dro. InProf</td>
<td>The number of in-profile packets and octets discarded due to MBS exceeded, buffer pool limit exceeded, etc.</td>
</tr>
<tr>
<td>Dro. OutProf</td>
<td>The number of out-of-profile packets and octets due to MBS exceeded, buffer pool limit exceeded, etc.</td>
</tr>
<tr>
<td>For. InProf</td>
<td>The number of in-profile packets and octets (rate below CIR) forwarded.</td>
</tr>
<tr>
<td>For. OutProf</td>
<td>The number of out-of-profile packets and octets (rate above CIR) forwarded.</td>
</tr>
<tr>
<td>Ingress TD Profile</td>
<td>The profile ID applied to the ingress SAP.</td>
</tr>
<tr>
<td>Egress TD Profile</td>
<td>The profile ID applied to the egress SAP.</td>
</tr>
</tbody>
</table>
Sample Output

sdp

Syntax

sdp  sdp-id:vc-id {mrp}
sdp  [sdp-id | far-end ip-addr] [detail]

Context

show>service>id

Description

This command displays information for the SDPs associated with the service. If no optional parameters are specified, a summary of all associated SDPs is displayed.

Parameters

sdp-id — Displays only information for the specified SDP ID.
  Default All SDPs
  Values 1 — 17407

far-end ip-addr — Displays only SDPs matching with the specified far-end IP address.
  Default SDPs with any far-end IP address.

detail — Displays detailed SDP information.

Output

Show Service-ID SDP — The following table describes show service-id SDP output fields.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sdp Id</td>
<td>The SDP identifier.</td>
</tr>
<tr>
<td>Type</td>
<td>Indicates whether the SDP is spoke.</td>
</tr>
<tr>
<td>Split Horizon Group</td>
<td>Indicates the name of the split horizon group that the SDP belongs to.</td>
</tr>
<tr>
<td>VC Type</td>
<td>Displays the VC type: ether, vlan, or vpls.</td>
</tr>
<tr>
<td>VC Tag</td>
<td>Displays the explicit dot1Q value used when encapsulating to the SDP far end.</td>
</tr>
<tr>
<td>I. Lbl</td>
<td>The VC label used by the far-end device to send packets to this device in this service by the SDP.</td>
</tr>
<tr>
<td>Admin Path MTU</td>
<td>The operating path MTU of the SDP is equal to the admin path MTU (when one is set) or the dynamically computed tunnel MTU, when no admin path MTU is set (the default case.)</td>
</tr>
</tbody>
</table>
### Table of SDP Label and Description

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oper Path MTU</td>
<td>The actual largest service frame size (in octets) that can be transmitted through this SDP to the far-end router, without requiring the packet to be fragmented.</td>
</tr>
<tr>
<td>Far End</td>
<td>Specifies the IP address of the remote end of the GRE or MPLS tunnel defined by this SDP.</td>
</tr>
<tr>
<td>Delivery</td>
<td>Specifies the type of delivery used by the SDP: GRE or MPLS.</td>
</tr>
<tr>
<td>Admin State</td>
<td>The administrative state of this SDP.</td>
</tr>
<tr>
<td>Oper State</td>
<td>The current status of the SDP.</td>
</tr>
<tr>
<td>Ingress Label</td>
<td>The label used by the far-end device to send packets to this device in this service by this SDP.</td>
</tr>
<tr>
<td>Egress Label</td>
<td>The label used by this device to send packets to the far-end device in this service by the SDP.</td>
</tr>
<tr>
<td>Last Changed</td>
<td>The date and time of the most recent change to the SDP.</td>
</tr>
<tr>
<td>Signaling</td>
<td>Specifies the signaling protocol used to obtain the ingress and egress labels used in frames transmitted and received on this SDP.</td>
</tr>
<tr>
<td>Admin State</td>
<td>The administrative state of the Keepalive process.</td>
</tr>
<tr>
<td>Oper State</td>
<td>The operational state of the Keepalive process.</td>
</tr>
<tr>
<td>Hello Time</td>
<td>Specifies how often the SDP echo request messages are transmitted on this SDP.</td>
</tr>
<tr>
<td>Max Drop Count</td>
<td>Specifies the maximum number of consecutive SDP Echo Request messages that can be unacknowledged before the keepalive protocol reports a fault.</td>
</tr>
<tr>
<td>Hello Msg Len</td>
<td>Specifies the length of the SDP echo request messages transmitted on this SDP.</td>
</tr>
<tr>
<td>Hold Down Time</td>
<td>Specifies the amount of time to wait before the Keepalive operating status is eligible to enter the alive state.</td>
</tr>
<tr>
<td>I. Fwd. Pkts.</td>
<td>Specifies the number of forwarded ingress packets.</td>
</tr>
<tr>
<td>I. Dro. Pkts</td>
<td>Specifies the number of dropped ingress packets.</td>
</tr>
<tr>
<td>E. Fwd. Pkts.</td>
<td>Specifies the number of forwarded egress packets.</td>
</tr>
<tr>
<td>E. Fwd. Octets</td>
<td>Specifies the number of forwarded egress octets.</td>
</tr>
<tr>
<td>Associated LSP List</td>
<td>When the SDP type is MPLS, a list of LSPs used to reach the far-end router displays. All the LSPs in the list must terminate at the IP address specified in the far end field. If the SDP type is GRE, then the following message displays: SDP delivery mechanism is not MPLS</td>
</tr>
</tbody>
</table>
Sample Output

*A:Dut-C# show service id 1001 sdp 17407:4294967295 detail
========================================================================
Service Destination Point (Sdp Id : 17407:4294967295) Details
========================================================================

Sdp Id 17407:4294967295 -(0.0.0.0)

Description     : (Not Specified)
SDP Id             : 17407:4294967295         Type            : VplsPmsi
Split Horiz Grp    : (Not Specified)
VC Type            : Ether                    VC Tag            : n/a
Admin Path MTU     : 9194                     Oper Path MTU     : 9194
Far End            : not applicable           Delivery          : MPLS
Tunnel Far End     : n/a                    LSP Types         : None
Hash Label         : Disabled               Hash Lbl Sig Cap  : Disabled
Oper Hash Label    : Disabled
Admin State        : Up                     Oper State        : Up
Acct. Pol          : None                   Collect Stats     : Disabled
Ingress Label      : 0                        Egress Label      : 3
Ingr Mac Fltr-Id   : n/a                      Egr Mac Fltr-Id   : n/a

Peer Pw Bits

Indicates the bits set by the LDP peer when there is a fault on its side of the pseudowire. LAC failures occur on the SAP that has been configured on the pipe service, PSN bits are set by SDP-binding failures on the pipe service. The pwNotForwarding bit is set when none of the above failures apply, such as an MTU mismatch failure. This value is only applicable if the peer is using the pseudowire status signalling method to indicate faults.

pwNotForwarding — Pseudowire not forwarding
lacIngressFault Local — Attachment circuit RX fault
lacEgressFault Local — Attachment circuit TX fault
psnIngressFault Local — PSN-facing PW RX fault
psnEgressFault Local — PSN-facing PW TX fault
pwFwdingStandby — Pseudowire in standby mode
Ingr IP Fltr-Id : n/a    Egr IP Fltr-Id : n/a
Ingr IPv6 Fltr-Id : n/a   Egr IPv6 Fltr-Id : n/a
Admin ControlWord : Not Preferred  Oper ControlWord : False
Last Status Change : 01/31/2012 00:51:46  Signaling : None
Last Mgmt Change : 01/31/2012 00:49:58  Force Vlan-Vc : Disabled
Endpoint : N/A  Precedence : 4
FW Status Sig : Enabled
Class Fwding State : Down
Flags : None
Time to RetryReset : never  Retries Left : 3
Mac Move : Blockable  Blockable Level : Tertiary
Local Pw Bits : None
Peer Pw Bits : None
Peer Fault Ip : None
Application Profile: None
Max Nbr of MAC Addr: No Limit  Total MAC Addr : 0
Learned MAC Addr : 0  Static MAC Addr : 0
MAC Learning : Enabled  Discard Unkwn Srce: Disabled
MAC Aging : Enabled
BPDU Translation : Disabled
L2PT Termination : Disabled
MAC Pinning : Disabled
Ignore Standby Sig : False  Block On Mesh Fail: False
Oper Group : (none)  Monitor Oper Grp : (none)
Rest Prot Src Mac : Disabled
Auto Learn Mac Prot: Disabled  RestProtSrcMacAct : Disable
Ingress Qos Policy : (none)  Egress Qos Policy : (none)
Ingress FP QGrp : (none)  Egress Port QGrp : (none)
Ing FP QGrp Inst : (none)  Egr Port QGrp Inst: (none)

------------------------------------------------------------------------
ETH-CFM SDP-Bind specifics
------------------------------------------------------------------------
V-MEP Filtering : Disabled
KeepAlive Information :
<table>
<thead>
<tr>
<th>Admin State</th>
<th>Oper State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disabled</td>
<td>Disabled</td>
</tr>
<tr>
<td>Hello Time</td>
<td>Hello Msg Len</td>
</tr>
<tr>
<td>10</td>
<td>0</td>
</tr>
<tr>
<td>Max Drop Count</td>
<td>Hold Down Time</td>
</tr>
<tr>
<td>3</td>
<td>10</td>
</tr>
</tbody>
</table>

Statistics :
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>E. Fwd. Pkts.</th>
<th>E. Fwd. Octets</th>
</tr>
</thead>
<tbody>
<tr>
<td>5937639</td>
<td>356258340</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>MCAC Policy Name</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>MCAC Max Unconst BW: no limit</th>
<th>MCAC Max Mand BW : no limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>MCAC In use Mand BW: 0</td>
<td>MCAC Avail Mand BW: unlimited</td>
</tr>
<tr>
<td>MCAC In use Opnl BW: 0</td>
<td>MCAC Avail Opnl BW: unlimited</td>
</tr>
</tbody>
</table>

------------------------------------------------------------------------
RSVP/Static LSPs
------------------------------------------------------------------------
Associated LSP List :
No LSPs Associated

------------------------------------------------------------------------
Class-based forwarding :
------------------------------------------------------------------------
Class forwarding : Disabled
EnforceDSTELspFc : Disabled
Default LSP : Uknwn
Multicast LSP : None

FC Mapping Table
Show, Clear, Debug Commands

---------------------------------------------------------------
FC Name    LSP Name
---------------------------------------------------------------
No FC Mappings

---------------------------------------------------------------
Stp Service Destination Point specifics

---------------------------------------------------------------
Stp Admin State  : Down                Stp Oper State  : Down
Core Connectivity: Down
Port Role       : N/A                    Port State     : Forwarding
Port Number     : 0                    Port Priority : 128
Port Path Cost  : 10                    Auto Edge    : Enabled
Admin Edge      : Disabled                Oper Edge    : N/A
Link Type       : Pt-pt                  BPDU Encap    : Dot1d
Root Guard      : Disabled                Active Protocol: N/A
Last BPDU from  : N/A                    Designated Bridge: N/A
Designated Port Id: N/A
Fwd Transitions: 0                        Bad BPDU rcvd : 0
Cfg BPDU rcvd   : 0                        Cfg BPDU tx  : 0
TCN BPDU rcvd   : 0                        TCN BPDU tx : 0
TC bit BPDU rcvd: 0                        TC bit BPDU tx : 0
RST BPDU rcvd   : 0                        RST BPDU tx  : 0

---------------------------------------------------------------
Number of SDPs : 1

---------------------------------------------------------------
A:Dut-A# show service id 1 sdp detail

Services: Service Destination Points Details

Sdp Id 1:1  -(10.20.1.2)
### VPLS Show Commands

<table>
<thead>
<tr>
<th>Description</th>
<th>Default sdp description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SDP Id</td>
<td>1:1</td>
</tr>
<tr>
<td>Type</td>
<td>Spoke</td>
</tr>
<tr>
<td>VC Type</td>
<td>Ether</td>
</tr>
<tr>
<td>VC Tag</td>
<td>n/a</td>
</tr>
<tr>
<td>Admin Path MTU</td>
<td>0</td>
</tr>
<tr>
<td>Oper Path MTU</td>
<td>9186</td>
</tr>
<tr>
<td>Far End</td>
<td>10.20.1.2</td>
</tr>
<tr>
<td>Delivery</td>
<td>MPLS</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Admin State</th>
<th>Up</th>
<th>Oper State</th>
<th>Up</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acct. Pol</td>
<td>None</td>
<td>Collect Stats</td>
<td>Disabled</td>
</tr>
<tr>
<td>Ingress Label</td>
<td>2048</td>
<td>Egress Label</td>
<td>2048</td>
</tr>
<tr>
<td>Ingress mac Fltr</td>
<td>n/a</td>
<td>Egress mac Fltr</td>
<td>n/a</td>
</tr>
<tr>
<td>Ingress ip Fltr</td>
<td>n/a</td>
<td>Egress ip Fltr</td>
<td>n/a</td>
</tr>
<tr>
<td>Ingress ipv6 Fltr</td>
<td>n/a</td>
<td>Egress ipv6 Fltr</td>
<td>n/a</td>
</tr>
<tr>
<td>Admin ControlWord</td>
<td>Not Preferred</td>
<td>Oper ControlWord</td>
<td>False</td>
</tr>
<tr>
<td>Last Status Change</td>
<td>05/31/2007 00:45:43</td>
<td>Signaling</td>
<td>None</td>
</tr>
<tr>
<td>Last Mgmt Change</td>
<td>05/31/2007 00:45:43</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Class Fwding State</td>
<td>Up</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Flags</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Peer Pw Bits</td>
<td>None</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Peer Fault Ip</td>
<td>None</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Peer Vccv CV Bits</td>
<td>None</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Peer Vccv CC Bits</td>
<td>None</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Max Nbr of MAC Addr</td>
<td>No Limit</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Learned MAC Addr</td>
<td>0</td>
<td>Total MAC Addr</td>
<td>0</td>
</tr>
<tr>
<td>MAC Learning</td>
<td>Enabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MAC Aging</td>
<td>Enabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td>L2PT Termination</td>
<td>Disabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MAC Pinning</td>
<td>Disabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td>KeepAlive Information</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Admin State</td>
<td>Disabled</td>
<td>Oper State</td>
<td>Disabled</td>
</tr>
<tr>
<td>Hello Time</td>
<td>10</td>
<td>Hello Msg Len</td>
<td>0</td>
</tr>
<tr>
<td>Max Drop Count</td>
<td>3</td>
<td>Hold Down Time</td>
<td>10</td>
</tr>
<tr>
<td>Statistics</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>I. Fwd. Pkts.</td>
<td>0</td>
<td>I. Dro. Pkts.</td>
<td>0</td>
</tr>
<tr>
<td>I. Fwd. Octs.</td>
<td>0</td>
<td>I. Dro. Octs.</td>
<td>0</td>
</tr>
<tr>
<td>E. Fwd. Pkts.</td>
<td>0</td>
<td>E. Fwd. Octets</td>
<td>0</td>
</tr>
<tr>
<td>MCAC Policy Name</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MCAC Max Unconst BW</td>
<td>no limit</td>
<td>MCAC Max Mand BW</td>
<td>no limit</td>
</tr>
<tr>
<td>MCAC In use Mand BW</td>
<td>0</td>
<td>MCAC Avail Mand BW</td>
<td>unlimited</td>
</tr>
<tr>
<td>MCAC In use Opnl BW</td>
<td>0</td>
<td>MCAC Avail Opnl BW</td>
<td>unlimited</td>
</tr>
</tbody>
</table>

### Associated LSP LIST

<table>
<thead>
<tr>
<th>Lsp Name</th>
<th>A_B_1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin State</td>
<td>Up</td>
</tr>
<tr>
<td>Time Since Last Tr*: 00h26m35s</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Lsp Name</th>
<th>A_B_2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin State</td>
<td>Up</td>
</tr>
<tr>
<td>Time Since Last Tr*: 00h26m35s</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Lsp Name</th>
<th>A_B_3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin State</td>
<td>Up</td>
</tr>
<tr>
<td>Time Since Last Tr*: 00h26m34s</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Lsp Name</th>
<th>A_B_4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin State</td>
<td>Up</td>
</tr>
<tr>
<td>Time Since Last Tr*: 00h26m34s</td>
<td></td>
</tr>
</tbody>
</table>
Lsp Name       : A_B_5  
Admin State    : Up   Oper State  : Up  
Time Since Last Tr*: 00h26m34s

Lsp Name       : A_B_6  
Admin State    : Up   Oper State  : Up  
Time Since Last Tr*: 00h26m34s

Lsp Name       : A_B_7  
Admin State    : Up   Oper State  : Up  
Time Since Last Tr*: 00h26m34s

Lsp Name       : A_B_8  
Admin State    : Up   Oper State  : Up  
Time Since Last Tr*: 00h26m34s

Class-based forwarding :
Class forwarding   : enabled  
Default LSP        : A_B_10  Multicast LSP     : A_B_9

FC Mapping Table
<table>
<thead>
<tr>
<th>FC Name</th>
<th>LSP Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>af</td>
<td>A_B_3</td>
</tr>
<tr>
<td>be</td>
<td>A_B_1</td>
</tr>
<tr>
<td>ef</td>
<td>A_B_6</td>
</tr>
<tr>
<td>h1</td>
<td>A_B_7</td>
</tr>
<tr>
<td>h2</td>
<td>A_B_5</td>
</tr>
<tr>
<td>l1</td>
<td>A_B_4</td>
</tr>
<tr>
<td>l2</td>
<td>A_B_2</td>
</tr>
<tr>
<td>nc</td>
<td>A_B_8</td>
</tr>
</tbody>
</table>

Stp Service Destination Point specifics
Mac Move       : Blockable  
Stp Admin State : Up   Stp Oper State : Down  
Core Connectivity : Down  
Port Role      : N/A   Port State  : Forwarding  
Port Number    : 2049  Port Priority : 128  
Port Path Cost : 10   Auto Edge  : Enabled  
Admin Edge     : Disabled  
Link Type      : Pt-pt  BPDU Encap  : Dot1d  
Root Guard     : Disabled  
Last BPDU from : N/A   Active Protocol  : N/A  
Designated Bridge : N/A   Designated Port Id: 0
Fwd Transitions : 0   Bad BPDUs rcvd : 0  
Cfg BPDUs rcvd  : 0   Cfg BPDUs tx  : 0  
TCN BPDUs rcvd  : 0   TCN BPDUs tx  : 0  
RST BPDUs rcvd  : 0   RST BPDUs tx  : 0
Number of SDPs : 1

* indicates that the corresponding row element may have been truncated.

---

A:Dut-A# show service id x all

---

SAP 1/1/4:500

---

<table>
<thead>
<tr>
<th>Service Id</th>
<th>Encap</th>
<th>Description</th>
<th>Admin State</th>
<th>Oper State</th>
<th>Flags</th>
<th>Multi Svc Site</th>
<th>Last Status Change</th>
<th>Last Mgmt Change</th>
<th>Sub Type</th>
<th>Dot1Q Ethertype</th>
<th>QinQ Ethertype</th>
<th>Split Horizon Group</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>500</td>
<td>q-tag</td>
<td>(Not Specified)</td>
<td>Up</td>
<td>Down</td>
<td>PortOperDown</td>
<td>None</td>
<td>09/19/2013 11:43:04</td>
<td>09/19/2013 11:43:05</td>
<td>regular</td>
<td>0x8100</td>
<td>0x8100</td>
<td>(Not Specified)</td>
</tr>
</tbody>
</table>

---

Admin MTU : 1518
Ingr IP Fltr-Id : n/a
Ingr Mac Fltr-Id : n/a
Ingr IPv6 Fltr-Id : n/a
tod-suite : None
Endpoin : N/A
Q Frame-Based Acct : Disabled
Vlan-translation : None
Acct. Pol : None
Application Profile : None
Transit Policy : None
Oper Group : (none)
Host Lockout Plcy : n/a
Ignore Oper Down : Disabled
Lag Link Map Prof : (none)
Cflowd : Disabled

---

ETH-CFM SAP specifics

---

Tunnel Faults : n/a
MC Prop-Hold-Timer : n/a
Squelch Levels : 0 1 2 3 4 5 6 7
AIS : Disabled

---

QOS

---

Ingress qos-policy : 1
Egress qos-policy : 1

---

Service Destination Points(SDPs)

---

Sdp Id 1:2 -(1.1.1.1)
<table>
<thead>
<tr>
<th>Description</th>
<th>(Not Specified)</th>
</tr>
</thead>
<tbody>
<tr>
<td>SDP Id</td>
<td>1:2</td>
</tr>
<tr>
<td>Type</td>
<td>Spoke</td>
</tr>
<tr>
<td>Spoke Descr</td>
<td>(Not Specified)</td>
</tr>
<tr>
<td>Split Horiz Grp</td>
<td>(Not Specified)</td>
</tr>
<tr>
<td>VC Type</td>
<td>Ether</td>
</tr>
<tr>
<td>VC Tag</td>
<td>n/a</td>
</tr>
<tr>
<td>Admin Path MTU</td>
<td>0</td>
</tr>
<tr>
<td>Oper Path MTU</td>
<td>0</td>
</tr>
<tr>
<td>Delivery</td>
<td>GRE</td>
</tr>
<tr>
<td>Far End</td>
<td>1.1.1.1</td>
</tr>
<tr>
<td>Tunnel Far End</td>
<td>n/a</td>
</tr>
<tr>
<td>LSP Types</td>
<td>n/a</td>
</tr>
<tr>
<td>Hash Label</td>
<td>Disabled</td>
</tr>
<tr>
<td>Hash Lbl Sig Cap</td>
<td>Disabled</td>
</tr>
<tr>
<td>Oper Hash Label</td>
<td>Disabled</td>
</tr>
<tr>
<td>Admin State</td>
<td>Up</td>
</tr>
<tr>
<td>Oper State</td>
<td>Down</td>
</tr>
<tr>
<td>Acct. Pol</td>
<td>None</td>
</tr>
<tr>
<td>Collect Stats</td>
<td>Disabled</td>
</tr>
<tr>
<td>Ingress Label</td>
<td>0</td>
</tr>
<tr>
<td>Egress Label</td>
<td>0</td>
</tr>
<tr>
<td>Ingr Mac Fltr-Id</td>
<td>n/a</td>
</tr>
<tr>
<td>Egr Mac Fltr-Id</td>
<td>n/a</td>
</tr>
<tr>
<td>Ingr IP Fltr-Id</td>
<td>n/a</td>
</tr>
<tr>
<td>Egr IP Fltr-Id</td>
<td>n/a</td>
</tr>
<tr>
<td>Ingr IPv6 Fltr-Id</td>
<td>n/a</td>
</tr>
<tr>
<td>Egr IPv6 Fltr-Id</td>
<td>n/a</td>
</tr>
<tr>
<td>Admin ControlWord</td>
<td>Not Preferred</td>
</tr>
<tr>
<td>Oper ControlWord</td>
<td>False</td>
</tr>
<tr>
<td>Last Status Change</td>
<td>09/11/2013 20:02:40</td>
</tr>
<tr>
<td>Signaling</td>
<td>TLDP</td>
</tr>
<tr>
<td>Last Mgmt Change</td>
<td>09/15/2013 13:56:56</td>
</tr>
<tr>
<td>Force Vlan-Vc</td>
<td>Disabled</td>
</tr>
<tr>
<td>Endpoint</td>
<td>N/A</td>
</tr>
<tr>
<td>Precedence</td>
<td>4</td>
</tr>
<tr>
<td>PW Status Sig</td>
<td>Enabled</td>
</tr>
<tr>
<td>Class Fwding State</td>
<td>Down</td>
</tr>
<tr>
<td>Flags</td>
<td>SdpOperDown</td>
</tr>
<tr>
<td>NoIngVCLabel</td>
<td>NoEgrVLabel</td>
</tr>
<tr>
<td>PathMTUTooSmall</td>
<td></td>
</tr>
<tr>
<td>Time to RetryReset</td>
<td>never</td>
</tr>
<tr>
<td>Retries Left</td>
<td>3</td>
</tr>
<tr>
<td>Mac Move</td>
<td>Blockable</td>
</tr>
<tr>
<td>Blockable Level</td>
<td>Tertiary</td>
</tr>
<tr>
<td>Local Pw Bits</td>
<td>None</td>
</tr>
<tr>
<td>Peer Pw Bits</td>
<td>None</td>
</tr>
<tr>
<td>Peer Fault Ip</td>
<td>None</td>
</tr>
<tr>
<td>Peer Vccv CV Bits</td>
<td>None</td>
</tr>
<tr>
<td>Peer Vccv CC Bits</td>
<td>None</td>
</tr>
<tr>
<td>Application Profile</td>
<td>None</td>
</tr>
<tr>
<td>Transit Policy</td>
<td>None</td>
</tr>
<tr>
<td>Max Nbr of MAC Addr</td>
<td>No Limit</td>
</tr>
<tr>
<td>Total MAC Addr</td>
<td>0</td>
</tr>
<tr>
<td>Learned MAC Addr</td>
<td>0</td>
</tr>
<tr>
<td>Static MAC Addr</td>
<td>0</td>
</tr>
<tr>
<td>OAM MAC Addr</td>
<td>0</td>
</tr>
<tr>
<td>DHCP MAC Addr</td>
<td>0</td>
</tr>
<tr>
<td>Host MAC Addr</td>
<td>0</td>
</tr>
<tr>
<td>Intf MAC Addr</td>
<td>0</td>
</tr>
<tr>
<td>SPB MAC Addr</td>
<td>0</td>
</tr>
<tr>
<td>Cond MAC Addr</td>
<td>0</td>
</tr>
<tr>
<td>MAC Learning</td>
<td>Enabled</td>
</tr>
<tr>
<td>Discard Unkwn Srce</td>
<td>Disabled</td>
</tr>
<tr>
<td>MAC Aging</td>
<td>Enabled</td>
</tr>
<tr>
<td>BPDU Translation</td>
<td>Disabled</td>
</tr>
<tr>
<td>L2PT Termination</td>
<td>Disabled</td>
</tr>
<tr>
<td>MAC Pinning</td>
<td>Disabled</td>
</tr>
<tr>
<td>Ignore Standby Sig</td>
<td>False</td>
</tr>
<tr>
<td>Block On Mesh Fail</td>
<td>False</td>
</tr>
<tr>
<td>Oper Group</td>
<td>(none)</td>
</tr>
<tr>
<td>Monitor Oper Grp</td>
<td>(none)</td>
</tr>
<tr>
<td>Rest Prot Src Mac</td>
<td>Disabled</td>
</tr>
<tr>
<td>Auto Learn Mac Prot</td>
<td>Disabled</td>
</tr>
<tr>
<td>RestProtSrcMacAct</td>
<td>Disable</td>
</tr>
<tr>
<td>Ingress Qos Policy</td>
<td>(none)</td>
</tr>
<tr>
<td>Egress Qos Policy</td>
<td>(none)</td>
</tr>
<tr>
<td>Ingress FP QGrp</td>
<td>(none)</td>
</tr>
<tr>
<td>Egress Port QGrp</td>
<td>(none)</td>
</tr>
<tr>
<td>Ing FP QGrp Inst</td>
<td>(none)</td>
</tr>
<tr>
<td>Egr Port QGrp Inst</td>
<td>(none)</td>
</tr>
</tbody>
</table>

---

**ETH-CFM SDP-Bind specifics**

---
V-MEP Filtering : Disabled

KeepAlive Information :
Admin State : Disabled Oper State : Disabled
Hello Time : 10 Hello Msg Len : 0
Max Drop Count : 3 Hold Down Time : 10

Statistics :
I. Fwd. Pkts. : 0 I. Dro. Pkts. : 0
E. Fwd. Pkts. : 0 E. Fwd. Octets : 0
Squelch Levels : 0 1 2 3 4 5 6 7

site

Syntax site [detail]
site name

Context show>service>id

Description This command displays sites configures for the service.

Parameters name — Specifies the site name.

Values 32 chars max

split-horizon-group

Syntax split-horizon-group [group-name]

Context show>service>id

Description This command displays service split horizon groups.

*A:ALA-1# show service id 700 split-horizon-group
----------------------------------------------------------------------------------------------------
Service: Split Horizon Group
----------------------------------------------------------------------------------------------------
Name Description
----------------------------------------------------------------------------------------------------
No. of Split Horizon Groups: 1
----------------------------------------------------------------------------------------------------
*A:ALA-1#

*A:ALA-1# show service id 700 split-horizon-group DSL-group1
----------------------------------------------------------------------------------------------------
Service: Split Horizon Group
----------------------------------------------------------------------------------------------------
Name Description
----------------------------------------------------------------------------------------------------
Associations
----------------------------------------------------------------------------------------------------
SAP 1/1/3:1
SDP 108:1
Show, Clear, Debug Commands

SDP 109:1

SAPs Associated : 1  SDP Associated : 2

*A:ALA-1#
VPLS Show Commands

stp

**Syntax**

stp [detail]

stp mst-instance mst-inst-number

**Context**

show>service>id

**Description**

This command displays information for the spanning tree protocol instance for the service.

**Parameters**

- **detail** — Displays detailed information.
- **mst-inst-number** — Displays information about the specified MST.

**Values**

1 — 4094

**Output**

**Show Service-ID STP Output** — The following table describes show service-id STP output fields:

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bridge-id</td>
<td>Specifies the MAC address used to identify this bridge in the network.</td>
</tr>
<tr>
<td>Bridge fwd delay</td>
<td>Specifies how fast a bridge changes its state when moving toward the forwarding state.</td>
</tr>
<tr>
<td>Bridge Hello time</td>
<td>Specifies the amount of time between the transmission of Configuration BPDUs.</td>
</tr>
<tr>
<td>Bridge max age</td>
<td>Specifies the maximum age of Spanning Tree Protocol information learned from the network on any port before it is discarded. This is the actual value that this bridge is currently using.</td>
</tr>
<tr>
<td>Bridge priority</td>
<td>Defines the priority of the Spanning Tree Protocol instance associated with this service.</td>
</tr>
<tr>
<td>Topology change</td>
<td>Specifies whether a topology change is currently in progress.</td>
</tr>
<tr>
<td>Last Top. change</td>
<td>Specifies the time (in hundredths of a second) since the last time a topology change was detected by the Spanning Tree Protocol instance associated with this service.</td>
</tr>
<tr>
<td>Top. change count</td>
<td>Specifies the total number of topology changes detected by the Spanning Tree Protocol instance associated with this service since the management entity was last reset or initialized.</td>
</tr>
<tr>
<td>Root bridge-id</td>
<td>Specifies the bridge identifier of the root of the spanning tree as determined by the Spanning Tree Protocol instance associated with this service. This value is used as the Root Identifier parameter in all Configuration BPDUs originated by this node.</td>
</tr>
<tr>
<td>Root path cost</td>
<td>Specifies the cost of the path to the root bridge as seen from this bridge.</td>
</tr>
<tr>
<td>Root forward delay</td>
<td>Specifies how fast the root changes its state when moving toward the forwarding state.</td>
</tr>
</tbody>
</table>
### Sample Output

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Root hello time</td>
<td>Specifies the amount of time between the transmission of configuration BPDUs.</td>
</tr>
<tr>
<td>Root max age</td>
<td>Specifies the maximum age of Spanning Tree Protocol information learned from the network on any port before it is discarded.</td>
</tr>
<tr>
<td>Root priority</td>
<td>This object specifies the priority of the bridge that is currently selected as root-bridge for the network.</td>
</tr>
<tr>
<td>Root port</td>
<td>Specifies the port number of the port which offers the lowest cost path from this bridge to the root bridge.</td>
</tr>
<tr>
<td>SAP Identifier</td>
<td>The ID of the access port where this SAP is defined.</td>
</tr>
<tr>
<td>BPDU encap</td>
<td>Specifies the type of encapsulation used on BPDUs sent out and received on this SAP.</td>
</tr>
<tr>
<td>Port Number</td>
<td>Specifies the value of the port number field which is contained in the least significant 12 bits of the 16-bit port ID associated with this SAP.</td>
</tr>
<tr>
<td>Priority</td>
<td>Specifies the value of the port priority field which is contained in the most significant 4 bits of the 16-bit port ID associated with this SAP.</td>
</tr>
<tr>
<td>Cost</td>
<td>Specifies the contribution of this port to the path cost of paths towards the spanning tree root which include this port.</td>
</tr>
<tr>
<td>Designated Port</td>
<td>Specifies the port identifier of the port on the designated bridge for this port's segment.</td>
</tr>
<tr>
<td>Designated Bridge</td>
<td>Specifies the bridge identifier of the bridge which this port considers to be the designated bridge for this port's segment.</td>
</tr>
</tbody>
</table>
IGMP Snooping Show Commands

igmp-snooping

Syntax
igmp-snooping

Context
show>service>id

Description
This command enables the context to display IGMP snooping information.

all

Syntax
all

Context
show>service>id>igmp-snooping

Description
This command displays detailed information for all aspects of IGMP snooping on the VPLS service.

Output
Show All Service-ID — The following table describes the show all service-id command output fields:

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin State</td>
<td>The administrative state of the IGMP instance.</td>
</tr>
<tr>
<td>Querier</td>
<td>Displays the address of the IGMP querier on the IP subnet to which the</td>
</tr>
<tr>
<td></td>
<td>interface is attached.</td>
</tr>
<tr>
<td>Sap Id</td>
<td>Displays the SAP IDs of the service ID.</td>
</tr>
<tr>
<td>Oper State</td>
<td>Displays the operational state of the SAP IDs of the service ID.</td>
</tr>
<tr>
<td>Mrtr Port</td>
<td>Specifies if the port is a multicast router port.</td>
</tr>
<tr>
<td>Send Queries</td>
<td>Specifies whether the send-queries command is enabled or disabled.</td>
</tr>
<tr>
<td>Max Num Groups</td>
<td>Specifies the maximum number of multicast groups that can be joined on this</td>
</tr>
<tr>
<td></td>
<td>SAP.</td>
</tr>
<tr>
<td>Num Groups</td>
<td>Specifies the actual number of multicast groups that can be joined on this</td>
</tr>
<tr>
<td></td>
<td>SAP.</td>
</tr>
</tbody>
</table>

Sample Output
Show, Clear, Debug Commands

**mfib**

**Syntax**

```
mfib [brief | statistics] [ip | mac] brief
mfib [group grp-address | *]
```

**Context**

`show>service>id`

**Description**

This command displays the multicast FIB on the VPLS service.

**Parameters**

- `brief` — Displays a brief output.
- `group grp grp-address` — Displays the multicast FIB for a specific multicast group address.

**Output**

`Show Output` — The following table describes the command output fields:

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Address</td>
<td>IPv4 multicast group address.</td>
</tr>
<tr>
<td>SAP ID</td>
<td>Indicates the SAP/SDP to which the corresponding multicast stream will be forwarded/blocked.</td>
</tr>
<tr>
<td>Forwarding/Blocking</td>
<td>Indicates whether the corresponding multicast stream will be blocked/forwarded.</td>
</tr>
<tr>
<td>Number of Entries</td>
<td>Specifies the number of entries in the MFIB.</td>
</tr>
<tr>
<td>Forwarded Packets</td>
<td>Indicates the number of multicast packets forwarded for the corresponding source/group.</td>
</tr>
<tr>
<td>Forwarded Octets</td>
<td>Indicates the number of octets forwarded for the corresponding source/group.</td>
</tr>
<tr>
<td>Svc ID</td>
<td>Indicates the service to which the corresponding multicast stream will forwarded/blocked. Local means that the multicast stream will be forwarded/blocked to a SAP or SDP local to the service.</td>
</tr>
</tbody>
</table>

**mrouters**

**Syntax**

```
mrouters [detail]
```

**Context**

`show>service>id>igmp-snooping`

**Description**

This command displays all multicast routers.

**Parameters**

- `detail` — Displays detailed information.
port-db

**Syntax**

```
port-db sap sap-id [detail]
port-db sap sap-id group grp-address
port-db sdp sdp-id:vc-id [detail]
port-db sdp sdp-id:vc-id group grp-address
```

**Context**

```
show>service>id>igmp-snooping
```

**Description**

This command displays information on the IGMP snooping port database for the VPLS service.

**Parameters**

- **group grp-ip-address** — Displays the IGMP snooping port database for a specific multicast group address.
- **sap sap-id** — Displays the IGMP snooping port database for a specific SAP. See Common CLI Command Descriptions on page 1783 for command syntax.
- **sdp sdp-id** — Displays only IGMP snooping entries associated with the specified mesh SDP or spoke SDP. For a spoke SDP, the VC ID must be specified, for a mesh SDP, the VC ID is optional.

**Values**

- **vc-id** — The virtual circuit ID on the SDP ID for which to display information.
  - **Default** For mesh SDPs only, all VC IDs.
  - **Values** 1 — 4294967295

**Output**

**Show Output** — The following table describes the show output fields:

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Address</td>
<td>The IP multicast group address for which this entry contains information.</td>
</tr>
<tr>
<td>Mode</td>
<td>Specifies the type of membership report(s) received on the interface for the group.</td>
</tr>
<tr>
<td></td>
<td>In the include mode, reception of packets sent to the specified multicast address is requested only from those IP source addresses listed in the source-list parameter of the IGMP membership report.</td>
</tr>
<tr>
<td></td>
<td>In exclude' mode, reception of packets sent to the given multicast address is requested from all IP source addresses except those listed in the source-list parameter.</td>
</tr>
<tr>
<td>Type</td>
<td>Indicates how this group entry was learned.</td>
</tr>
<tr>
<td></td>
<td>If this group entry was learned by IGMP, the value is set to dynamic.</td>
</tr>
<tr>
<td></td>
<td>For statically configured groups, the value is set to static.</td>
</tr>
</tbody>
</table>
## Show, Clear, Debug Commands

### Compatibility mode

Specifies the IGMP mode. This is used in order for routers to be compatible with older version routers. IGMPv3 hosts must operate in Version 1 and Version 2 compatibility modes. IGMPv3 hosts must keep state per local interface regarding the compatibility mode of each attached network. A host's compatibility mode is determined from the host compatibility mode variable which can be in one of three states: IGMPv1, IGMPv2 or IGMPv3. This variable is kept per interface and is dependent on the version of general queries heard on that interface as well as the older version querier present timers for the interface.

### V1 host expires

The time remaining until the local router will assume that there are no longer any IGMP Version 1 members on the IP subnet attached to this interface. Upon hearing any IGMPv1 membership report, this value is reset to the group membership timer. While this time remaining is non-zero, the local router ignores any IGMPv2 leave messages for this group that it receives on this interface.

### V2 host expires

The time remaining until the local router will assume that there are no longer any IGMP Version 2 members on the IP subnet attached to this interface. Upon hearing any IGMPv2 membership report, this value is reset to the group membership timer. While this time remaining is non-zero, the local router ignores any IGMPv3 leave messages for this group that it receives on this interface.

### Source address

The source address for which this entry contains information.

### Up Time

The time since the source group entry was created.

### Expires

The amount of time remaining before this entry will be aged out.

### Number of sources

Indicates the number of IGMP group and source specific queries received on this SAP.

### Forwarding/Blocking

Indicates whether this entry is on the forward list or block list.

### Number of groups

Indicates the number of groups configured for this SAP.

## Sample Output

**proxy-db**

### Syntax

- `proxy-db [detail]`
- `proxy-db group grp-address`

### Context

`show>service?id>igmp-snooping`
VPLS Show Commands

Description
This command displays information on the IGMP snooping proxy reporting database for the VPLS service.

Parameters
- **group grp-ip-address** — Displays the IGMP snooping proxy reporting database for a specific multicast group address.

Output
- **Show Output** — The following table describes the show output fields:

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Address</td>
<td>The IP multicast group address for which this entry contains information.</td>
</tr>
<tr>
<td>Mode</td>
<td>Specifies the type of membership report(s) received on the interface for the group. In the include mode, reception of packets sent to the specified multicast address is requested only from those IP source addresses listed in the source-list parameter of the IGMP membership report. In the “exclude” mode, reception of packets sent to the given multicast address is requested from all IP source addresses except those listed in the source-list parameter.</td>
</tr>
<tr>
<td>Up Time</td>
<td>The total operational time in seconds.</td>
</tr>
<tr>
<td>Num Sources</td>
<td>Indicates the number of IGMP group and source specific queries received on this interface.</td>
</tr>
<tr>
<td>Number of groups</td>
<td>Number of IGMP groups.</td>
</tr>
<tr>
<td>Source Address</td>
<td>The source address for which this entry contains information.</td>
</tr>
</tbody>
</table>

Sample Output

querier

Syntax
- **querier**

Context
- show>service>id>igmp-snooping

Description
This command displays information on the IGMP snooping queriers for the VPLS service.

Output
- **Show Output** — The following table describes the show output fields:

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP Id</td>
<td>Specifies the SAP ID of the service.</td>
</tr>
<tr>
<td>IP address</td>
<td>Specifies the IP address of the querier.</td>
</tr>
<tr>
<td>Expires</td>
<td>The time left, in seconds, that the query will expire.</td>
</tr>
</tbody>
</table>
### Sample Output

<table>
<thead>
<tr>
<th>Label</th>
<th>Description (Continued)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Up time</td>
<td>The length of time the query has been enabled.</td>
</tr>
<tr>
<td>Version</td>
<td>The configured version of IGMP.</td>
</tr>
<tr>
<td>General Query</td>
<td>The frequency at which host-query packets are transmitted.</td>
</tr>
<tr>
<td>Interval</td>
<td></td>
</tr>
<tr>
<td>Query Response</td>
<td>The time to wait to receive a response to the host-query message from the host.</td>
</tr>
<tr>
<td>Interval</td>
<td></td>
</tr>
<tr>
<td>Robust Count</td>
<td>Specifies the value used to calculate several IGMP message intervals.</td>
</tr>
</tbody>
</table>

**Sample Output**
static

Syntax  
static [sap sap-id | sdp sdp-id:vc-id]

Context  
show>service>id>igmp-snooping

Description  
This command displays information on static IGMP snooping source groups for the VPLS service.

Parameters  
sap sap-id — Displays static IGMP snooping source groups for a specific SAP. See Common CLI Command Descriptions on page 1783 for command syntax.

sdp sdp-id — Displays the IGMP snooping source groups for a specific spoke or mesh SDP.

vc-id — The virtual circuit ID on the SDP ID for which to display information.

Default  
For mesh SDPs only, all VC IDs.

Values  
1 — 17407

Output  
Show Output — The following table describes the show output fields:

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source</td>
<td>Displays the IP source address used in IGMP queries.</td>
</tr>
<tr>
<td>Group</td>
<td>Displays the static IGMP snooping source groups for a specified SAP.</td>
</tr>
</tbody>
</table>

Sample Output

*A:ALA-1>show>service>id>snooping# static
===============================================================================
IGMP Snooping Static Source Groups for SAP 1/1/2
===============================================================================
Source | Group
*     | 225.0.0.2
*     | 225.0.0.3
===============================================================================
Static (*,G)/(S,G) entries: 2
===============================================================================
IGMP Snooping Static Source Groups for SDP 10:10
===============================================================================
Source | Group
1.1.1.1| 225.0.0.10
===============================================================================
Static (*,G)/(S,G) entries: 1
*A:ALA-1>show>service>id>snooping#
statistics

Syntax  statistics [sap sap-id | sdp sdp-id:vc-id]

Context  show>service{id>igmp-snooping

Description  This command displays IGMP snooping statistics for the VPLS service.

Parameters  sap sap-id — Displays IGMP snooping statistics for a specific SAP. See Common CLI Command Descriptions on page 1783 for command syntax.

sdp sdp-id — Displays the IGMP snooping statistics for a specific spoke or mesh SDP.

Values  vc-id — The virtual circuit ID on the SDP ID for which to display information.

Default  For mesh SDPs only, all VC IDs.

Values  1 — 4294967295

Sample Output

bgp-evpn

Syntax  bgp-evpn

Context  show>service{id

Description  This command displays the bgp-evpn configured parameters for a given service, including the admin status of vxlan, the configuration for mac-advertisement and unknown-mac-route as well as the mac-duplication parameters. The command shows the duplicate mac addresses that mac-duplication has detected.

Sample Output

*A:DutA# show service id 1 bgp-evpn

+-----------------------------------------------------+
| BGP EVPN Table                                      |
| MAC Advertisement : Enabled                         |
| Unknown MAC Route : Disabled                        |
| VXLAN Admin Status : Enabled                         |
| Creation Origin : manual                            |
| MAC Dup Detn Moves : 5                               |
| MAC Dup Detn Window : 3                              |
| MAC Dup Detn Retry : 9                               |
| Number of Dup MACs : 1                              |

+-----------------------------------------------------+
<table>
<thead>
<tr>
<th>Detected Duplicate MAC Addresses Time Detected</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:12:12:12:12:12:00 01/17/2014 16:01:02</td>
</tr>
</tbody>
</table>
+-----------------------------------------------------+
VPLS Clear Commands

id

Syntax
id service-id

Context
clear>service
clear>service>statistics

Description
This command clears commands for a specific service.

Parameters
service-id — The ID that uniquely identifies a service.

Values
service-id: 1 — 214748364
svc-name: A string up to 64 characters in length.

statistics

Syntax
statistics

Context
clear>service>stats

Description
This command clears session statistics for this service.

fdb

Syntax
fdb {all | mac ieee-address | sap sap-id} | mesh-sdp sdp-id[:vc-id] | spoke-sdp sdp-id:vc-id

Context
clear>service>id

Description
This command clears FDB entries for the service.

Parameters
all — Clears all FDB entries.

mac ieee-address — Clears only FDB entries in the FDB table with the specified 48-bit MAC address. The MAC address can be expressed in the form aa:bb:cc:dd:ee:ff or aa-bb-cc-dd-ee-ff where aa, bb, cc, dd, ee and ff are hexadecimal numbers.

sap-id — Specifies the physical port identifier portion of the SAP definition. See Common CLI Command Descriptions on page 1783 for command syntax.

mesh-sdp — Clears only service FDB entries associated with the specified mesh SDP ID. For a mesh SDP, the VC ID is optional.

spoke-sdp — Clears only service FDB entries associated with the specified spoke SDP ID. For a spoke SDP, the VC ID must be specified.
Show, Clear, Debug Commands

- **sdp-id** — The SDP ID for which to clear associated FDB entries.
- **vc-id** — The virtual circuit ID on the SDP ID for which to clear associated FDB entries.

### Values

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>sdp-id</td>
<td>1 — 17407</td>
</tr>
<tr>
<td>vc-id</td>
<td>1 — 4294967295</td>
</tr>
</tbody>
</table>

#### mesh-sdp

**Syntax**

```
mesh-sdp sdp-id[vc-id] ingress-vc-label
```

**Context**

clear>service>id

**Description**

This command clears and resets the mesh SDP bindings for the service.

**Parameters**

- **sdp-id** — The mesh SDP ID to be reset.
  - **Values**
    - 1 — 17407
- **vc-id** — The virtual circuit ID on the SDP ID to be reset.
  - **Default**
    - All VC IDs on the SDP ID.
  - **Values**
    - 1 — 4294967295

#### spoke-sdp

**Syntax**

```
spoke-sdp sdp-id[vc-id] {all | counters | stp | l2pt}
```

**Context**

clear>service>id

**Description**

This command clears and resets the spoke SDP bindings for the service.

**Parameters**

- **sdp-id** — The spoke SDP ID to be reset.
  - **Values**
    - 1 — 17407
- **vc-id** — The virtual circuit ID on the SDP ID to be reset.
  - **Values**
    - 1 — 4294967295

- **all** — Clears all queue statistics and STP statistics associated with the SDP.
- **counters** — Clears all queue statistics associated with the SDP.
- **stp** — Clears all STP statistics associated with the SDP.
- **l2pt** — Clears all L2PT statistics associated with the SDP.
**sap**

**Syntax**  
`sap sap-id`

**Context**  
clear>service>statistics

**Description**  
This command clears statistics for the SAP bound to the service.

**Parameters**  
`sap-id` — See Common CLI Command Descriptions on page 1783 for command syntax.

`all` — Clears all queue statistics and STP statistics associated with the SAP.

`counters` — Clears all queue statistics associated with the SAP.

**counters**

**Syntax**  
counters

**Context**  
clear>service>statistics>id

**Description**  
This command clears all traffic queue counters associated with the service ID.

**l2pt**

**Syntax**  
l2pt

**Context**  
clear>service>statistics>id

**Description**  
This command clears the l2pt statistics for this service.

**mesh-sdp**

**Syntax**  
`mesh-sdp sdp-id[;vc-id] {all | counters | stp | mrp}`

**Context**  
clear>service>statistics>id

**Description**  
This command clears the statistics for a particular mesh SDP bind.

**Parameters**  
`sdp-id[;vc-id]` —  
sdp-id - [1..17407]

vc-id - [1..4294967295]

`all` — Clears all queue statistics and STP statistics associated with the SDP.

`counters` — Clears all queue statistics associated with the SDP.

`stp` — Clears all STP statistics associated with the SDP.

`mrp` — Clears all MRP statistics associated with the SDP.
show, clear, debug commands

spoke-sdp

Syntax  

spoke-sdp  sdp-id[:vc-id] {all | counters | stp| l2pt | mrp}

Context  clear>service>statistics>id

Description  This command clears statistics for the spoke SDP bound to the service.

Parameters  

sdp-id — The spoke SDP ID for which to clear statistics.

Values  

1 — 17407

vc-id — The virtual circuit ID on the SDP ID to be reset.

Values  

1 — 4294967295

all — Clears all queue statistics and STP statistics associated with the SDP.

counters — Clears all queue statistics associated with the SDP.

stp — Clears all STP statistics associated with the SDP.

l2pt — Clears all L2PT statistics associated with the SDP.

stp

Syntax  stp

Context  clear>service>statistics>id

Description  Clears all spanning tree statistics for the service ID.

detected-protocols

Syntax  detected-protocols {all | sap sap-id}

Context  clear>service>id>stp

Description  RSTP automatically falls back to STP mode when it receives an STP BPDU. The clear detected-protocols command forces the system to revert to the default RSTP mode on the SAP

Parameters  

all — Clears all detected protocol statistics.

sap-id — Clears the specified lease state SAP information. See Common CLI Command Descriptions on page 1783 for command syntax.

port-db

Syntax  port-db [sap sap-id] [group grp-address [source ip-address]]

port-db  sdp  sdp-id:vc-id [group grp-address [source ip-address]]

Context  clear>service>id>igmp-snooping
**Description**
This command clears the information on the IGMP snooping port database for the VPLS service.

**Parameters**
- **sap sap-id** — Clears IGMP snooping statistics matching the specified SAP ID and optional encapsulation value. See Common CLI Command Descriptions on page 1783 for command syntax.

- **sdp-id** — Clears only IGMP snooping entries associated with the specified mesh SDP or spoke SDP. For a spoke SDP, the VC ID must be specified, for a mesh SDP, the VC ID is optional.
  
  **Values**
  - 1 — 17407

- **vc-id** — The virtual circuit ID on the SDP ID for which to clear information.
  
  **Default**
  - For mesh SDPs only, all VC IDs.
  
  **Values**
  - 1 — 4294967295

- **group grp-address** — Clears IGMP snooping statistics matching the specified group address.

- **source ip-address** — Clears IGMP snooping statistics matching the specified particular source.

**querier**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>querier</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Context</strong></td>
<td>clear&gt;service?id&gt;igmp-snooping</td>
</tr>
</tbody>
</table>

| **Description** | This command clears the information on the IGMP snooping queriers for the VPLS service. |
VPLS Debug Commands

id

Syntax  
id service-id

Context  
debug>service

Description  
This command debugs commands for a specific service.

Parameters  
  
service-id — The ID that uniquely identifies a service.

Values  
  service-id: 1 — 214748364
  svc-name: A string up to 64 characters in length.

arp-host

Syntax  
[no] arp-host

Context  
debug>service>id

Description  
This command enables and configures ARP host debugging. The no form of the command disables ARP host debugging.

igmp-snooping

Syntax  
[no] igmp-snooping

Context  
debug>service>id

Description  
This command enables and configures IGMP-snooping debugging.

detail-level

Syntax  
detail-level {low | medium | high}

no detail-level

Context  
debug>service>id>igmp

Description  
This command enables and configures the IGMP tracing detail level. The no form of the command disables the IGMP tracing detail level.
mac

Syntax  [no] mac ieee-address
Context  debug>service>id>igmp
Description  This command shows IGMP packets for the specified MAC address. The no form of the command disables the MAC debugging.

mode

Syntax  mode {dropped-only | ingr-and-dropped | egr-ingr-and-dropped}
        no mode
Context  debug>service>id>igmp
Description  This command enables and configures the IGMP tracing mode. The no form of the command disables the IGMP tracing mode.

sap

Syntax  [no] sap sap-id
Context  debug>service>id>igmp
Description  This command shows IGMP packets for a specific SAP. The no form of the command disables the debugging for the SAP.

sdp

Syntax  [no] sdp sdp-id:vc-id
Context  debug>service>id>igmp
Description  This command shows IGMP packets for a specific SDP. The no form of the command disables the debugging for the SDP.

Parameters  sdp-id — Displays only IGMP snooping entries associated with the specified mesh SDP or spoke SDP. For a spoke SDP, the VC ID must be specified, for a mesh SDP, the VC ID is optional.

Values  1 — 17407

vc-id — The virtual circuit ID on the SDP ID for which to display information.

Values  1 — 4294967295
Show, Clear, Debug Commands

event-type

Syntax  

\[ \text{[no]} \text{ event-type \{config-change|svc-oper-status-change|sap-oper-status-change|sdpbind-oper-status-change\}} \]

Context  debug>service>id

Description  This command enables a particular debugging event type. The \text{no} form of the command disables the event type debugging.

Parameters  

\text{config-change} — Debugs configuration change events.

\text{svc-oper-status-change} — Debugs service operational status changes.

\text{sap-oper-status-change} — Debugs SAP operational status changes.

\text{sdpbind-oper-status-change} — Debugs SDP operational status changes.

sap

Syntax  

\[ \text{[no]} \text{ sap sap-id} \]

Context  debug>service>id

Description  This command enables debugging for a particular SAP.

Parameters  

\text{sap-id} — Specifies the SAP ID.

stp

Syntax  

\text{stp}

Context  debug>service>id

Description  This command enables the context for debugging STP.

all-events

Syntax  

\text{all-events}

Context  debug>service>id>stp

Description  This command enables STP debugging for all events.

bpdu

Syntax  

\[ \text{[no]} \text{ bpdu} \]

Context  debug>service>id>stp
Description: This command enables STP debugging for received and transmitted BPDUs.

core-connectivity

Syntax: [no] core-connectivity
Context: debug>service>id>stp
Description: This command enables STP debugging for core connectivity.

exception

Syntax: [no] exception
Context: debug>service>id>stp
Description: This command enables STP debugging for exceptions.

fsm-state-changes

Syntax: [no] fsm-state-changes
Context: debug>service>id>stp
Description: This command enables STP debugging for FSM state changes.

fsm-timers

Syntax: [no] fsm-timers
Context: debug>service>id>stp
Description: This command enables STP debugging for FSM timer changes.

port-role

Syntax: [no] port-role
Context: debug>service>id>stp
Description: This command enables STP debugging for changes in port roles.
Show, Clear, Debug Commands

port-state

Syntax  
\[no\] port-state

Context  
debug>service>id>stp

Description  
This command enables STP debugging for port states.

sap

Syntax  
\[no\] sap sap-id

Context  
debug>service>id>stp

Description  
This command enables STP debugging for a specific SAP.

Parameters  
sap-id — Specifies the physical port identifier portion of the SAP definition. See Common CLI Command Descriptions on page 1783 for command syntax.

sdp

Syntax  
\[no\] sdp sdp-id:vc-id

Context  
debug>service>stp

Description  
This command enables STP debugging for a specific SDP.

provider-tunnels

Syntax  
provider-tunnels type

Context  
tools>dump>service>vpls

Description  
This command dumps the inclusive provider tunnels based on type.

Output  
*A:Dut-C>tools# dump service vpls 1001 provider-tunnels type terminating
VPLS 1001 Inclusive Provider Tunnels Terminating

ipmsi (RSVP)  P2MP-ID Tunl-ID Ext-Tunl-ID

1001  61440  10.20.1.1
1001  64944  10.20.1.2

*A:Dut-C>tools# dump service vpls 1001 provider-tunnels type originating
VPLS 1001 Inclusive Provider Tunnels Originating
VPLS Show Commands

*A:Dut-C>tools# dump service vpls 1001 provider-tunnels

VPLS 1001 Inclusive Provider Tunnels Originating

<table>
<thead>
<tr>
<th>ipmsi (RSVP)</th>
<th>P2MP-ID</th>
<th>Tunl-ID</th>
<th>Ext-Tunl-ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipmsi-1001-73728</td>
<td>1001</td>
<td>61440</td>
<td>10.20.1.3</td>
</tr>
</tbody>
</table>

VPLS 1001 Inclusive Provider Tunnels Terminating

<table>
<thead>
<tr>
<th>ipmsi (RSVP)</th>
<th>P2MP-ID</th>
<th>Tunl-ID</th>
<th>Ext-Tunl-ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>1001 61440 10.20.1.1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1001 64944 10.20.1.2</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*A:Dut-C>tools# dump service vpls 1001 provider-tunnels type terminating

VPLS 1001 Inclusive Provider Tunnels Terminating

<table>
<thead>
<tr>
<th>ipmsi (RSVP)</th>
<th>P2MP-ID</th>
<th>Tunl-ID</th>
<th>Ext-Tunl-ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>1001 61440 10.20.1.1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1001 64944 10.20.1.2</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*A:Dut-C>tools# dump service vpls 1001 provider-tunnels type originating

VPLS 1001 Inclusive Provider Tunnels Originating

<table>
<thead>
<tr>
<th>ipmsi (RSVP)</th>
<th>P2MP-ID</th>
<th>Tunl-ID</th>
<th>Ext-Tunl-ID</th>
</tr>
</thead>
</table>
vxlan

**Syntax**: vxlan [clear]

**Context**: tools>dump>service

**Description**: This command displays the number of times a service could not add a VXLAN binding or <VTEP, Egress VNI> due to the following limits:

- The per System VTEP limit has been reached
- The per System <VTEP, Egress VNI> limit has been reached
- The per Service <VTEP, Egress VNI> limit has been reached
- The per System Bind limit: Total bind limit or vxlan bind limit has been reached.

The command adds a [clear] option to clear the above statistics.

**Output**: *A:PE63# tools dump service id 3 vxlan
VTEP, Egress VNI Failure statistics at 000 00:03:55.710:
statistics last cleared at 000 00:00:00.000:

<table>
<thead>
<tr>
<th>Statistic</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>-------------------</td>
<td>-------</td>
</tr>
</tbody>
</table>

---

### Show, Clear, Debug Commands

```
*A:Dut-C>tools# dump service vpls 1001 provider-tunnels

VPLS 1001 Inclusive Provider Tunnels Originating

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>ipmsi (RSVP)</td>
<td>P2MP-ID</td>
<td>Tunl-ID</td>
</tr>
<tr>
<td>----------------</td>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td>ipmsi-1001-73728</td>
<td>1001</td>
<td>61440</td>
</tr>
</tbody>
</table>

VPLS 1001 Inclusive Provider Tunnels Terminating

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>ipmsi (RSVP)</td>
<td>P2MP-ID</td>
<td>Tunl-ID</td>
</tr>
<tr>
<td>----------------</td>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td>1001</td>
<td>61440</td>
<td>10.20.1.1</td>
</tr>
<tr>
<td>1001</td>
<td>64944</td>
<td>10.20.1.2</td>
</tr>
</tbody>
</table>
```
VPLS Show Commands

<table>
<thead>
<tr>
<th>VTEP</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Limit</td>
<td>0</td>
</tr>
<tr>
<td>System Limit</td>
<td>0</td>
</tr>
<tr>
<td>Egress Mcast List Limit</td>
<td>0</td>
</tr>
<tr>
<td>Duplicate VTEP, Egress VNI</td>
<td>1</td>
</tr>
</tbody>
</table>

**dup-vtep-egrvni**

**Syntax**
dup-vtep-egrvni [clear]

**Context**
tools>dump>service>vxlan

**Description**
This command dumps the <VTEP, VNI> bindings that have been detected as duplicate attempts, that is, an attempt to add the same binding to more than one service. The command provides a ‘clear’ option.

**Output**
*A:PE71# tools dump service vxlan dup-vtep-egrvni
Duplicate VTEP, Egress VNI usage attempts at 000 00:03:41.570:
1. 10.1.1.1:100

**usage**

**Syntax**
usage

**Context**
tools>dump>service>vxlan

**Description**
This command displays the consumed VXLAN resources in the system.

**Output**
*A:PE71# tools dump service vxlan usage
VXLAN usage statistics at 001 17:46:11.170:

VTEP : 5/8191
VTEP, Egress VNI : 5/131071
Sdp Bind + VTEP, Egress VNI : 13/196607
RVPLS Egress VNI : 0/40959
hPBB Show Commands

eth-cfm

Syntax
eth-cfm

Context
show

Description
This command displays 802.1ag CFM information.

association

Syntax
association [ma-index] [detail]

Context
show>eth-cfm

Description
Shows association information.

Parameters
ma-index — Specifies the MA index value.

Values
1 — 4294967295

detail — Displays all association detail.

Output
*A:alcag1-R6# show eth-cfm association
---------------------------------------------------------------------
CFM Association Table
---------------------------------------------------------------------
Md-index Ma-index Name            CCM-interval Bridge-id
---------------------------------------------------------------------
1     1    ivpls  1   5000
---------------------------------------------------------------------
*A:alcag1-R6#
Show, Clear, Debug Commands

cfm-stack-table

Syntax

- `cfm-stack-table`
- `cfm-stack-table port [port-id] [vlan vlan-id] [level 0..7] [direction up | down]`
- `cfm-stack-table sdp [sdp-id [:vc-id]] [level 0..7] [direction up | down]`
- `cfm-stack-table virtual [service-id] [level 0..7]`

Context

- `show > eth-cfm`

Description

Summarizes all MEPs/MIPs.

Parameters

- `port-id` — Displays information about the specified port.
  - Values:
    - `port-id` — Displays information about the specified port.
    - `slot/mda/port[.channel]` — Displays information about the specified port.
    - `lag-id` — Displays information about the specified port.

- `sdp-id[vc-id]` — Specifies an existing SDP and VC ID.
  - Values:
    - `1 — 17407`

- `vlan-id` — Specifies the VLAN ID.
  - Values:
    - `0 — 4094`

- `level` — Specifies the level.
  - Values:
    - `0 — 7`

- `direction up | down` — Indicates the direction in which the maintenance association (MEP or MIP) faces on the bridge port.
  - `down` — Displays continuity check information configured away from the MAC relay entity.
  - `up` — Displays continuity check information configured toward the MAC relay entity.

- `service-id` — Specifies information about the specified service ID.
  - Values:
    - `1 — 2147483648`

Sample Output

```
*A:alcag1-R6# show eth-cfm cfm-stack-table
**********************************************************************************************************************************************
CFM SAP Stack Table
**********************************************************************************************************************************************
Sap    Level Dir  Md-index  Ma-index  Mep-id  Mac-address
------------------------------------------------------------------------
1/2/9:5  4 Up 1 1 51 00:ae:ae:ae:ae:ae
**********************************************************************************************************************************************
CFM SDP Stack Table
**********************************************************************************************************************************************
Sdp   Level Dir  Md-index  Ma-index  Mep-id  Mac-address
------------------------------------------------------------------------
No Matching Entries
**********************************************************************************************************************************************
*A:alcag1-R6#
```
domain

Syntax  domain [md-index] [association ma-index | all-associations [detail]]

Context  show>eth-cfm>domain

Description  This command displays domain information.

Parameters

  md-index — Specifies the maintenance domain (MD) index value.

    Values  1 — 4294967295

  ma-index — Specifies the MA index value.

    Values  1 — 4294967295

  all-associations — Displays information all maintenance associations.

  detail — Displays detailed information.

Sample Output

*A:alcag1-R6# show eth-cfm domain

==============================================================================
<table>
<thead>
<tr>
<th>CFM Domain Table</th>
</tr>
</thead>
<tbody>
<tr>
<td>Md-index</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>-------------------</td>
</tr>
</tbody>
</table>
*A:alcag1-R6# *

*A:alcag1-R6# show eth-cfm mep 51 domain 1 association 1

-------------------------------------------------------------------------------
<table>
<thead>
<tr>
<th>Mep Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Md-index : 1</td>
</tr>
<tr>
<td>Ma-index : 1</td>
</tr>
<tr>
<td>MepId : 51</td>
</tr>
<tr>
<td>IfIndex : 38043648</td>
</tr>
<tr>
<td>FngState : fngReset</td>
</tr>
<tr>
<td>LowestDefectPri : allDef</td>
</tr>
<tr>
<td>HighestDefect : none</td>
</tr>
<tr>
<td>Defect Flags : None</td>
</tr>
<tr>
<td>Mac Address : 00:ae:ae:ae:ae</td>
</tr>
<tr>
<td>CcmTx : 775</td>
</tr>
<tr>
<td>CcmLtmPriority : 7</td>
</tr>
<tr>
<td>CcmSequenceErr : 0</td>
</tr>
</tbody>
</table>

*CcmLastFailure Frame: None*

*XconCcmFailure Frame: None*
*A:alcag1-R6#*
**mep**

**Syntax**

```
mep mep-id domain md-index association ma-index [loopback] [linktrace]
```

**Context**

`show>eth-cfm>domain`

**Description**

This command displays Maintenance Endpoint (MEP) information.

**Parameters**

- `mep-id` — Specifies the maintenance association end point identifier.
  - **Values**
    - 1 — 8191
- `md-index` — Specifies the maintenance domain (MD) index value.
  - **Values**
    - 1 — 4294967295
- `ma-index` — Specifies the MA index value.
  - **Values**
    - 1 — 4294967295
- `loopback` — Displays loopback information for the specified MEP.
- `linktrace` — Displays linktrace information for specified MEP.

**Sample Output**

```
*A:alcag1-R6# oam eth-cfm loopback 00:af:af:af:af mep 51 domain 1 association 1
eth-cfm Loopback Test Initiated: Mac-Address: 00:af:af:af:af, out sap: 1/2/9:5
Sent 1 packets, received 1 packets [0 out-of-order, 0 Bad Msdu] -- OK
*A:alcag1-R6#
```

```
*A:alcag1-R6# oam eth-cfm linktrace 00:af:af:af:af mep 51 domain 1 association 1
Index Ingress Mac          Egress Mac          Relay      Action
----- -------------------- -------------------- ---------- ----------
1     00:00:00:00:00:00    00:AF:AF:AF:AF:AF    rlyHit     terminate
----- -------------------- -------------------- ---------- ----------
No more responses received in the last 5 seconds.
*A:alcag1-R6#
```

**i-vpls**

**Syntax**

```
i-vpls
```

**Context**

`show>service>id`

**Description**

Displays I-VPLS services associated with the B-VPLS service. This command only applies when the service is a B-VPLS.

**Sample Output**

```
*A:SetupCLI# show service id 2002 i-vpls
Related ivpls services for evpls service 2002
-------------------------------------------------------------------
ivpls SvcId | Op ISID | Admin | Oper
```
## hPBB Show Commands

### base

**Syntax**

base

**Context**

show>service>pbb

**Sample**

*A:Dut-B# show service pbb base

---

### mac-name

**Syntax**

mac-name [detail]

**Context**

show>service>pbb

**Description**

This command displays information on a specific MAC name.

**Sample**

*A:Dut-B# show service pbb mac-name

---
id

**Syntax**

```
 id service-id
```

**Context**

```
 show>service
```

**Description**

This command displays information on a specific service ID.

**Sample**

```
*A:Dut-B# show service id 1 all
```

```
Service Detailed Information
Service Id : 1 Vpn Id : 0
Service Type : b-VPLS
Description : (Not Specified)
Customer Id : 1
Last Status Change: 05/17/2009 19:33:11
Last Mgmt Change : 05/17/2009 19:31:59
Admin State : Up Oper State : Up
MTU : 2000 Def. Mesh VC Id : 1
SAP Count : 1 SDP Bind Count : 0
Snd Flush on Fail : Disabled Host Conn Verify : Disabled
Propagate MacFlush: Disabled
Oper Backbone Src : 00:03:00:00:04:01 Use SAP B-MAC : enabled
i-Vpls Count : 0
Epipe Count : 900

*A:Dut-B# show service id 501 all
```

```
Service Detailed Information
Service Id : 501 Vpn Id : 0
Service Type : Epipe
Description : (Not Specified)
Customer Id : 1
Last Status Change: 05/17/2009 19:41:32
Last Mgmt Change : 05/17/2009 19:40:03
Admin State : Up Oper State : Up
MTU : 1514
Vc Switching : False
SAP Count : 1 SDP Bind Count : 0
```

- **Number of services:** 1

```
*A:Dut-B#
```
mrp

**Syntax**
```
mrp
```

**Context**
```
show>service>id
```

**Description**
This command displays information on a per service MRP configuration.

**Output**
```
*A:PE-A# show service id 10 mrp
```

```
<table>
<thead>
<tr>
<th>MRP Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin State          : Up</td>
</tr>
<tr>
<td>Failed Register Cnt: 0</td>
</tr>
<tr>
<td>Max Attributes        : 2048</td>
</tr>
<tr>
<td>Attribute Count       : 10</td>
</tr>
<tr>
<td>Flood Time            : Off</td>
</tr>
</tbody>
</table>
```

```
*A:PE-A#
```

mrp-policy

**Syntax**
```
mrp-policy [mrp-policy]
```
```
mrp-policy mrp-policy [association]
```
```
mrp-policy mrp-policy [entry entry-id]
```

**Context**
```
show>service
```

**Description**
This command displays MRP policy information.

**Parameters**
- **mrp-policy** — Specifies the MRP policy.
  ```
  Values 32 chars max
  ```
- **entry-id** — Specifies the entry ID.
  ```
  Values 1..65535
  ```

mmrp

**Syntax**
```
mmrp mac [ieee-address]
```

**Context**
```
show>service>id
```

**Description**
This command displays information on MACs. If a MAC address is specified, information will be displayed relevant to the specific group. No parameter will display information on all group MACs on a server.
**Parameters**


**Output**

```
*A:PE-A# show service id 10 mmrp mac 01:1E:83:00:00:65
-------------------------------------------------------------------------------
  SAP/SDP            MAC Address       Registered  Declared
-------------------------------------------------------------------------------
  sap:1/1/4:10       01:1e:83:00:00:65  No          Yes
  sap:1/2/2:10       01:1e:83:00:00:65  No          Yes
  sap:2/2/5:10       01:1e:83:00:00:65  Yes         Yes
-------------------------------------------------------------------------------
*A:PE-A#
```

```
*A:PE-A# show service id 10 mmrp mac
-------------------------------------------------------------------------------
  SAP/SDP            MAC Address       Registered  Declared
-------------------------------------------------------------------------------
  sap:1/1/4:10       01:1e:83:00:00:65  No          Yes
  sap:1/1/4:10       01:1e:83:00:00:66  No          Yes
  sap:1/1/4:10       01:1e:83:00:00:67  No          Yes
  sap:1/1/4:10       01:1e:83:00:00:68  No          Yes
  sap:1/1/4:10       01:1e:83:00:00:69  No          Yes
  sap:1/1/4:10       01:1e:83:00:00:6a  No          Yes
  sap:1/1/4:10       01:1e:83:00:00:6b  No          Yes
  sap:1/1/4:10       01:1e:83:00:00:6c  No          Yes
  sap:1/1/4:10       01:1e:83:00:00:6d  No          Yes
  sap:1/1/4:10       01:1e:83:00:00:6e  No          Yes
  sap:1/2/2:10       01:1e:83:00:00:65  No          Yes
  sap:1/2/2:10       01:1e:83:00:00:66  No          Yes
  sap:1/2/2:10       01:1e:83:00:00:67  No          Yes
  sap:1/2/2:10       01:1e:83:00:00:68  No          Yes
  sap:1/2/2:10       01:1e:83:00:00:69  No          Yes
  sap:1/2/2:10       01:1e:83:00:00:6a  No          Yes
  sap:1/2/2:10       01:1e:83:00:00:6b  No          Yes
  sap:1/2/2:10       01:1e:83:00:00:6c  No          Yes
  sap:1/2/2:10       01:1e:83:00:00:6d  No          Yes
  sap:1/2/2:10       01:1e:83:00:00:6e  No          Yes
  sap:2/2/5:10       01:1e:83:00:00:65  Yes         Yes
  sap:2/2/5:10       01:1e:83:00:00:66  Yes         Yes
  sap:2/2/5:10       01:1e:83:00:00:67  Yes         Yes
  sap:2/2/5:10       01:1e:83:00:00:68  Yes         Yes
  sap:2/2/5:10       01:1e:83:00:00:69  Yes         Yes
  sap:2/2/5:10       01:1e:83:00:00:6a  Yes         Yes
  sap:2/2/5:10       01:1e:83:00:00:6b  Yes         Yes
  sap:2/2/5:10       01:1e:83:00:00:6c  Yes         Yes
  sap:2/2/5:10       01:1e:83:00:00:6d  Yes         Yes
  sap:2/2/5:10       01:1e:83:00:00:6e  Yes         Yes
-------------------------------------------------------------------------------
*A:PE-A#
```

**spb**

**Syntax**

`spb`

**Context**

`clear>service>id`

**Description**

This command clears STP related data.
adjacency

Syntax adjacency [detail]

Context show>service>id>spb

Description This command displays SPB adjacency information.

Parameters detail — Show detailed information.

Output Sample Output

```
ISIS Adjacency
System ID Usage State Hold Interface MT Enab
---------------------------------------------------------------
Dut-B L1 Up 19 sap:1/2/2:1.1 No
Dut-C L1 Up 21 sap:1/2/3:1.1 No
---------------------------------------------------------------
Adjacencies : 2
```

base

Syntax base

Context show>service>id>spb

Description This command displays SPB base information.

Output Sample Output

```
*A:Dut-A# show service id 100001 spb base

Service SPB Information
Admin State : Up Oper State : Up
ISIS Instance : 1024 FID : 1
Bridge Priority : 8 Fwd Tree Top Ucast : spf
Fwd Tree Top Mcast : st
Bridge Id : 80:00.00:10:00:01:00:01
Mcast Desig Bridge : 80:00.00:10:00:01:00:01

ISIS Interfaces
Interface Level CircID Oper State L1/L2 Metric
---------------------------------------------------------------
sap:1/2/2:1.1 L1 65536 Up 10/-
sap:1/2/3:1.1 L1 65537 Up 10/-

Interfaces : 2
FID ranges using ECT Algorithm
1-99 low-path-id
```
Show, Clear, Debug Commands

100-100   high-path-id
101-4095  low-path-id

database

Syntax    database
Context   show>service>id>spb
Description This command displays SPB database information.

Output  Sample Output

*A:Dut-A# show service id 100001 spb database

ISIS Database

<table>
<thead>
<tr>
<th>LSP ID</th>
<th>Sequence</th>
<th>Checksum</th>
<th>Lifetime</th>
<th>Attributes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dut-A.00-00</td>
<td>0xc</td>
<td>0xbaba</td>
<td>1103</td>
<td>L1</td>
</tr>
<tr>
<td>Dut-B.00-00</td>
<td>0x13</td>
<td>0xe780</td>
<td>1117</td>
<td>L1</td>
</tr>
<tr>
<td>Dut-C.00-00</td>
<td>0x13</td>
<td>0x85a</td>
<td>1117</td>
<td>L1</td>
</tr>
<tr>
<td>Dut-D.00-00</td>
<td>0xe</td>
<td>0x174a</td>
<td>1119</td>
<td>L1</td>
</tr>
</tbody>
</table>

Level (1) LSP Count : 4

fate-sharing

Syntax    fate-sharing
Context   show>service>id>spb
Description This command displays SPB fate-sharing information on User B-VPLS service, in correspond to associated Control B-VPLS service.

Output  Sample Output

*A:Dut-A# Node show service id spb fate-sharing

User service fate-shared sap/sdp-bind information

<table>
<thead>
<tr>
<th>Control SvcId</th>
<th>Control Sap/SdpBind</th>
<th>FID</th>
<th>User SvcId</th>
<th>User Sap/SdpBind</th>
</tr>
</thead>
<tbody>
<tr>
<td>500</td>
<td>1/1/20:500</td>
<td>502</td>
<td>502</td>
<td>1/1/20:502</td>
</tr>
</tbody>
</table>

fdb
**Syntax**
```
fdb
```

**Context**
```
show>service>id>spb
```

**Description**
This command displays SPB Forwarding database information.

**Output**

**Sample Output**
```
*A:Dut-A# show service id 100001 spb fdb
```

---

```
User service FDB information
```

<table>
<thead>
<tr>
<th>MacAddr</th>
<th>UCast Source</th>
<th>State</th>
<th>MCast Source</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:10:00:01:00:02</td>
<td>1/2/2:1.1</td>
<td>ok</td>
<td>1/2/2:1.1</td>
<td>ok</td>
</tr>
<tr>
<td>00:10:00:01:00:03</td>
<td>1/2/3:1.1</td>
<td>ok</td>
<td>1/2/3:1.1</td>
<td>ok</td>
</tr>
<tr>
<td>00:10:00:01:00:04</td>
<td>1/2/2:1.1</td>
<td>ok</td>
<td>1/2/2:1.1</td>
<td>ok</td>
</tr>
</tbody>
</table>

Entries found: 3

---

**fid**

**Syntax**
```
 fid [fid] fate-sharing
 fid [fid] user-service
 fid [fid] fdb
 fid [fid] mfib [group-mac ieee-address]
 fid [fid] mfib [isid isid]
```

**Context**
```
show>service>id>spb
```

**Description**
This command displays SPB control service FID information.

**Parameters**
- `fid` — A user service FID may be specified. All user service FIDs are displayed if the FID is not specified.
- `user-service` — Specifies user VPLS information for each control VPLS per forwarding data-base identifier. A user service FID may be specified. All user service FIDs are displayed if the FID is not specified.
- `fdb` — Specifies user VPLS Shortest Path Bridging (SPB) multicast forwarding data-base (Mfib) information.
- `mfib` —
  - `group-mac ieee-address` — Specifies the 48-bit IEEE 802.3 group MAC address.
  - `isid isid` — Specifies the value of ISID of the group MAC address of this entry.

**Output**

**Sample Output**
```
*A:Dut-A# show service id 100001 spb fid fate-sharing
```

---

```
Control service fate-shared sap/adp-bind information
```

<table>
<thead>
<tr>
<th>Control SvcId</th>
<th>Control Sap/ SdpBind</th>
<th>FID User SvcId</th>
<th>User Sap/ SdpBind</th>
</tr>
</thead>
</table>

---
hostname

**Syntax**

hostname

**Context**

show>service>id>spb

**Description**

This command displays SPB system-id to hostname mapping.

**Output**

**Sample Output**

*A:Dut-A# show service id 100001 spb hostname

<table>
<thead>
<tr>
<th>System Id</th>
<th>Hostname</th>
</tr>
</thead>
<tbody>
<tr>
<td>0000.00AA.AAAA</td>
<td>cses-B02</td>
</tr>
<tr>
<td>0000.00BB.BBBB</td>
<td>cses-B07</td>
</tr>
</tbody>
</table>

Entries found: 6
interface

Syntax:  interface

Context:  show>service>id>spb

Description:  This command displays SPB interfaces.

Output:  Sample Output

```
*A:Dut-A# show service id 100001 spb interface

+--------------------------------------------+
<table>
<thead>
<tr>
<th>ISIS Interfaces</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface                        Level CircID  Oper State   L1/L2 Metric</td>
</tr>
<tr>
<td>--------------------------------------------</td>
</tr>
<tr>
<td>sap:1/1/20:500                        L1    65536   Up           10/-</td>
</tr>
<tr>
<td>--------------------------------------------</td>
</tr>
</tbody>
</table>

Interfaces : 1

+--------------------------------------------+
```

mfib

Syntax:  mfib [group-mac ieee-address][isid isid]

Context:  show service id <svcId> spb

Description:  This command displays multicast forwarding data-base information.

Parameters:  
- group-mac — Optional IEEE group MAC format:

- isid — Optional I-SID.
  Format: 0..16777215

Output:  Sample Output

```
*A:Dut-A# show service id 100001 spb mfib

+--------------------------------------------+
<table>
<thead>
<tr>
<th>User service MFIB information</th>
</tr>
</thead>
<tbody>
<tr>
<td>MacAddr          ISID     Status</td>
</tr>
<tr>
<td>--------------------------------------------</td>
</tr>
<tr>
<td>01:1E:83:00:27:11 100001    Ok</td>
</tr>
<tr>
<td>--------------------------------------------</td>
</tr>
</tbody>
</table>

Entries found: 1

+--------------------------------------------+
```

routes

Syntax:  routes

Context:  show>service>id>spb
**Description**
This command displays SPB route information.

**Sample Output**

```plaintext
*A:Dut-A# show service id 100001 spb routes

MAC Route Table

<table>
<thead>
<tr>
<th>Fid</th>
<th>MAC</th>
<th>Ver.</th>
<th>Metric</th>
<th>NextHop If</th>
<th>SysID</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>00:10:00:01:00:02</td>
<td>10</td>
<td>10</td>
<td>sap:1/2/2:1.1</td>
<td>Dut-B</td>
</tr>
<tr>
<td>1</td>
<td>00:10:00:01:00:03</td>
<td>10</td>
<td>10</td>
<td>sap:1/2/3:1.1</td>
<td>Dut-C</td>
</tr>
<tr>
<td>100</td>
<td>00:10:00:02:00:02</td>
<td>10</td>
<td>10</td>
<td>sap:1/2/2:1.1</td>
<td>Dut-B</td>
</tr>
<tr>
<td>100</td>
<td>00:10:00:02:00:03</td>
<td>10</td>
<td>10</td>
<td>sap:1/2/3:1.1</td>
<td>Dut-C</td>
</tr>
</tbody>
</table>

Fwd Tree: unicast

<table>
<thead>
<tr>
<th>Fid</th>
<th>MAC</th>
<th>Ver.</th>
<th>Metric</th>
<th>NextHop If</th>
<th>SysID</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>00:10:00:01:00:02</td>
<td>10</td>
<td>10</td>
<td>sap:1/2/2:1.1</td>
<td>Dut-B</td>
</tr>
<tr>
<td>1</td>
<td>00:10:00:01:00:03</td>
<td>10</td>
<td>10</td>
<td>sap:1/2/3:1.1</td>
<td>Dut-C</td>
</tr>
<tr>
<td>1</td>
<td>00:10:00:01:00:04</td>
<td>10</td>
<td>20</td>
<td>sap:1/2/2:1.1</td>
<td>Dut-B</td>
</tr>
<tr>
<td>100</td>
<td>00:10:00:02:00:02</td>
<td>10</td>
<td>10</td>
<td>sap:1/2/2:1.1</td>
<td>Dut-B</td>
</tr>
<tr>
<td>100</td>
<td>00:10:00:02:00:03</td>
<td>10</td>
<td>10</td>
<td>sap:1/2/3:1.1</td>
<td>Dut-C</td>
</tr>
<tr>
<td>100</td>
<td>00:10:00:02:00:04</td>
<td>10</td>
<td>20</td>
<td>sap:1/2/3:1.1</td>
<td>Dut-C</td>
</tr>
</tbody>
</table>

ISID Route Table

<table>
<thead>
<tr>
<th>Fid</th>
<th>ISID</th>
<th>Ver.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>10001</td>
<td>10</td>
</tr>
<tr>
<td>100</td>
<td>10002</td>
<td>10</td>
</tr>
</tbody>
</table>

No. of ISID Routes: 2

A:Dut-A# show service id spb fate-sharing
```
User service fate-shared sap/sdp-bind information

<table>
<thead>
<tr>
<th>Control SvcId</th>
<th>Control Sap/ SdpBind</th>
<th>FID</th>
<th>User SvcId</th>
<th>User Sap/ SdpBind</th>
</tr>
</thead>
<tbody>
<tr>
<td>500</td>
<td>1/1/20:500</td>
<td>502</td>
<td>502</td>
<td>1/1/20:502</td>
</tr>
</tbody>
</table>

**spf**

**Syntax**
```
spf
```

**Context**
```
show>service>id>spb
```

**Description**
This command displays SPF information.

**Sample Output**
```
A:cses-B01# show service id spb spf
```

---

**Path Table**

---

**Sample Output**
```
Fwd Tree: unicast, ECT Alg: low-path-id
-----------------------------
cses-B07.00  sap:1/1/20:500  cses-B07
cses-B01.00  sap:1/1/20:500  cses-B07
cses-B07.00  sap:1/1/20:500  cses-B07
```

---

**Sample Output**
```
Fwd Tree: unicast, ECT Alg: high-path-id
-----------------------------
cses-B07.00  sap:1/1/20:500  cses-B07
cses-B01.00  sap:1/1/20:500  cses-B07
cses-B07.00  sap:1/1/20:500  cses-B07
```

---

**Sample Output**
```
Fwd Tree: multicast, ECT Alg: low-path-id
-----------------------------
cses-B07.00  sap:1/1/20:500  cses-B07
cses-B01.00  sap:1/1/20:500  cses-B07
cses-B07.00  sap:1/1/20:500  cses-B07
```

---

**Sample Output**
```
Fwd Tree: multicast, ECT Alg: high-path-id
-----------------------------
cses-B07.00  sap:1/1/20:500  cses-B07
cses-B01.00  sap:1/1/20:500  cses-B07
cses-B07.00  sap:1/1/20:500  cses-B07
```

---

**Spf-log**

**Syntax**
```
spf-log
```
Context: show>service>id>spb

**Description**
This command displays SPF Log information.

**Output**

A:cses-B01# show service id spb spf-log

```
A:cses-B01# show service id spb spf-log

ISIS SPF Log

===============================================================================
<table>
<thead>
<tr>
<th>When</th>
<th>Duration</th>
<th>L1 Nodes</th>
<th>L2 Nodes</th>
<th>Event Count</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>07/23/2012 16:01:13</td>
<td>&lt;0.01s</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>Reg</td>
</tr>
<tr>
<td>07/23/2012 16:01:19</td>
<td>&lt;0.01s</td>
<td>1</td>
<td>0</td>
<td>4</td>
<td>Reg</td>
</tr>
<tr>
<td>07/23/2012 16:01:24</td>
<td>&lt;0.01s</td>
<td>3</td>
<td>0</td>
<td>2</td>
<td>Reg</td>
</tr>
<tr>
<td>07/23/2012 16:01:29</td>
<td>&lt;0.01s</td>
<td>4</td>
<td>0</td>
<td>1</td>
<td>Reg</td>
</tr>
</tbody>
</table>

Log Entries : 4
```

**statistics**

**Syntax**
statistics

**Context**
show>service>id>spb

**Description**
This command displays SPB statistics.

**Output**

A:cses-B01# show service id spb statistics

```
A:cses-B01# show service id spb statistics

ISIS Statistics

<table>
<thead>
<tr>
<th>ISIS Instance</th>
<th>SPF Runs</th>
<th>LSP Regens.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1024</td>
<td>4</td>
<td>11</td>
</tr>
</tbody>
</table>

CSPF Statistics

<table>
<thead>
<tr>
<th>Requests</th>
<th>Request Drops</th>
<th>Paths Found</th>
<th>Paths Not Found</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

PDU Type | Received | Processed | Dropped | Sent | Retransmitted |
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>LSP</td>
<td>31</td>
<td>31</td>
<td>0</td>
<td>9</td>
<td>0</td>
</tr>
<tr>
<td>IIH</td>
<td>532</td>
<td>532</td>
<td>0</td>
<td>533</td>
<td>0</td>
</tr>
<tr>
<td>CSNP</td>
<td>479</td>
<td>479</td>
<td>0</td>
<td>479</td>
<td>0</td>
</tr>
<tr>
<td>PSNP</td>
<td>9</td>
<td>9</td>
<td>0</td>
<td>27</td>
<td>0</td>
</tr>
<tr>
<td>Unknown</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
```

**status**

**Syntax**
status
**Context**
show>service>id>spb

**Description**
This command displays SPB status.

**Output**
Sample Output

```
A:cses-B01# show service id spb status

isis status

System Id        : 0000.00AA.AAAA
Admin State      : Up
Oper State       : Up
SPB Routing      : Enabled
Last Enabled     : 07/23/2012 16:01:06
Level Capability : L1
Authentication Check : True
Authentication Type : None
CSNP-Authentication : Enabled
HELLO-Authentication : Enabled
PSNP-Authentication : Enabled
Overload-On-Boot Time*: 0
LSP Lifetime     : 1200
LSP Wait         : 5 sec (Max) 0 sec (Initial) 1 sec (Second)
LSP MTU Size     : 1492 (Config) 1492 (Oper)
Adjacency Check  : loose
L1 Auth Type     : none
L1 CSNP-Authenticati*: Enabled
L1 HELLO-Authenticat*: Enabled
L1 PSNP-Authenticati*: Enabled
L1 Preference    : 15
L1 Ext. Preference : 160
L1 Wide Metrics  : Enabled
L1 LSDB Overload : Disabled
L1 LSPs          : 4
L1 Default Metric : 10
L1 IPV6 Def Metric : 10
Last SPF         : 07/23/2012 16:01:29
SPF Wait         : 10 sec (Max) 1000 ms (Initial) 1000 ms (Second)
Multi-topology   : Disabled
Area Addresses   : 00
Total Exp Routes (L1) : 0
IID TLV          : Disabled
All-L1-MacAddr   : 01:80:c2:00:00:14
```

PBB Clear Commands

counters

Syntax counters
Context clear>service>statistics>id
Description This command clears all traffic queue counters associated with the service ID.

mesh-sdp

Syntax mesh-sdp sdp-id[:vc-id] {all | counters | stp | mrp}
Context clear>service>statistics>id
Description This command clears the statistics for a particular mesh SDP bind.
Parameters sdp-id — Specifies the SDP ID for which to display information.
   Default All SDPs.
   Values 1 — 17407
vc-id — Displays information about the virtual circuit identifier.
   Values 1 — 4294967295
all — Clears all queue statistics and STP statistics associated with the SDP.
counters — Clears all queue statistics associated with the SDP.
stp — Clears all STP statistics associated with the SDP.
mrp — Clears all MRP statistics associated with the SDP.

mrp

Syntax mrp
Context clear>service>statistics>id
Description This command clears all MRP statistics for the service ID.

spoke-sdp

Syntax spoke-sdp sdp-id[:vc-id] {all | counters | stp | l2pt | mrp}
Context clear>service>statistics>id
Description
This command clears statistics for the spoke SDP bound to the service.

Parameters
sdp-id — The spoke SDP ID for which to clear statistics.

Values
1 — 17407

vc-id — The virtual circuit ID on the SDP ID to be reset.

Values
1 — 4294967295

Values
all — Clears all queue statistics and STP statistics associated with the SDP.
counters — Clears all queue statistics associated with the SDP.
stp — Clears all STP statistics associated with the SDP.
l2pt — Clears all L2PT statistics associated with the SDP.
mrp — Clears all MRP statistics associated with the SDP.

sap

Syntax
sap sap-id {all | counters | stp | l2pt | mrp}

Context
clear>service>statistics>id

Description
This command clears statistics for the SAP.

Parameters
sap-id — The SAP ID for which to clear statistics.

Values
all — Clears all queue statistics and STP statistics associated with the SAP.
counters — Clears all queue statistics associated with the SAP.
stp — Clears all STP statistics associated with the SAP.
l2pt — Clears all L2PT statistics associated with the SAP.
mrp — Clears all MRP statistics associated with the SAP.

stp

Syntax
stp

Context
clear>service>statistics>id

Description
Clears all spanning tree statistics for the service ID.
PBB Debug Commands

mrp

Syntax: [no] mrp
Context: debug>service>id
Description: This command enables and configures MRP debugging.

all-events

Syntax: all-events
Context: debug>service>id>mrp
Description: This command enables MRP debugging for the applicant, leave all, periodic and registrant state machines and enables debugging of received and transmutted MRP PDUs.

applicant-sm

Syntax: [no] applicant-sm
Context: debug>service>id>mrp
Description: This command enables debugging of the applicant state machine.
The no form of the command disables debugging of the applicant state machine.

leave-all-sm

Syntax: [no] leave-all-sm
Context: debug>service>id>mrp
Description: This command enables debugging of the leave all state machine.
The no form of the command disables debugging of the leave all state machine.

mmrp-mac

Syntax: [no] mmrp-mac ieee-address
Context: debug>service>id>mrp
**mrpdu**

- **Syntax**  
  ```  
  [no] mrpdu  
  ```

- **Context**  
  `debug>service?id>mrp`

- **Description**  
  This command enables debugging of the MRP PDUs that are received or transmitted.  
  The **no** form of the command disables debugging of MRP PDUs.

**periodic-sm**

- **Syntax**  
  ```  
  [no] periodic-sm  
  ```

- **Context**  
  `debug>service?id>mrp`

- **Description**  
  This command enables debugging of the periodic state machine.  
  The **no** form of the command disables debugging of the periodic state machine.

**registrant-sm**

- **Syntax**  
  ```  
  [no] registrant-sm  
  ```

- **Context**  
  `debug>service?id>mrp`

- **Description**  
  This command enables debugging of the registrant state machine.  
  The **no** form of the command disables debugging of the registrant state machine.

**sap**

- **Syntax**  
  ```  
  [no] sap sap-id  
  ```

- **Context**  
  `debug>service?id>mrp`

- **Description**  
  This command filters debug events and only shows events for the particular SAP.  
  The **no** form of the command removes the debug filter.

- **Parameters**  
  `sap-id` — See Common CLI Command Descriptions on page 1469 for command syntax.
sdp

Syntax  [no] sdp sdp-id:vc-id

Context  debug>service>id>mrp

Description  This command filters debug events and only shows events for the particular SDP. The no form of the command removes the debug filter.

Parameters  sdp-id — Specifies the SDP ID for which to display information.

  Default  All SDPs.

  Values  1 — 17407

vc-id — Displays information about the virtual circuit identifier.

  Values  1 — 4294967295
IES Show Commands

customer

Syntax  customer [customer-id] [site customer-site-name]

Context  show>service

Description  This command displays service customer information.

Parameters  

- **customer-id** — Displays only information for the specified customer ID.
  
  **Default**  All customer IDs display
  
  **Values**  1 — 2147483647

- **site customer-site-name** — Specifies the customer site which is an anchor point for an ingress and egress virtual scheduler hierarchy.

Output  Show Customer Command Output — The following table describes show customer command output fields:

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer-ID</td>
<td>The ID that uniquely identifies a customer.</td>
</tr>
<tr>
<td>Contact</td>
<td>The name of the primary contact person.</td>
</tr>
<tr>
<td>Description</td>
<td>Generic information about the customer.</td>
</tr>
<tr>
<td>Phone</td>
<td>The phone/pager number to reach the primary contact person.</td>
</tr>
<tr>
<td>Total Customers</td>
<td>The total number of customers configured.</td>
</tr>
<tr>
<td>Multi-service site Site</td>
<td>Multi-service site name. A multi-service customer site is a group of SAPs with common origination and termination points.</td>
</tr>
<tr>
<td>Description</td>
<td>Information about a specific customer's multi-service site.</td>
</tr>
<tr>
<td>Assignment</td>
<td>The port ID, MDA, or card number, where the SAP's that are members of this multi-service site are defined.</td>
</tr>
<tr>
<td>I. Sched Pol</td>
<td>The ingress QoS scheduler policy assigned to this multi-service site.</td>
</tr>
<tr>
<td>E. Sched Pol</td>
<td>The egress QoS scheduler policy assigned to this multi-service site.</td>
</tr>
<tr>
<td>Service Association Service-ID</td>
<td>The ID that uniquely identifies a service.</td>
</tr>
<tr>
<td>SAP</td>
<td>Specifies the SAP assigned to the service.</td>
</tr>
</tbody>
</table>
Sample Output

*A:ALA-12# show service customer
==============================================================================
Customer-ID : 1
Contact : Manager
Description : Default customer
Phone : (123) 555-1212

Customer-ID : 2
Contact : Tech Support
Description : TiMetra Networks
Phone : (234) 555-1212

Customer-ID : 3
Contact : Fred
Description : TiMetra Networks
Phone : (345) 555-1212

Customer-ID : 6
Contact : Ethel
Description : Epipe Customer
Phone : (456) 555-1212

Customer-ID : 7
Contact : Lucy
Description : ABC Customer
Phone : (567) 555-1212

Customer-ID : 8
Contact : Customer Service
Description : IES Customer
Phone : (678) 555-1212

Customer-ID : 274
Contact : Mssrs. Beaucoup
Description : ABC Company
Phone : 650 123-4567

Customer-ID : 94043
Contact : Test Engineer on Duty
Description : TEST Customer
Phone : (789) 555-1212
==============================================================================
Total Customers : 8
==============================================================================
*A:ALA-12#

*A:ALA-12# show service customer 274
==============================================================================
Customer : 274
==============================================================================
Customer-ID : 274
Contact : Mssrs. Beaucoup
Description : ABC Company
Phone : 650 123-4567
Multi Service Site

Site : west
Description : (Not Specified)

*A:ALA-12#

*A:ALA-12# show service customer 274 site west

Customer 274

Customer-ID : 274
Contact : Mssrs. Beaucoup
Description : ABC Company
Phone : 650 123-4567

Multi Service Site

Site : west
Description : (Not Specified)
Assignment : Card 5
I. Sched Pol: SLA1
E. Sched Pol: (Not Specified)

Service Association

No Service Association Found.

*A:ALA-12#

sap-using

Syntax

sap-using [msap] [dyn-script] [description]
sap-using [sap sap-id] [vlan-translation | anti-spoof] [description]
sap-using [sap sap-id]
sap-using interface [ip-address | ip-int-name]
sap-using [ingress | egress] filter filter-id
sap-using [ingress | qos-policy] qos-policy-id

Context

show>service

Description
Displays SAP information.

If no optional parameters are specified, the command displays a summary of all defined SAPs. The optional parameters restrict output to only SAPs matching the specified properties.

Parameters

sap sap-id — Specifies the physical port identifier portion of the SAP definition. See Common CLI Command Descriptions on page 1783 for command syntax.

ingress — Specifies matching an ingress policy.

egress — Specifies matching an egress policy.

filter filter-id — The ingress or egress filter policy ID for which to display matching SAPs.

Values

1 — 65535
**dyn-script** — Displays dynamic service SAPs information.

**interface** — Specifies matching SAPs with the specified IP interface.

**ip-addr** — The IP address of the interface for which to display matching SAPs.

**Values**

1.0.0.0 — 223.255.255.255

**ip-int-name** — The IP interface name for which to display matching SAPs.

**Output**

**Show Service SAP** — The following table describes show service SAP output fields:

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port ID</td>
<td>The ID of the access port where the SAP is defined.</td>
</tr>
<tr>
<td>Svc ID</td>
<td>The value that identifies the service.</td>
</tr>
<tr>
<td>Igr.QoS</td>
<td>The SAP ingress QoS policy number specified on the ingress SAP.</td>
</tr>
<tr>
<td>Ing.Fltr</td>
<td>The MAC or IP filter policy ID applied to the ingress SAP.</td>
</tr>
<tr>
<td>Egr.Fltr</td>
<td>The MAC or IP filter policy ID applied to the egress SAP.</td>
</tr>
<tr>
<td>Adm</td>
<td>The administrative state of the SAP.</td>
</tr>
<tr>
<td>Opr</td>
<td>The actual state of the SAP.</td>
</tr>
</tbody>
</table>

**Sample Output**

```
*A:ALA-48# show service sap-using sap 2/1/10:0
---------------------------------------------------------------
Service Access Points Using Port 2/1/10:0
---------------------------------------------------------------
<table>
<thead>
<tr>
<th>PortId</th>
<th>SvcId</th>
<th>Ing. QoS</th>
<th>Ing. Fltr</th>
<th>Egr. QoS</th>
<th>Egr. Fltr</th>
<th>Adm</th>
<th>Opr</th>
</tr>
</thead>
<tbody>
<tr>
<td>2/1/10:0</td>
<td>13</td>
<td>1</td>
<td>none</td>
<td>1</td>
<td>none</td>
<td>Up</td>
<td>Down</td>
</tr>
</tbody>
</table>
---------------------------------------------------------------
Number of SAPs : 1
---------------------------------------------------------------
```
service-using

Syntax  
```
service-using [ies] [customer customer-id]
```

Context  
```
show>service
```

Description  
This command displays the services matching certain usage properties. If no optional parameters are specified, all services defined on the system are displayed.

Parameters  
```
ies — Displays matching IES services.
customer customer-id — Displays services only associated with the specified customer ID.
```

Default  
```
Services associated with an customer.
```

Values  
```
1 — 2147483647
```

Output  
```
Show Service Service-Using — The following table describes show service service-using output fields:
```

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Id</td>
<td>The value that identifies the service.</td>
</tr>
<tr>
<td>Type</td>
<td>Specifies the service type configured for the service ID.</td>
</tr>
<tr>
<td>Adm</td>
<td>The administrative state of the service.</td>
</tr>
<tr>
<td>Opr</td>
<td>The operating state of the service.</td>
</tr>
<tr>
<td>CustomerID</td>
<td>The ID of the customer who owns this service.</td>
</tr>
<tr>
<td>Last Mgmt Change</td>
<td>The date and time of the most recent management-initiated change to this service.</td>
</tr>
</tbody>
</table>

Sample Output

```
A:ALA-48# show service service-using ies
===============================================================================
Services [ies]
===============================================================================
ServiceId    Type      Adm    Opr        CustomerId        Last Mgmt Change
-------------------------------------------------------------------------------
89           IES       Up     Down       8                 07/25/2006 15:46:28
104          IES       Up     Down       1                 07/25/2006 15:46:28
200          IES       Up     Down       1                 07/25/2006 15:46:28
321          IES       Up     Down       1                 07/25/2006 15:46:28
322          IES       Down   Down       1                 07/25/2006 15:46:28
1001         IES       Up     Down       1730              07/25/2006 15:46:28
-------------------------------------------------------------------------------
Matching Services : 8
-------------------------------------------------------------------------------
A:ALA-48#
```
id

**Syntax**
```plaintext
id service-id {all | arp | base | sap}
```

**Context**
```
show>service
```

**Description**
This command displays information for a particular service-id.

**Parameters**
- `service-id` — The unique service identification number to identify the service in the service domain.
- `all` — Display detailed information about the service.
- `arp` — Display ARP entries for the service.
- `base` — Display basic service information.
- `interface` — Display service interfaces.
- `sap` — Display SAPs associated to the service.

---

all

**Syntax**
```plaintext
all
```

**Context**
```
show>service>id
```

**Description**
This command displays detailed information for all aspects of the service.

**Output**
**Show All Service-ID Output** — The following table describes the show all service-id command output fields:

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Id</td>
<td>The service identifier.</td>
</tr>
<tr>
<td>VPN Id</td>
<td>The number which identifies the VPN.</td>
</tr>
<tr>
<td>Service Type</td>
<td>Specifies the type of service.</td>
</tr>
<tr>
<td>SDP Id</td>
<td>The SDP identifier.</td>
</tr>
<tr>
<td>Description</td>
<td>Generic information about the service.</td>
</tr>
<tr>
<td>Customer Id</td>
<td>The customer identifier.</td>
</tr>
<tr>
<td>Last Mgmt Change</td>
<td>The date and time of the most recent management-initiated change to this customer.</td>
</tr>
<tr>
<td>SAP Count</td>
<td>The number of SAPs specified for this service.</td>
</tr>
<tr>
<td>SDP Bind Count</td>
<td>The number of SDPs bound to this service.</td>
</tr>
<tr>
<td>Label</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Service Destination Points (SDPs)</td>
<td></td>
</tr>
<tr>
<td>SDP Id</td>
<td>The SDP identifier.</td>
</tr>
<tr>
<td>Type</td>
<td>Indicates whether this Service SDP binding is a spoke or a mesh.</td>
</tr>
<tr>
<td>Admin Path MTU</td>
<td>The largest service frame size (in octets) that can be transmitted through this SDP to the far-end router, without requiring the packet to be fragmented.</td>
</tr>
<tr>
<td>Oper Path MTU</td>
<td>The actual largest service frame size (in octets) that can be transmitted through this SDP to the far-end router, without requiring the packet to be fragmented.</td>
</tr>
<tr>
<td>Delivery</td>
<td>Specifies the type of delivery used by the SDP: GRE or MPLS.</td>
</tr>
<tr>
<td>Admin State</td>
<td>The administrative state of this SDP.</td>
</tr>
<tr>
<td>Oper State</td>
<td>The operational state of this SDP.</td>
</tr>
<tr>
<td>Ingress Label</td>
<td>The label used by the far-end device to send packets to this device in this service by this SDP.</td>
</tr>
<tr>
<td>Egress Label</td>
<td>The label used by this device to send packets to the far-end device in this service by this SDP.</td>
</tr>
<tr>
<td>Ingress Filter</td>
<td>The ID of the ingress filter policy.</td>
</tr>
<tr>
<td>Egress Filter</td>
<td>The ID of the egress filter policy.</td>
</tr>
<tr>
<td>Far End</td>
<td>Specifies the IP address of the remote end of the GRE or MPLS tunnel defined by this SDP.</td>
</tr>
<tr>
<td>Last Changed</td>
<td>The date and time of the most recent change to this customer.</td>
</tr>
<tr>
<td>Signaling</td>
<td>Specifies the signaling protocol used to obtain the ingress and egress labels used in frames transmitted and received on this SDP.</td>
</tr>
<tr>
<td>Admin State</td>
<td>Specifies the operating status of the service.</td>
</tr>
<tr>
<td>Oper State</td>
<td>The current status of the service.</td>
</tr>
<tr>
<td>Hello Time</td>
<td>Specifies how often the SDP echo request messages are transmitted on this SDP.</td>
</tr>
<tr>
<td>Hello Msg Len</td>
<td>Specifies the length of the SDP echo request messages transmitted on this SDP.</td>
</tr>
<tr>
<td>Max Drop Count</td>
<td>Specifies the maximum number of consecutive SDP Echo Request messages that can be unacknowledged before the keepalive protocol reports a fault.</td>
</tr>
<tr>
<td>Hold Down Time</td>
<td>Specifies the amount of time to wait before the keepalive operating status is eligible to enter the alive state.</td>
</tr>
<tr>
<td>Label</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SDP Delivery Mechanism</td>
<td>When the SDP type is MPLS, a list of LSPs used to reach the far-end router displays. All the LSPs in the list must terminate at the IP address specified in the far-end field. If the SDP type is GRE, then the following message displays: “SDP Delivery Mechanism is not MPLS”</td>
</tr>
<tr>
<td>Number of SDPs</td>
<td>The total number SDPs applied to this service ID.</td>
</tr>
<tr>
<td>Service Access Points</td>
<td></td>
</tr>
<tr>
<td>Service Id</td>
<td>The service identifier.</td>
</tr>
<tr>
<td>Port Id</td>
<td>The ID of the access port where this SAP is defined.</td>
</tr>
<tr>
<td>Description</td>
<td>Generic information about the SAP.</td>
</tr>
<tr>
<td>Encap</td>
<td>The value of the label used to identify this SAP on the access port.</td>
</tr>
<tr>
<td>Admin State</td>
<td>The desired state of the SAP.</td>
</tr>
<tr>
<td>Oper State</td>
<td>The operating state of the SAP.</td>
</tr>
<tr>
<td>Last Changed</td>
<td>The date and time of the last change.</td>
</tr>
<tr>
<td>Admin MTU</td>
<td>The largest service frame size (in octets) that can be transmitted through this SDP to the far-end router, without requiring the packet to be fragmented.</td>
</tr>
<tr>
<td>Oper MTU</td>
<td>The actual largest service frame size (in octets) that can be transmitted through this SDP to the far-end router, without requiring the packet to be fragmented.</td>
</tr>
<tr>
<td>Ingress qos-policy</td>
<td>The SAP ingress QoS policy ID.</td>
</tr>
<tr>
<td>Egress qos-policy</td>
<td>The SAP egress QoS policy ID.</td>
</tr>
<tr>
<td>Ingress Filter-Id</td>
<td>The SAP ingress filter policy ID.</td>
</tr>
<tr>
<td>Egress Filter-Id</td>
<td>The SAP egress filter policy ID.</td>
</tr>
<tr>
<td>Multi Svc Site</td>
<td>Indicates the multi-service site that the SAP is a member.</td>
</tr>
<tr>
<td>Ingress sched-policy</td>
<td>Indicates the ingress QoS scheduler for the SAP.</td>
</tr>
<tr>
<td>Egress sched-policy</td>
<td>Indicates the egress QoS scheduler for the SAP.</td>
</tr>
<tr>
<td>Acct. Pol</td>
<td>Indicates the accounting policy applied to the SAP.</td>
</tr>
<tr>
<td>Collect Stats</td>
<td>Specifies whether accounting statistics are collected on the SAP.</td>
</tr>
<tr>
<td>SAP Statistics</td>
<td></td>
</tr>
<tr>
<td>Dropped</td>
<td>The number of packets or octets dropped.</td>
</tr>
<tr>
<td>Label</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Offered Hi Priority</td>
<td>The number of high priority packets, as determined by the SAP ingress QoS policy.</td>
</tr>
<tr>
<td>Offered Low Priority</td>
<td>The number of low priority packets, as determined by the SAP ingress QoS policy.</td>
</tr>
<tr>
<td>Forwarded In Profile</td>
<td>The number of in-profile packets or octets (rate below CIR) forwarded.</td>
</tr>
<tr>
<td>Forwarded Out Profile</td>
<td>The number of out-of-profile packets or octets (rate above CIR) forwarded.</td>
</tr>
</tbody>
</table>

**Queueing Stats**

- **Dropped In Profile**: The number of in-profile packets or octets discarded.
- **Dropped Out Profile**: The number of out-of-profile packets or octets discarded.
- **Forwarded In Profile**: The number of in-profile packets or octets (rate below CIR) forwarded.
- **Forwarded Out Profile**: The number of out-of-profile packets or octets (rate above CIR) forwarded.

**SAP per Queue stats**

- **Ingress Queue 1**: The index of the ingress QoS queue of this SAP.
- **High priority offered**: The packets or octets count of the high priority traffic for the SAP.
- **High priority dropped**: The number of high priority traffic packets/octets dropped.
- **Low priority offered**: The packets or octets count of the low priority traffic.
- **Low priority dropped**: The number of low priority traffic packets/octets dropped.
- **In profile forwarded**: The number of in-profile packets or octets (rate below CIR) forwarded.
- **Out profile forwarded**: The number of out-of-profile octets (rate above CIR) forwarded.
- **Egress Queue 1**: The index of the egress QoS queue of the SAP.
- **In profile forwarded**: The number of in-profile packets or octets (rate below CIR) forwarded.

**IPCP Address Extension Details**

- **In profile dropped**: The number of in-profile packets or octets dropped for the SAP.
- **Peer IP Addr**: Specifies the remote IP address to be assigned to the far-end of the associated PPP/MLPPP link via IPCP extensions.
<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peer Pri DNS Addr</td>
<td>Specifies a unicast IPv4 address for the primary DNS server to be signaled to the far-end of the associate PPP/MLPPP link via IPCP extensions.</td>
</tr>
<tr>
<td>Peer Sec DNS Addr</td>
<td>Specifies a unicast IPv4 address for the secondary DNS server to be signaled to the far-end of the associate PPP/MLPPP link via IPCP extensions. (optional)</td>
</tr>
</tbody>
</table>
arp

Syntax  
arp [ip-address] | [mac ieee-address] | [sap sap-id] | [interface ip-int-name] [sdp sdp-id:vc-id]

Context  
show>service>id

Description  
Displays the ARP table for the IES instance. The ARP entries are displayed uniquely. Each MAC associated
with the child group-interfaces are displayed with each ARP entry. They do not reflect actual ARP entries
but are displayed along the interfaces ARP entry for easy lookup.

Parameters  
ip-address — Displays only ARP entries in the ARP table with the specified IP address.

  Default  All IP addresses.

mac ieee-address — Displays only ARP entries in the ARP table with the specified 48-bit MAC address.

  The MAC address can be expressed in the form aa:bb:cc:dd:ee:ff or aa-bb-cc-dd-ee-ff where aa, bb, cc,
  dd, ee and ff are hexadecimal numbers.

  Default  All MAC addresses.

sap sap-id — Displays SAP information for the specified SAP ID. See Common CLI Command

  Descriptions on page 1783 for command syntax.

  port-id — interface — Specifies matching service ARP entries associated with the IP interface.

  ip-address — The IP address of the interface for which to display matching ARP entries.

    Values  1.0.0.0 — 223.255.255.255

  ip-int-name — The IP interface name for which to display matching ARPs.

  sdp-id — The SDP identifier.

    Values  1 — 4294967295

Output  
Show Service-ID ARP — The following table describes show service-id ARP output fields.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>The IP address.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>The specified MAC address.</td>
</tr>
<tr>
<td>Type</td>
<td>Static — FDB entries created by management.</td>
</tr>
<tr>
<td></td>
<td>Learned — Dynamic entries created by the learning process.</td>
</tr>
<tr>
<td></td>
<td>OAM — Entries created by the OAM process.</td>
</tr>
<tr>
<td></td>
<td>Other — Local entries for the IP interfaces created.</td>
</tr>
<tr>
<td>Expiry</td>
<td>The age of the ARP entry.</td>
</tr>
<tr>
<td>Interface</td>
<td>The interface applied to the service.</td>
</tr>
<tr>
<td>SAP</td>
<td>The SAP ID.</td>
</tr>
</tbody>
</table>

Sample Output
Show, Clear, Debug Commands

base

Syntax base

Context show>service>id

Description This command displays basic information about this IES service.

Sample Output

*A:ALA-A# show service id 100 base

---------------------------------------------------------------
Service Basic Information
---------------------------------------------------------------
Service Id        : 100                 Vpn Id            : 100
Service Type      : IES
Description       : Default Ies description for service id 100
Customer Id       : 1
Last Status Change: 08/29/2006 17:44:28
Last Mgmt Change  : 08/29/2006 17:44:28
Admin State       : Up                  Oper State        : Up
SAP Count         : 2

-------------------------------------------------------------------------------
Service Access & Destination Points
-------------------------------------------------------------------------------
Identifier                       Type         AdmMTU  OprMTU  Adm     Opr
-------------------------------------------------------------------------------
sap:1/1/3                        null         1514    1514    Up      Up
sap:1/1/4                        null         1514    1514    Up      Up

===============================================================================
*A:ALA-A#
host-connectivity-verify

Syntax  
host-connectivity-verify statistics [sap sap-id]

Context  
show>service>id

Description  
Displays host connectivity check statistics.

Parameters  
statistics — Displays host connectivity verification data.

sap sap-id — See Common CLI Command Descriptions on page 1783 for command syntax.

Output  
Show Service Id Host Connectivity Verify — The following table describes show service-id host connectivity verification output fields:

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Svc Id</td>
<td>The service identifier.</td>
</tr>
<tr>
<td>SapId/SdpId</td>
<td>The SAP and SDP identifiers.</td>
</tr>
<tr>
<td>DestIp Address</td>
<td>The destination IP address.</td>
</tr>
<tr>
<td>Last Response</td>
<td>The time when the last response was received.</td>
</tr>
<tr>
<td>Time Expired</td>
<td>Displays whether the interval value has expired.</td>
</tr>
<tr>
<td>Oper State</td>
<td>Displays the current operational state of the service.</td>
</tr>
</tbody>
</table>

Sample Output

A:ALA-48>show>service>id# host-connectivity-verify statistics sap 1/1/9:0

----------------------------------------------------------
Host connectivity check statistics
----------------------------------------------------------
Svc   SapId/          DestIp          Last              Time            Oper
Id    SdpId           Address         Response           Expired State
----------------------------------------------------------
    1000  551/2/3:0       143.144.145.1 Up
----------------------------------------------------------
A:ALA-48>show>service>id#

interface

Syntax  
interface [ip-address | ip-int-name] [interface-type] [detail] [family]

Context  
show>service>id

Description  
This command displays information for the IP interfaces associated with the IES service. If no optional parameters are specified, a summary of all IP interfaces associated to the service are displayed.

Parameters  
ip-address — The IP address of the interface for which to display information.

Values  
ipv4-address: a.b.c.d (host bits must be 0)
ipv6-address: x:x:x:x:x:x:x (eight 16-bit pieces)

**Show, Clear, Debug Commands**

```
x:x:x:x:x:d.d.d
x: [0 — FFFF]H
d: [0 — 255]
```

*ip-int-name* — Specifies the IP interface name for which to display information.  
**Values** 32 characters maximum

*family* — Displays the router IP interface table to display.  
**Values**  
- ipv4 — Displays only those peers that have the IPv4 family enabled.  
- ipv6 — Displays the peers that are IPv6-capable.

*interface-type* — Specifies to display either group or interfaces.  
**Values** group, subscriber

*detail* — Displays detailed IP interface information.  
**Default** IP interface summary output.

**Output**  
Show Service-ID — The following table describes show service-id output fields.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>If Name</td>
<td>The name used to refer to the IES interface.</td>
</tr>
<tr>
<td>Type</td>
<td>Specifies the interface type.</td>
</tr>
<tr>
<td>IP-Address</td>
<td>Specifies the IP address/IP subnet/broadcast address of the interface.</td>
</tr>
<tr>
<td>Adm</td>
<td>The administrative state of the interface.</td>
</tr>
<tr>
<td>Opr</td>
<td>The operational state of the interface.</td>
</tr>
<tr>
<td>Admin State</td>
<td>The administrative state of the interface.</td>
</tr>
<tr>
<td>Oper State</td>
<td>The operational state of the interface.</td>
</tr>
<tr>
<td>IP Addr/mask</td>
<td>Specifies the IP address/IP subnet/broadcast address of the interface.</td>
</tr>
<tr>
<td>If Index</td>
<td>The index corresponding to this IES interface. The primary index is 1; all IES interfaces are defined in the base virtual router context.</td>
</tr>
<tr>
<td>If Type</td>
<td>Specifies the interface type.</td>
</tr>
<tr>
<td>SAP Id</td>
<td>Specifies the SAP's port ID.</td>
</tr>
<tr>
<td>SNTP B.Cast</td>
<td>Specifies whether SNTP broadcast client mode is enabled or disabled.</td>
</tr>
<tr>
<td>Arp Timeout</td>
<td>Specifies the timeout for an ARP entry learned on the interface.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>Specifies the 48-bit IEEE 802.3 MAC address.</td>
</tr>
<tr>
<td>ICMP Mask Reply</td>
<td>Specifies whether ICMP mask reply is enabled or disabled.</td>
</tr>
<tr>
<td>Cflowd</td>
<td>Specifies whether Cflowd collection and analysis on the interface is enabled or disabled.</td>
</tr>
</tbody>
</table>
Sample Output

A:ALA-49# show service id 88 interface

<table>
<thead>
<tr>
<th>Interface-Name</th>
<th>Adm</th>
<th>Opr(v4/v6)</th>
<th>Type</th>
<th>Port/SapId</th>
<th>PfxState</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sector A</td>
<td>Up</td>
<td>Down/Down</td>
<td>IES</td>
<td>1/1/2.2</td>
<td>n/a</td>
</tr>
<tr>
<td>test</td>
<td>Up</td>
<td>Down/Down</td>
<td>IES</td>
<td>1/1/2:0</td>
<td>n/a</td>
</tr>
<tr>
<td>1.1.1.1/31</td>
<td></td>
<td></td>
<td>IES</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>1.1.1.1/31</td>
<td></td>
<td></td>
<td>IES</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>1.1.2.1/31</td>
<td></td>
<td></td>
<td>IES</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>test2?</td>
<td>Up</td>
<td>Up/--</td>
<td>IES Sub subscriber</td>
<td>n/a</td>
<td></td>
</tr>
<tr>
<td>192.168.10.21/24</td>
<td>Up</td>
<td>Down/--</td>
<td>IES Grp 1/2/2</td>
<td>n/a</td>
<td></td>
</tr>
<tr>
<td>Interfaces : 4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

A:ALA-49#

labels

Syntax labels

Context show>service>id

Description Displays the labels being used by the service.

Output Show Service-ID Labels — The following table describes show service-id labels output fields:

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Svc Id</td>
<td>The service identifier.</td>
</tr>
<tr>
<td>Sdp Id</td>
<td>The SDP identifier.</td>
</tr>
<tr>
<td>Type</td>
<td>Indicates whether the SDP is a spoke or a mesh.</td>
</tr>
<tr>
<td>I.Lbl</td>
<td>The VC label used by the far-end device to send packets to this device in this service by the SDP.</td>
</tr>
<tr>
<td>E.Lbl</td>
<td>The VC label used by this device to send packets to the far-end device in this service by the SDP.</td>
</tr>
</tbody>
</table>
### Sample Output

*A:ALA-12# show service id 1 labels

Martini Service Labels

<table>
<thead>
<tr>
<th>Svc Id</th>
<th>Sdp Id</th>
<th>Type</th>
<th>I.Lbl</th>
<th>E.Lbl</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>10:1</td>
<td>Mesh</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>20:1</td>
<td>Mesh</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>30:1</td>
<td>Mesh</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>40:1</td>
<td>Mesh</td>
<td>130081</td>
<td>131061</td>
</tr>
<tr>
<td>1</td>
<td>60:1</td>
<td>Mesh</td>
<td>131019</td>
<td>131016</td>
</tr>
<tr>
<td>1</td>
<td>100:1</td>
<td>Mesh</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Number of Bound SDPs : 6

*A:ALA-12#
VPRN Show Commands

egress-label

**Syntax**  
`egress-label egress-label1 [egress-label2]`

**Context**  
`show>service`

**Description**  
Display services using the range of egress labels.

If only the mandatory `egress-label1` parameter is specified, only services using the specified label are displayed.

If both `egress-label1` and `egress-label2` parameters are specified, the services using the range of labels `X` where `egress-label1 <= X <= egress-label2` are displayed.

Use the `show router ldp bindings` command to display dynamic labels.

**Parameters**  
`egress-label1` — The starting egress label value for which to display services using the label range. If only `egress-label1` is specified, services only using `egress-label1` are displayed.

- **Values**  
  0, 2049 — 131071

`egress-label2` — The ending egress label value for which to display services using the label range.

- **Default**  
  The `egress-label1` value.

- **Values**  
  2049 — 131071

**Output**  
**Show Service Egress Command Output** — The following table describes show service egress label output fields.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Svc Id</td>
<td>The ID that identifies a service.</td>
</tr>
<tr>
<td>Sdp Id</td>
<td>The ID that identifies an SDP.</td>
</tr>
<tr>
<td>Type</td>
<td>Indicates whether the SDP binding is a spoke or a mesh.</td>
</tr>
<tr>
<td>I. Lbl</td>
<td>The VC label used by the far-end device to send packets to this device in this service by the SDP.</td>
</tr>
<tr>
<td>E. Lbl</td>
<td>The VC label used by this device to send packets to the far-end device in this service by the SDP.</td>
</tr>
<tr>
<td>Number of bindings found</td>
<td>The total number of SDP bindings that exist within the specified egress label range.</td>
</tr>
</tbody>
</table>
Sample Output

*A:ALA-12# show service egress-label 0 10000

==============================================================================
Martini Service Labels
==============================================================================

<table>
<thead>
<tr>
<th>Svc Id</th>
<th>Sdp Id</th>
<th>Type</th>
<th>ILbl</th>
<th>ELbl</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>10:1</td>
<td>Mesh</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>20:1</td>
<td>Mesh</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>30:1</td>
<td>Mesh</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>100:1</td>
<td>Mesh</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>...</td>
<td>107:1</td>
<td>Mesh</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>108:1</td>
<td>Mesh</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>300:1</td>
<td>Mesh</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>301:1</td>
<td>Mesh</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>302:1</td>
<td>Mesh</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>400:1</td>
<td>Mesh</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>500:2</td>
<td>Spok</td>
<td>131070</td>
<td>2001</td>
</tr>
<tr>
<td>1</td>
<td>501:1</td>
<td>Mesh</td>
<td>131069</td>
<td>2000</td>
</tr>
<tr>
<td>100</td>
<td>300:100</td>
<td>Spok</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>200</td>
<td>301:200</td>
<td>Spok</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>300</td>
<td>302:300</td>
<td>Spok</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>400</td>
<td>400:400</td>
<td>Spok</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Number of Bindings Found : 23

==============================================================================
*A:ALA-12#

ingress-label

**Syntax**  ingress-label start-label [end-label]

**Context**  show>service

**Description**  Display services using the range of ingress labels.

If only the mandatory `start-label` parameter is specified, only services using the specified label are displayed.

If both `start-label` and `end-label` parameters are specified, the services using the range of labels X where `start-label <= X <= end-label` are displayed.

Use the `show router vprn-service-id ldp bindings` command to display dynamic labels.

**Parameters**

- **start-label** — The starting ingress label value for which to display services using the label range. If only `start-label` is specified, services only using `start-label` are displayed.
  
  **Values**  0, 2048 — 131071

- **end-label** — The ending ingress label value for which to display services using the label range.
  
  **Default**  The `start-label` value.

  **Values**  2048 — 131071

**Output**  **Show Service Ingress-Label** — The following table describes show service ingress-label output fields:
Sample Output

*A:ALa-12#  show service ingress-label 0

Martini Service Labels

<table>
<thead>
<tr>
<th>Svc Id</th>
<th>Sdp Id</th>
<th>Type</th>
<th>I.Lbl</th>
<th>E.Lbl</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>10:1</td>
<td>Mesh</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>20:1</td>
<td>Mesh</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>30:1</td>
<td>Mesh</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>50:1</td>
<td>Mesh</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>100:1</td>
<td>Mesh</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>101:1</td>
<td>Mesh</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>102:1</td>
<td>Mesh</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>103:1</td>
<td>Mesh</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>104:1</td>
<td>Mesh</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>105:1</td>
<td>Mesh</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>106:1</td>
<td>Mesh</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>107:1</td>
<td>Mesh</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>108:1</td>
<td>Mesh</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>300:1</td>
<td>Mesh</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>301:1</td>
<td>Mesh</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>302:1</td>
<td>Mesh</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>400:1</td>
<td>Mesh</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>100</td>
<td>300:100</td>
<td>Spok</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>200</td>
<td>301:200</td>
<td>Spok</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>300</td>
<td>302:300</td>
<td>Spok</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>400</td>
<td>400:400</td>
<td>Spok</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Number of Bindings Found : 21

*A:ALa-12#
Show, Clear, Debug Commands

**sap-using**

**Syntax**

- `sap-using [msap] [dyn-script] [description]`
- `sap-using [sap sap-id] [vlan-translation | anti-spoof] [description]`
- `sap-using [sap sap-id]`  
  `sap-using interface [ip-address | ip-int-name]`
- `sap-using [ingress | egress] atm-td-profile td-profile-id`
- `sap-using [ingress | egress] filter filter-id`
- `sap-using [ingress | egress] qos-policy qos-policy-id`
- `sap-using authentication-policy policy-name`

**Context**

- `show>service`

**Description**

This command displays SAP information.

If no optional parameters are specified, the command displays a summary of all defined SAPs.

The optional parameters restrict output to only SAPs matching the specified properties.

**Parameters**

- `sap-id` — Specifies the physical port identifier portion of the SAP definition. See [Common CLI Command Descriptions](#) on page 1783 for command syntax.

- `interface` — Specifies matching SAPs with the specified IP interface.

- `ip-address` — The IP address of the interface for which to display matching SAPs.

  **Values**

  - `1.0.0.0 — 223.255.255.255`

- `ip-int-name` — The IP interface name for which to display matching SAPs.

- `dyn-script` — Displays dynamic service SAPs information.

- `ingress` — Specifies matching an ingress policy.

- `egress` — Specifies matching an egress policy.

- `qos-policy qos-policy-id` — The ingress or egress QoS Policy ID for which to display matching SAPs.

  **Values**

  - `1 — 65535`

- `atm-td-profile td-profile-id` — Displays SAPs using this traffic description.

- `filter filter-id` — The ingress or egress filter policy ID for which to display matching SAPs.

  **Values**

  - `1 — 65535`

- `authentication-policy policy name` — Specifies an existing authentication policy.

**Output**

**Show Service SAP** — The following table describes show service SAP output fields:

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port ID</td>
<td>The ID of the access port where the SAP is defined.</td>
</tr>
<tr>
<td>Svc ID</td>
<td>The service identifier.</td>
</tr>
<tr>
<td>SapMTU</td>
<td>The SAP MTU value.</td>
</tr>
<tr>
<td>I.QoS</td>
<td>The SAP ingress QoS Policy number specified on the ingress SAP.</td>
</tr>
<tr>
<td>I.MAC/IP</td>
<td>The MAC or IP filter policy ID applied to the ingress SAP.</td>
</tr>
</tbody>
</table>
Sample Output

*A:ALA-12# show service sap-using sap 1/1

Service Access Points

<table>
<thead>
<tr>
<th>PortId</th>
<th>SvcId</th>
<th>SapMTU</th>
<th>I.QoS</th>
<th>I.Mac/IP</th>
<th>E.QoS</th>
<th>E.Mac/IP</th>
<th>A.Pol</th>
<th>Adm</th>
<th>Opr</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1/7:0</td>
<td>1</td>
<td>1</td>
<td>10</td>
<td>8</td>
<td>10</td>
<td>none</td>
<td>none</td>
<td>Up</td>
<td>Up</td>
</tr>
<tr>
<td>1/1/11:0</td>
<td>100</td>
<td>1</td>
<td>1</td>
<td>none</td>
<td>1</td>
<td>none</td>
<td>none</td>
<td>Down</td>
<td>Down</td>
</tr>
<tr>
<td>1/1/7:300</td>
<td>300</td>
<td>1</td>
<td>10</td>
<td>none</td>
<td>10</td>
<td>none</td>
<td>1000</td>
<td>Up</td>
<td>Up</td>
</tr>
</tbody>
</table>

Number of SAPs : 3

*A:ALA-12#

*A:ALA-12# show service sap-using egress atm-td-profile 2

Service Access Points Using ATM Traffic Profile 2

<table>
<thead>
<tr>
<th>PortId</th>
<th>SvcId</th>
<th>I.QoS</th>
<th>I.Fltr</th>
<th>E.QoS</th>
<th>E.Fltr</th>
<th>A.Pol</th>
<th>Adm</th>
<th>Opr</th>
</tr>
</thead>
<tbody>
<tr>
<td>/1/1/0/11</td>
<td>511111</td>
<td>2</td>
<td>none</td>
<td>2</td>
<td>none</td>
<td>none</td>
<td>Up</td>
<td>Up</td>
</tr>
<tr>
<td>/1/1/0/12</td>
<td>511112</td>
<td>2</td>
<td>none</td>
<td>2</td>
<td>none</td>
<td>none</td>
<td>Up</td>
<td>Up</td>
</tr>
<tr>
<td>/1/1/0/13</td>
<td>511113</td>
<td>2</td>
<td>none</td>
<td>2</td>
<td>none</td>
<td>none</td>
<td>Up</td>
<td>Up</td>
</tr>
<tr>
<td>/1/1/0/14</td>
<td>511114</td>
<td>2</td>
<td>none</td>
<td>2</td>
<td>none</td>
<td>none</td>
<td>Up</td>
<td>Up</td>
</tr>
<tr>
<td>/1/1/0/15</td>
<td>511115</td>
<td>2</td>
<td>none</td>
<td>2</td>
<td>none</td>
<td>none</td>
<td>Up</td>
<td>Up</td>
</tr>
<tr>
<td>/1/1/0/16</td>
<td>511116</td>
<td>2</td>
<td>none</td>
<td>2</td>
<td>none</td>
<td>none</td>
<td>Up</td>
<td>Up</td>
</tr>
<tr>
<td>/1/1/0/17</td>
<td>511117</td>
<td>2</td>
<td>none</td>
<td>2</td>
<td>none</td>
<td>none</td>
<td>Up</td>
<td>Up</td>
</tr>
<tr>
<td>/1/1/0/18</td>
<td>511118</td>
<td>2</td>
<td>none</td>
<td>2</td>
<td>none</td>
<td>none</td>
<td>Up</td>
<td>Up</td>
</tr>
<tr>
<td>/1/1/0/19</td>
<td>511119</td>
<td>2</td>
<td>none</td>
<td>2</td>
<td>none</td>
<td>none</td>
<td>Up</td>
<td>Up</td>
</tr>
<tr>
<td>/1/1/0/20</td>
<td>511120</td>
<td>2</td>
<td>none</td>
<td>2</td>
<td>none</td>
<td>none</td>
<td>Up</td>
<td>Up</td>
</tr>
<tr>
<td>/1/1/0/21</td>
<td>511121</td>
<td>2</td>
<td>none</td>
<td>2</td>
<td>none</td>
<td>none</td>
<td>Up</td>
<td>Up</td>
</tr>
<tr>
<td>/1/1/0/22</td>
<td>511122</td>
<td>2</td>
<td>none</td>
<td>2</td>
<td>none</td>
<td>none</td>
<td>Up</td>
<td>Up</td>
</tr>
<tr>
<td>/1/1/0/23</td>
<td>511123</td>
<td>2</td>
<td>none</td>
<td>2</td>
<td>none</td>
<td>none</td>
<td>Up</td>
<td>Up</td>
</tr>
<tr>
<td>/1/1/0/24</td>
<td>511124</td>
<td>2</td>
<td>none</td>
<td>2</td>
<td>none</td>
<td>none</td>
<td>Up</td>
<td>Up</td>
</tr>
<tr>
<td>/1/1/0/25</td>
<td>511125</td>
<td>2</td>
<td>none</td>
<td>2</td>
<td>none</td>
<td>none</td>
<td>Up</td>
<td>Up</td>
</tr>
</tbody>
</table>

*A:ALA-12#

sdp

Syntax sd [sdp-id | far-end ip-address] [detail | keep-alive-history]

Context show>service
Description Displays SDP information.

If no optional parameters are specified, a summary SDP output for all SDPs is displayed.

Parameters

sdp-id — The SDP ID for which to display information.

<table>
<thead>
<tr>
<th>Default</th>
<th>All SDPs.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Values</td>
<td>1 — 17407</td>
</tr>
</tbody>
</table>

Far-end ip-address — Displays only SDPs matching with the specified far-end IP address.

<table>
<thead>
<tr>
<th>Default</th>
<th>SDPs with any far-end IP address.</th>
</tr>
</thead>
</table>

detail — Displays detailed SDP information.

<table>
<thead>
<tr>
<th>Default</th>
<th>SDP summary output.</th>
</tr>
</thead>
</table>

keep-alive-history — Displays the last fifty SDP keepalive events for the SDP.

<table>
<thead>
<tr>
<th>Default</th>
<th>SDP summary output.</th>
</tr>
</thead>
</table>

Output Show Service SDP — The following table describes show service SDP output fields:

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SDP Id</td>
<td>The SDP identifier.</td>
</tr>
<tr>
<td>Adm MTU</td>
<td>Specifies the largest service frame size (in octets) that can be transmitted through this SDP to the far-end router, without requiring the packet to be fragmented.</td>
</tr>
<tr>
<td>Opr MTU</td>
<td>Specifies the actual largest service frame size (in octets) that can be transmitted through this SDP to the far-end router, without requiring the packet to be fragmented.</td>
</tr>
<tr>
<td>IP address</td>
<td>Specifies the IP address of the remote end of the GRE or MPLS tunnel defined by this SDP.</td>
</tr>
<tr>
<td>Adm Admin State</td>
<td>Specifies the state of the SDP.</td>
</tr>
<tr>
<td>Opr Oper State</td>
<td>Specifies the operating state of the SDP.</td>
</tr>
<tr>
<td>Flags</td>
<td>Specifies all the conditions that affect the operating status of this SDP.</td>
</tr>
<tr>
<td>Signal Signaling</td>
<td>Specifies the signaling protocol used to obtain the ingress and egress labels used in frames transmitted and received on the SDP.</td>
</tr>
<tr>
<td>Last Status Change</td>
<td>Specifies the time of the most recent operating status change to this SDP.</td>
</tr>
<tr>
<td>Last Mgmt Change</td>
<td>Specifies the time of the most recent management-initiated change to this SDP.</td>
</tr>
<tr>
<td>Number of SDPs</td>
<td>Specifies the total number of SDPs displayed according to the criteria specified.</td>
</tr>
<tr>
<td>Hello Time</td>
<td>Specifies how often the SDP echo request messages are transmitted on this SDP.</td>
</tr>
</tbody>
</table>
Sample Output

*A:ALA-12# show service sdp

==============================================================================
Services: Service Destination Points
==============================================================================
SdpId    Adm MTU   Opr MTU   IP address       Adm  Opr         Deliver Signal
------------------------------------------------------------------------------
10       4462      4462      10.20.1.3        Up   Dn NotReady MPLS    TLDP
40       4462      1534      10.20.1.20       Up   Up          MPLS    TLDP
60       4462      1514      10.20.1.21       Up   Up          GRE     TLDP
100      4462      4462      180.0.0.2        Down Down        GRE     TLDP
500      4462      4462      10.20.1.50       Up   Dn NotReady GRE     TLDP
------------------------------------------------------------------------------
Number of SDPs : 5
==============================================================================

*A:ALA-12#
*A:ALA-12#  show service sdp 2 detail
-----------------------------------------------------------------------------------------------
Service Destination Point (Sdp Id : 2) Details
-----------------------------------------------------------------------------------------------
Sdp Id 2  -(10.10.10.104)
-----------------------------------------------------------------------------------------------
Description          : GRE=10.10.10.104
SDP Id                : 2
Admin Path MTU       : 0     Oper Path MTU : 0
Far End               : 10.10.10.104  Delivery : GRE
Admin State           : Up     Oper State : Down
Flags                 : SignalingSessDown TransportTunnDown
Signaling             : TLDP     VLAN VC Etype : 0x8100
Last Status Change    : 02/01/2007 09:11:39  Adv. MTU Over. : No
Last Mgmt Change      : 02/01/2007 09:11:46
KeepAlive Information :
Admin State           : Disabled   Oper State : Disabled
Hello Time            : 10       Hello Msg Len : 0
Hello Timeout         : 5        Unmatched Replies : 0
Max Drop Count        : 3        Hold Down Time : 10
Tx Hello Msgs         : 0        Rx Hello Msgs : 0
Associated LSP LIST :
SDP Delivery Mechanism is not MPLS
-----------------------------------------------------------------------------------------------

*A:ALA-12#  show service sdp 8
-----------------------------------------------------------------------------------------------
Service Destination Point (Sdp Id : 8)
-----------------------------------------------------------------------------------------------
SdpId  Adm MTU  Opr MTU  IP address  Adm  Opr  Deliver  Signal
-------------------------------------------------------------------------------
8       4462      4462      10.10.10.104     Up   Dn NotReady MPLS    TLDP
-----------------------------------------------------------------------------------------------
Service Destination Point (Sdp Id : 8) Details
-----------------------------------------------------------------------------------------------
Sdp Id 8  -(10.10.10.104)
-----------------------------------------------------------------------------------------------
Description          : MPLS=10.10.10.104
SDP Id                : 8
Admin Path MTU       : 0     Oper Path MTU : 0
Far End               : 10.10.10.104  Delivery : MPLS
Admin State           : Up     Oper State : Down
Flags                 : SignalingSessDown TransportTunnDown
Signaling             : TLDP     VLAN VC Etype : 0x8100
Last Status Change    : 02/01/2007 09:11:39  Adv. MTU Over. : No
Last Mgmt Change      : 02/01/2007 09:11:46
KeepAlive Information :
Admin State           : Disabled   Oper State : Disabled
Hello Time            : 10       Hello Msg Len : 0
Hello Timeout         : 5        Unmatched Replies : 0
Max Drop Count        : 3        Hold Down Time : 10
Tx Hello Msgs         : 0        Rx Hello Msgs : 0
Associated LSP LIST :
Lsp Name              : to-104
Admin State           : Up     Oper State : Down
Time Since Last Tran*: 01d07h36m
**sdp-using**

**Syntax**  
`sdp-using [sdp-id[:vc-id] | far-end ip-address]`

**Context**  
`show>service`

**Description**  
Display services using SDP or far-end address options.

**Parameters**  
`sdp-id` — Displays only services bound to the specified SDP ID.

- **Values**  
  1 — 17407

`vc-id` — The virtual circuit identifier.

- **Values**  
  1 — 4294967295

`far-end ip-address` — Displays only services matching with the specified far-end IP address.

- **Default**  
  Services with any far-end IP address.

**Output**  
Show Service SDP Using X — The following table describes show service sdp-using output fields.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Svc ID</td>
<td>The service identifier.</td>
</tr>
<tr>
<td>Sdp ID</td>
<td>The SDP identifier.</td>
</tr>
<tr>
<td>Type</td>
<td>Type of SDP: spoke or mesh.</td>
</tr>
<tr>
<td>Far End</td>
<td>The far end address of the SDP.</td>
</tr>
<tr>
<td>Oper State</td>
<td>The operational state of the service.</td>
</tr>
<tr>
<td>Ingress Label</td>
<td>The label used by the far-end device to send packets to this device in this service by this SDP.</td>
</tr>
<tr>
<td>Egress Label</td>
<td>The label used by this device to send packets to the far-end device in this service by this SDP.</td>
</tr>
</tbody>
</table>

**Sample Output**  
*A:ALA-1# show service sdp-using 300*

<table>
<thead>
<tr>
<th>SvcId</th>
<th>SdpId</th>
<th>Type</th>
<th>Far End</th>
<th>Opr State</th>
<th>I.Label</th>
<th>E.Label</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>300:1</td>
<td>Mesh</td>
<td>10.0.0.13</td>
<td>Up</td>
<td>131071</td>
<td>131071</td>
</tr>
<tr>
<td>2</td>
<td>300:2</td>
<td>Spok</td>
<td>10.0.0.13</td>
<td>Up</td>
<td>131070</td>
<td>131070</td>
</tr>
<tr>
<td>100</td>
<td>300:100</td>
<td>Mesh</td>
<td>10.0.0.13</td>
<td>Up</td>
<td>131069</td>
<td>131069</td>
</tr>
<tr>
<td>101</td>
<td>300:101</td>
<td>Mesh</td>
<td>10.0.0.13</td>
<td>Up</td>
<td>131068</td>
<td>131068</td>
</tr>
<tr>
<td>102</td>
<td>300:102</td>
<td>Mesh</td>
<td>10.0.0.13</td>
<td>Up</td>
<td>131067</td>
<td>131067</td>
</tr>
</tbody>
</table>
Show, Clear, Debug Commands

Number of SDPs: 5

* A:ALA-1#

A:ALA-48# show service sdp-using

SDP Using

<table>
<thead>
<tr>
<th>SvcId</th>
<th>SdpId</th>
<th>Type</th>
<th>Far End</th>
<th>Opr State</th>
<th>I.Label</th>
<th>E.Label</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>2:3</td>
<td>Spok</td>
<td>10.20.1.2</td>
<td>Up</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>103</td>
<td>3:103</td>
<td>Spok</td>
<td>10.20.1.3</td>
<td>Up</td>
<td>131067</td>
<td>131068</td>
</tr>
<tr>
<td>103</td>
<td>4:103</td>
<td>Spok</td>
<td>10.20.1.2</td>
<td>Up</td>
<td>131065</td>
<td>131069</td>
</tr>
<tr>
<td>105</td>
<td>3:105</td>
<td>Spok</td>
<td>10.20.1.3</td>
<td>Up</td>
<td>131066</td>
<td>131067</td>
</tr>
</tbody>
</table>

Number of SDPs: 4

A:ALA-48

service-using

**Syntax**  
`service-using [sdp sdp-id] [customer customer-id]`

**Context**  
show>service

**Description**  
Displays the services matching certain usage properties.
If no optional parameters are specified, all services defined on the system are displayed.

**Parameters**

- `ies` — Displays matching IES instances.
- `vprn` — Displays matching VPRN services.
- `mirror` — Displays mirror services.
- `sdp sdp-id` — Displays only services bound to the specified SDP ID.

**Default**  
Services bound to any SDP ID.

**Values**

1 — 17407

- `customer customer-id` — Displays services only associated with the specified customer ID.

**Default**  
Services associated with an customer.

**Values**

1 — 2147483647

**Output**  
Show Service Service-Using — The following table describes show service service-using output fields:

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Id</td>
<td>The service identifier.</td>
</tr>
<tr>
<td>Type</td>
<td>Specifies the service type configured for the service ID.</td>
</tr>
<tr>
<td>Adm</td>
<td>The desired state of the service.</td>
</tr>
<tr>
<td>Opr</td>
<td>The operating state of the service.</td>
</tr>
</tbody>
</table>

Page 1692  7950 SR  OS Services Guide
### Sample Output

* `A:ALA-12# show service service-using customer 10`

<table>
<thead>
<tr>
<th>ServiceId</th>
<th>Type</th>
<th>Adm</th>
<th>Opr</th>
<th>CustomerId</th>
<th>Last Mgmt Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>VPLS</td>
<td>Up</td>
<td>Up</td>
<td>10</td>
<td>09/05/2006 13:24:15</td>
</tr>
<tr>
<td>100</td>
<td>IES</td>
<td>Up</td>
<td>Up</td>
<td>10</td>
<td>09/05/2006 13:24:15</td>
</tr>
<tr>
<td>300</td>
<td>Epipe</td>
<td>Up</td>
<td>Up</td>
<td>10</td>
<td>09/05/2006 13:24:15</td>
</tr>
</tbody>
</table>

Matching Services: 4

* `A:ALA-12# show service service-using epipe`

<table>
<thead>
<tr>
<th>ServiceId</th>
<th>Type</th>
<th>Adm</th>
<th>Opr</th>
<th>CustomerId</th>
<th>Last Mgmt Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>Epipe</td>
<td>Up</td>
<td>Up</td>
<td>6</td>
<td>06/22/2006 23:05:58</td>
</tr>
<tr>
<td>7</td>
<td>Epipe</td>
<td>Up</td>
<td>Up</td>
<td>6</td>
<td>06/22/2006 23:05:58</td>
</tr>
<tr>
<td>8</td>
<td>Epipe</td>
<td>Up</td>
<td>Up</td>
<td>3</td>
<td>06/22/2006 23:05:58</td>
</tr>
<tr>
<td>103</td>
<td>Epipe</td>
<td>Up</td>
<td>Up</td>
<td>6</td>
<td>06/22/2006 23:05:58</td>
</tr>
</tbody>
</table>

Matching Services: 4

* `A:de14# show service service-using`

<table>
<thead>
<tr>
<th>ServiceId</th>
<th>Type</th>
<th>Adm</th>
<th>Opr</th>
<th>CustomerId</th>
<th>Last Mgmt Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>uVPLS</td>
<td>Up</td>
<td>Up</td>
<td>1</td>
<td>10/26/2006 15:44:57</td>
</tr>
<tr>
<td>2</td>
<td>Epipe</td>
<td>Up</td>
<td>Down</td>
<td>1</td>
<td>10/26/2006 15:44:57</td>
</tr>
<tr>
<td>10</td>
<td>mVPLS</td>
<td>Down</td>
<td>Down</td>
<td>1</td>
<td>10/26/2006 15:44:57</td>
</tr>
<tr>
<td>11</td>
<td>mVPLS</td>
<td>Down</td>
<td>Down</td>
<td>1</td>
<td>10/26/2006 15:44:57</td>
</tr>
<tr>
<td>100</td>
<td>mVPLS</td>
<td>Up</td>
<td>Up</td>
<td>1</td>
<td>10/26/2006 15:44:57</td>
</tr>
<tr>
<td>101</td>
<td>mVPLS</td>
<td>Up</td>
<td>Up</td>
<td>1</td>
<td>10/26/2006 15:44:57</td>
</tr>
<tr>
<td>102</td>
<td>mVPLS</td>
<td>Up</td>
<td>Up</td>
<td>1</td>
<td>10/26/2006 15:44:57</td>
</tr>
<tr>
<td>999</td>
<td>uVPLS</td>
<td>Down</td>
<td>Down</td>
<td>1</td>
<td>10/26/2006 16:14:33</td>
</tr>
</tbody>
</table>

Matching Services: 8

A:de14#
Show, Clear, Debug Commands

id

Syntax  
```
 id service-id { all | arp | base | fdb | labels | mfib | sap | sdp | split-horizon-group | stp }
```

Context  
```
show>service
```

Description  
This command displays information for a particular service-id.

Parameters  
```
service-id — The unique service identification number that identifies the service in the service domain.
all — Display detailed information about the service.
ar p — Display ARP entries for the service.
base — Display basic service information.
fdb — Display FDB entries.
interface — Display service interfaces.
labels — Display labels being used by this service.
sap — Display SAPs associated to the service.
sdp — Display SDPs associated with the service.
split-horizon-group — Display split horizon group information.
stp — Display STP information.
```

all

Syntax  
```
 all
```

Context  
```
show>service>id
```

Description  
Displays detailed information for all aspects of the service.

Show All Service-ID Output — The following table describes the show all service-id command output fields:

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Detailed Information</td>
<td></td>
</tr>
<tr>
<td>Service Id</td>
<td>The service identifier.</td>
</tr>
<tr>
<td>VPN Id</td>
<td>The number which identifies the VPN.</td>
</tr>
<tr>
<td>Customer Id</td>
<td>The customer identifier.</td>
</tr>
<tr>
<td>Last Status Change</td>
<td>The date and time of the most recent change in the administrative or operating status of the service.</td>
</tr>
<tr>
<td>Last Mgmt Change</td>
<td>The date and time of the most recent management-initiated change to this customer.</td>
</tr>
<tr>
<td>Admin State</td>
<td>The current administrative state.</td>
</tr>
<tr>
<td>Label</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Oper State</td>
<td>The current operational state.</td>
</tr>
<tr>
<td>Route Dist.</td>
<td>Displays the route distribution number.</td>
</tr>
<tr>
<td>AS Number</td>
<td>Displays the autonomous system number.</td>
</tr>
<tr>
<td>Router Id</td>
<td>Displays the router ID for this service.</td>
</tr>
<tr>
<td>ECMP</td>
<td>Displays equal cost multipath information.</td>
</tr>
<tr>
<td>ECMP Max Routes</td>
<td>Displays the maximum number of routes that can be received from the neighbors in the group or for the specific neighbor.</td>
</tr>
<tr>
<td>Max Routes</td>
<td>Displays the maximum number of routes that can be used for path sharing.</td>
</tr>
<tr>
<td>Auto Bind</td>
<td>Specifies the automatic binding type for the SDP assigned to this service.</td>
</tr>
<tr>
<td>Vrf Target</td>
<td>Specifies the VRF target applied to this service.</td>
</tr>
<tr>
<td>Vrf Import</td>
<td>Specifies the VRF import policy applied to this service.</td>
</tr>
<tr>
<td>Vrf Export</td>
<td>Specifies the VRF export policy applied to this service.</td>
</tr>
<tr>
<td>SDP Id</td>
<td>The SDP identifier.</td>
</tr>
<tr>
<td>Description</td>
<td>Generic information about the service.</td>
</tr>
<tr>
<td>SAP Count</td>
<td>The number of SAPs specified for this service.</td>
</tr>
<tr>
<td>SDP Bind Count</td>
<td>The number of SDPs bound to this service.</td>
</tr>
<tr>
<td>Split Horizon Group</td>
<td>Name of the split horizon group for this service.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the split horizon group.</td>
</tr>
<tr>
<td>Last Changed</td>
<td>The date and time of the most recent management-initiated change to this split horizon group.</td>
</tr>
</tbody>
</table>

**Service Destination Points (SDPs)**

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SDP Id</td>
<td>The SDP identifier.</td>
</tr>
<tr>
<td>Type</td>
<td>Indicates whether this Service SDP binding is a spoke or a mesh.</td>
</tr>
<tr>
<td>Admin Path MTU</td>
<td>The desired largest service frame size (in octets) that can be transmitted through this SDP to the far-end router, without requiring the packet to be fragmented.</td>
</tr>
<tr>
<td>Oper Path MTU</td>
<td>The actual largest service frame size (in octets) that can be transmitted through this SDP to the far-end router, without requiring the packet to be fragmented.</td>
</tr>
<tr>
<td>Delivery</td>
<td>Specifies the type of delivery used by the SDP: GRE or MPLS.</td>
</tr>
<tr>
<td>Admin State</td>
<td>The administrative state of this SDP.</td>
</tr>
</tbody>
</table>
### Show, Clear, Debug Commands

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oper State</td>
<td>The operational state of this SDP.</td>
</tr>
<tr>
<td>Ingress Label</td>
<td>The label used by the far-end device to send packets to this device in this service by this SDP.</td>
</tr>
<tr>
<td>Egress Label</td>
<td>The label used by this device to send packets to the far-end device in this service by this SDP.</td>
</tr>
<tr>
<td>Ingress Filter</td>
<td>The ID of the ingress filter policy.</td>
</tr>
<tr>
<td>Egress Filter</td>
<td>The ID of the egress filter policy.</td>
</tr>
<tr>
<td>Far End</td>
<td>Specifies the IP address of the remote end of the GRE or MPLS tunnel defined by this SDP.</td>
</tr>
<tr>
<td>Last Changed</td>
<td>The date and time of the most recent change to this customer.</td>
</tr>
<tr>
<td>Signaling</td>
<td>Specifies the signaling protocol used to obtain the ingress and egress labels used in frames transmitted and received on this SDP.</td>
</tr>
<tr>
<td>Admin State</td>
<td>Specifies the operating status of the keepalive protocol.</td>
</tr>
<tr>
<td>Oper State</td>
<td>The current status of the keepalive protocol.</td>
</tr>
<tr>
<td>Hello Time</td>
<td>Specifies how often the SDP echo request messages are transmitted on this SDP.</td>
</tr>
<tr>
<td>Hello Msg Len</td>
<td>Specifies the length of the SDP echo request messages transmitted on this SDP.</td>
</tr>
<tr>
<td>Max Drop Count</td>
<td>Specifies the maximum number of consecutive SDP Echo Request messages that can be unacknowledged before the keepalive protocol reports a fault.</td>
</tr>
<tr>
<td>Hold Down Time</td>
<td>Specifies the amount of time to wait before the keepalive operating status is eligible to enter the alive state.</td>
</tr>
<tr>
<td>SDP Delivery Mechanism</td>
<td>When the SDP type is MPLS, a list of LSPs used to reach the far-end router displays. All the LSPs in the list must terminate at the IP address specified in the far end field. If the SDP type is GRE, then the following message displays: SDP delivery mechanism is not MPLS</td>
</tr>
<tr>
<td>Max Drop Count</td>
<td>Specifies the maximum number of consecutive SDP Echo Request messages that can be unacknowledged before the keepalive protocol reports a fault.</td>
</tr>
<tr>
<td>Number of SDPs</td>
<td>The total number SDPs applied to this service ID.</td>
</tr>
<tr>
<td>Service Access Points</td>
<td></td>
</tr>
<tr>
<td>Service Id</td>
<td>The service identifier.</td>
</tr>
<tr>
<td>Port Id</td>
<td>The ID of the access port where this SAP is defined.</td>
</tr>
<tr>
<td>Description</td>
<td>Generic information about the SAP.</td>
</tr>
<tr>
<td>Label</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Encap Value</td>
<td>The value of the label used to identify this SAP on the access port.</td>
</tr>
<tr>
<td>Admin State</td>
<td>The desired state of the SAP.</td>
</tr>
<tr>
<td>Oper State</td>
<td>The operating state of the SAP.</td>
</tr>
<tr>
<td>Last Changed</td>
<td>The date and time of the last change.</td>
</tr>
<tr>
<td>Admin MTU</td>
<td>The desired largest service frame size (in octets) that can be transmitted through this SDP to the far-end router, without requiring the packet to be fragmented.</td>
</tr>
<tr>
<td>Oper MTU</td>
<td>The actual largest service frame size (in octets) that can be transmitted through this SDP to the far-end router, without requiring the packet to be fragmented.</td>
</tr>
<tr>
<td>Ingress qos-policy</td>
<td>The SAP ingress QoS policy ID.</td>
</tr>
<tr>
<td>Egress qos-policy</td>
<td>The SAP egress QoS policy ID.</td>
</tr>
<tr>
<td>Ingress Filter-Id</td>
<td>The SAP ingress filter policy ID.</td>
</tr>
<tr>
<td>Egress Filter-Id</td>
<td>The SAP egress filter policy ID.</td>
</tr>
<tr>
<td>Multi Svc Site</td>
<td>Indicates the multi-service site that the SAP is a member.</td>
</tr>
<tr>
<td>Ingress sched-policy</td>
<td>Indicates the ingress QoS scheduler for the SAP.</td>
</tr>
<tr>
<td>Egress sched-policy</td>
<td>Indicates the egress QoS scheduler for the SAP.</td>
</tr>
<tr>
<td>Acct. Pol</td>
<td>Indicates the accounting policy applied to the SAP.</td>
</tr>
<tr>
<td>Collect Stats</td>
<td>Specifies whether accounting statistics are collected on the SAP.</td>
</tr>
<tr>
<td>SAP Statistics</td>
<td></td>
</tr>
<tr>
<td>Dropped</td>
<td>The number of packets or octets dropped.</td>
</tr>
<tr>
<td>Offered Hi Priority</td>
<td>The number of high priority packets, as determined by the SAP ingress QoS policy.</td>
</tr>
<tr>
<td>Offered Low Priority</td>
<td>The number of low priority packets, as determined by the SAP ingress QoS policy.</td>
</tr>
<tr>
<td>Forwarded In Profile</td>
<td>The number of in-profile packets or octets (rate below CIR) forwarded.</td>
</tr>
<tr>
<td>Forwarded Out Profile</td>
<td>The number of out-of-profile packets or octets (rate above CIR) forwarded.</td>
</tr>
<tr>
<td>Queueing Stats</td>
<td></td>
</tr>
<tr>
<td>Dropped In Profile</td>
<td>The number of in-profile packets or octets discarded.</td>
</tr>
</tbody>
</table>
**Show, Clear, Debug Commands**

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dropped Out Profile</td>
<td>The number of out-of-profile packets or octets discarded.</td>
</tr>
<tr>
<td>Forwarded In Profile</td>
<td>The number of in-profile packets or octets (rate below CIR) forwarded.</td>
</tr>
<tr>
<td>Forwarded Out Profile</td>
<td>The number of out-of-profile packets or octets (rate above CIR) forwarded.</td>
</tr>
<tr>
<td>SAP per Queue stats</td>
<td></td>
</tr>
<tr>
<td>Ingress Queue 1</td>
<td>The index of the ingress QoS queue of this SAP.</td>
</tr>
<tr>
<td>High priority offered</td>
<td>The packets or octets count of the high priority traffic for the SAP.</td>
</tr>
<tr>
<td>High priority dropped</td>
<td>The number of high priority traffic packets/octets dropped.</td>
</tr>
<tr>
<td>Low priority offered</td>
<td>The packets or octets count of the low priority traffic.</td>
</tr>
<tr>
<td>Low priority dropped</td>
<td>The number of low priority traffic packets/octets dropped.</td>
</tr>
<tr>
<td>In profile forwarded</td>
<td>The number of in-profile packets or octets (rate below CIR) forwarded.</td>
</tr>
<tr>
<td>Out profile forwarded</td>
<td>The number of out-of-profile packets or octets (rate above CIR) forwarded.</td>
</tr>
<tr>
<td>Egress Queue 1</td>
<td>The index of the egress QoS queue of the SAP.</td>
</tr>
<tr>
<td>In profile forwarded</td>
<td>The number of in-profile packets or octets (rate below CIR) forwarded.</td>
</tr>
<tr>
<td>In profile dropped</td>
<td>The number of in-profile packets or octets dropped for the SAP.</td>
</tr>
<tr>
<td>Out profile forwarded</td>
<td>The number of out-of-profile packets or octets (rate above CIR) forwarded.</td>
</tr>
<tr>
<td>Out profile dropped</td>
<td>The number of out-of-profile packets or octets discarded.</td>
</tr>
<tr>
<td>State</td>
<td>Specifies whether DHCP relay is enabled on this SAP.</td>
</tr>
<tr>
<td>Info Option</td>
<td>Specifies whether Option 82 processing is enabled on this SAP.</td>
</tr>
<tr>
<td>Action</td>
<td>Specifies the Option 82 processing on this SAP or interface: keep, replace or drop.</td>
</tr>
<tr>
<td>Circuit ID</td>
<td>Specifies whether the If index is inserted in circuit ID sub-option of Option 82.</td>
</tr>
<tr>
<td>Remote ID</td>
<td>Specifies whether the far-end MAC address is inserted in Remote ID sub-option of Option 82.</td>
</tr>
<tr>
<td>Service Access Points</td>
<td></td>
</tr>
<tr>
<td>Label</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Managed by Service</td>
<td>Specifies the service-id of the management VPLS managing this SAP.</td>
</tr>
<tr>
<td>Managed by SAP</td>
<td>Specifies the sap-id inside the management VPLS managing this SAP.</td>
</tr>
<tr>
<td>Prune state</td>
<td>Specifies the STP state inherited from the management VPLS.</td>
</tr>
<tr>
<td>Spoke SDPs</td>
<td></td>
</tr>
<tr>
<td>Managed by Service</td>
<td>Specifies the service-id of the management VPLS managing this spoke SDP.</td>
</tr>
<tr>
<td>Managed by Spoke</td>
<td>Specifies the sap-id inside the management VPLS managing this spoke SDP.</td>
</tr>
<tr>
<td>Prune state</td>
<td>Specifies the STP state inherited from the management VPLS.</td>
</tr>
<tr>
<td>Peer Pw Bits</td>
<td>Indicates the bits set by the LDP peer when there is a fault on its side of</td>
</tr>
<tr>
<td></td>
<td>the pseudowire. LAC failures occur on the SAP that has been configured on</td>
</tr>
<tr>
<td></td>
<td>the pipe service, PSN bits are set by SDP-binding failures on the pipe</td>
</tr>
<tr>
<td></td>
<td>service. The pwNotForwarding bit is set when none of the above failures</td>
</tr>
<tr>
<td></td>
<td>apply, such as an MTU mismatch failure. This value is only applicable if</td>
</tr>
<tr>
<td></td>
<td>the peer is using the pseudowire status signalling method to indicate</td>
</tr>
<tr>
<td></td>
<td>faults.</td>
</tr>
<tr>
<td></td>
<td>pwNotForwarding — Pseudowire not forwarding</td>
</tr>
<tr>
<td></td>
<td>lacIngressFault Local — Attachment circuit RX fault</td>
</tr>
<tr>
<td></td>
<td>lacEgressFault Local — Attachment circuit TX fault</td>
</tr>
<tr>
<td></td>
<td>psnIngressFault Local — PSN-facing PW RX fault</td>
</tr>
<tr>
<td></td>
<td>psnEgressFault Local — PSN-facing PW TX fault</td>
</tr>
<tr>
<td></td>
<td>pwFwdingStandby — Pseudowire in standby mode</td>
</tr>
<tr>
<td>IPCP Address Extension Details</td>
<td></td>
</tr>
<tr>
<td>Peer IP Addr</td>
<td>Specifies the remote IP address to be assigned to the far-end of the</td>
</tr>
<tr>
<td></td>
<td>associated PPP/MLPPP link via IPCP extensions.</td>
</tr>
<tr>
<td>Peer Pri DNS Addr</td>
<td>Specifies a unicast IPv4 address for the primary DNS server to be signaled</td>
</tr>
<tr>
<td></td>
<td>to the far-end of the associate PPP/MLPPP link via IPCP extensions.</td>
</tr>
<tr>
<td>Peer Sec DNS Addr</td>
<td>Specifies a unicast IPv4 address for the secondary DNS server to be</td>
</tr>
<tr>
<td></td>
<td>signaled to the far-end of the associate PPP/MLPPP link via IPCP extensions.</td>
</tr>
</tbody>
</table>

Sample Output

A:ALA-48# show service id 1 all

```
+----------------+-----------------+----------------+-----------------+-----------------+-----------------+
| Service Id     |     Vpn Id      | Service Type   | Customer Id    | Last Status Change | Last Mgmt Change |
|----------------+-----------------+----------------+----------------+-----------------+-----------------+
| Admin State    |     : Up        | Oper State     | : Up           |                 |                 |
```
Route Dist.       : 10001:1    VPRN Type       : regular
AS Number        : 10000      Router Id       : 10.10.10.103
ECMP             : Enabled     ECMP Max Routes : 8
Max Routes       : 80         Auto Bind       : LDP
Vrf Target       : target:10001:1
Vrf Import       : vrfImpPolCust1
Vrf Export       : vrfExpPolCust1

SAP Count         : 2         SDP Bind Count : 3

Service Destination Points(SDPs)

Sdp Id 1:1 -(10.10.10.49)

Description     : to-GRE-10.10.10.49
SDP Id             : 1:1                Type              : Spoke
VC Type            : n/a               VC Tag             : n/a
Admin Path MTU     : 0               Oper Path MTU     : 0
Far End            : 10.10.10.49        Delivery          : GRE

Admin State        : Up                       Oper State        : Down
Acct. Pol          : None                     Collect Stats     : Disabled
Ingress Label      : n/a                      Egress Label      : n/a
Ing mac Fltr       : n/a                      Egr mac Fltr      : n/a
Ing ip Fltr        : n/a                      Egr ip Fltr       : n/a
Admin ControlWord  : Not Preferred            Oper ControlWord  : False
Admin BW(Kbps)     : 0                        Oper BW(Kbps)     : 0
Last Status Change : 06/18/2007 10:06:49      Signaling         : n/a
Last Mgmt Change   : 06/18/2007 10:07:01
Class Fwding State : Down
Flags              : SdpOperDown
Peer Pw Bits       : None
Peer Fault Ip      : None
Peer Vccv CV Bits  : None
Peer Vccv CC Bits  : None

KeepAlive Information :
Admin State        : Disabled                 Oper State        : Disabled
Hello Time         : 10                       Hello Msg Len     : 0
Max Drop Count     : 3                        Hold Down Time    : 10

Statistics :
I. Fwd. Pkts.      : n/a                      I. Dro. Pkts.     : n/a
I. Fwd. Octs.      : n/a                      I. Dro. Octs.     : n/a
E. Fwd. Pkts.      : n/a                      E. Fwd. Octets    : n/a

Associated LSP LIST :
SDP Delivery Mechanism is not MPLS

Sdp Id 1:10 -(10.10.10.49)

Description     : to-GRE-10.10.10.49
SDP Id             : 1:10                 Type              : Spoke
VC Type            : n/a               VC Tag             : n/a
Admin Path MTU     : 0               Oper Path MTU     : 0
Far End            : 10.10.10.49        Delivery          : GRE

Admin State        : Up                       Oper State        : Down
Acct. Pol          : None                     Collect Stats     : Disabled
Ingress Label      : 0                        Egress Label      : 0
Ing mac Fltr       : n/a                      Egr mac Fltr      : n/a
Ing ip Fltr        : n/a                      Egr ip Fltr       : n/a
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ingress IPv6 Filter</td>
<td>n/a</td>
</tr>
<tr>
<td>Egress IPv6 Filter</td>
<td>n/a</td>
</tr>
<tr>
<td>Admin Control Word</td>
<td>Not Preferred</td>
</tr>
<tr>
<td>Oper Control Word</td>
<td>False</td>
</tr>
<tr>
<td>Admin BW (Kbps)</td>
<td>0</td>
</tr>
<tr>
<td>Oper BW (Kbps)</td>
<td>0</td>
</tr>
<tr>
<td>Last Status Change</td>
<td>06/18/2007 10:06:49</td>
</tr>
<tr>
<td>Last Mgmt Change</td>
<td>06/18/2007 10:07:01</td>
</tr>
<tr>
<td>Class Fwding State</td>
<td>Down</td>
</tr>
<tr>
<td>Flags</td>
<td>SdpOperDown</td>
</tr>
<tr>
<td></td>
<td>NoInGVCLabel NoEgrVCLabel</td>
</tr>
<tr>
<td>Peer PW Bits</td>
<td>None</td>
</tr>
<tr>
<td>Peer Fault IP</td>
<td>None</td>
</tr>
<tr>
<td>Peer VCCV CV Bits</td>
<td>None</td>
</tr>
<tr>
<td>Peer VCCV CC Bits</td>
<td>None</td>
</tr>
<tr>
<td>Keep Alive Information</td>
<td></td>
</tr>
<tr>
<td>Admin State</td>
<td>Disabled</td>
</tr>
<tr>
<td>Oper State</td>
<td>Disabled</td>
</tr>
<tr>
<td>Hello Time</td>
<td>10</td>
</tr>
<tr>
<td>Hello Message Length</td>
<td>0</td>
</tr>
<tr>
<td>Max Drop Count</td>
<td>3</td>
</tr>
<tr>
<td>Hold Down Time</td>
<td>10</td>
</tr>
<tr>
<td>Statistics</td>
<td></td>
</tr>
<tr>
<td>Ingress Forwarded Packets</td>
<td>0</td>
</tr>
<tr>
<td>Egress Forwarded Packets</td>
<td>0</td>
</tr>
<tr>
<td>Ingress Forwarded Octets</td>
<td>0</td>
</tr>
<tr>
<td>Egress Forwarded Octets</td>
<td>0</td>
</tr>
<tr>
<td>Associated LSP LIST</td>
<td></td>
</tr>
<tr>
<td>SDP Delivery Mechanism</td>
<td>is not MPLS</td>
</tr>
<tr>
<td>SDP Id</td>
<td>3:4</td>
</tr>
<tr>
<td>Type</td>
<td>Spoke</td>
</tr>
<tr>
<td>VC Type</td>
<td>n/a</td>
</tr>
<tr>
<td>VC Tag</td>
<td>n/a</td>
</tr>
<tr>
<td>Admin Path MTU</td>
<td>0</td>
</tr>
<tr>
<td>Oper Path MTU</td>
<td>0</td>
</tr>
<tr>
<td>Far End</td>
<td>10.10.10.105</td>
</tr>
<tr>
<td>Delivery</td>
<td>GRE</td>
</tr>
<tr>
<td>Admin State</td>
<td>Up</td>
</tr>
<tr>
<td>Oper State</td>
<td>Down</td>
</tr>
<tr>
<td>Acct. Pol</td>
<td>None</td>
</tr>
<tr>
<td>Collect Stats</td>
<td>Disabled</td>
</tr>
<tr>
<td>Ingress Label</td>
<td>3000</td>
</tr>
<tr>
<td>Egress Label</td>
<td>2000</td>
</tr>
<tr>
<td>Ingress MAC Filter</td>
<td>n/a</td>
</tr>
<tr>
<td>Egress MAC Filter</td>
<td>n/a</td>
</tr>
<tr>
<td>Ingress IPv6 Filter</td>
<td>10</td>
</tr>
<tr>
<td>Egress IPv6 Filter</td>
<td>n/a</td>
</tr>
<tr>
<td>Admin Control Word</td>
<td>Not Preferred</td>
</tr>
<tr>
<td>Oper Control Word</td>
<td>False</td>
</tr>
<tr>
<td>Admin BW (Kbps)</td>
<td>0</td>
</tr>
<tr>
<td>Oper BW (Kbps)</td>
<td>0</td>
</tr>
<tr>
<td>Last Status Change</td>
<td>06/18/2007 10:06:49</td>
</tr>
<tr>
<td>Last Mgmt Change</td>
<td>06/18/2007 10:07:01</td>
</tr>
<tr>
<td>Class Fwding State</td>
<td>Down</td>
</tr>
<tr>
<td>Flags</td>
<td>SdpOperDown</td>
</tr>
<tr>
<td>Peer PW Bits</td>
<td>None</td>
</tr>
<tr>
<td>Peer Fault IP</td>
<td>None</td>
</tr>
<tr>
<td>Peer VCCV CV Bits</td>
<td>None</td>
</tr>
<tr>
<td>Peer VCCV CC Bits</td>
<td>None</td>
</tr>
<tr>
<td>Keep Alive Information</td>
<td></td>
</tr>
<tr>
<td>Admin State</td>
<td>Disabled</td>
</tr>
<tr>
<td>Oper State</td>
<td>Disabled</td>
</tr>
<tr>
<td>Hello Time</td>
<td>10</td>
</tr>
<tr>
<td>Hello Message Length</td>
<td>0</td>
</tr>
<tr>
<td>Max Drop Count</td>
<td>3</td>
</tr>
<tr>
<td>Hold Down Time</td>
<td>10</td>
</tr>
<tr>
<td>Statistics</td>
<td></td>
</tr>
<tr>
<td>Ingress Forwarded Packets</td>
<td>0</td>
</tr>
<tr>
<td>Egress Forwarded Packets</td>
<td>0</td>
</tr>
<tr>
<td>Ingress Forwarded Octets</td>
<td>0</td>
</tr>
<tr>
<td>Egress Forwarded Octets</td>
<td>0</td>
</tr>
<tr>
<td>Associated LSP LIST</td>
<td></td>
</tr>
<tr>
<td>SDP Delivery Mechanism</td>
<td>is not MPLS</td>
</tr>
</tbody>
</table>
Number of SDPs : 3

Service Access Points

SAP 1/1/21:0

Service Id : 1
SAP : 1/1/21:0
Encap : q-tag
Dot1Q Ethertype : 0x8100
QinQ Ethertype : 0x8100

Admin State : Up
Oper State : Down

Flags : PortOperDown
Last Status Change : 06/18/2007 10:06:49
Last Mgmt Change : 06/18/2007 10:07:01

Admin MTU : 1518
Oper MTU : 1518

Ingress qos-policy : 1
Egress qos-policy : 1

Shared Q policy : n/a
Multipoint shared : Disabled

Ingr IP Fltr-Id : n/a
Egr IP Fltr-Id : n/a
Ingr IPv6 Fltr-Id : n/a
Egr IPv6 Fltr-Id : n/a

tod-suite : None
qinq-pbit-marking : both

Multi Svc Site : None
Acct. Pol : None
Collect Stats : Disabled

Anti Spoofing : None
Nbr Static Hosts : 0

Sap Statistics

Last Cleared Time : N/A

Forwarding Engine Stats
Dropped : 0
Off. HiPrio : 0
Off. LowPrio : 0
Off. Uncolor : 0

Queueing Stats(Ingress QoS Policy 1)
Dro. HiPrio : 0
Dro. LowPrio : 0
For. InProf : 0
For. OutProf : 0

Queueing Stats(Egress QoS Policy 1)
Dro. InProf : 0
Dro. OutProf : 0
For. InProf : 0
For. OutProf : 0

Sap per Queue stats

Ingress Queue 1 (Unicast) (Priority)
Off. HiPrio : 0
Off. LoPrio : 0
Dro. HiPrio : 0
Dro. LoPrio : 0
For. InProf : 0
For. OutProf : 0

Egress Queue 1
For. InProf : 0
### VPRN Show Commands

<table>
<thead>
<tr>
<th>For. OutProf</th>
<th>Dro. InProf</th>
<th>Dro. OutProf</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

---

**SAP 1/2/4:0**

<table>
<thead>
<tr>
<th>Service Id</th>
<th>SAP</th>
<th>Encap</th>
<th>Encap Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1/2/4:0</td>
<td>q-tag</td>
<td>0x8100</td>
</tr>
</tbody>
</table>

**Admin State**: Up

**Flags**: PIN, PortOperDown

**Last Status Change**: 06/18/2007 10:06:49

**Last Mgmt Change**: 06/18/2007 10:07:01

<table>
<thead>
<tr>
<th>Admin MTU</th>
<th>Ingress qos-policy</th>
<th>Egress qos-policy</th>
<th>Shared Q policy</th>
<th>QinQ Ethertype</th>
</tr>
</thead>
<tbody>
<tr>
<td>1518</td>
<td>1</td>
<td>1</td>
<td>n/a</td>
<td>0x8100</td>
</tr>
</tbody>
</table>

**Ingr Mac Fltr-Id**: n/a

**Ingr IPv6 Fltr-Id**: n/a

**tod-suite**: None

**Egr Agg Rate Limit**: max

**Multi Svc Site**: None

**Acct. Pol**: None

**Collect Stats**: Disabled

**Anti Spoofing**: IP-MAC

---

**Subscriber Management**

<table>
<thead>
<tr>
<th>Admin State</th>
<th>MAC DA Hashing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Down</td>
<td>False</td>
</tr>
</tbody>
</table>

**Def Sub-Id**: None

**Def Sub-Profile**: None

**Def SLA-Profile**: None

**Def App-Profile**: None

**Sub-Ident-Policy**: None

**Subscriber Limit**: 1

**Single-Sub-Parameters**

**Prof Traffic Only**: False

**Non-Sub-Traffic**: N/A

---

**Sap Statistics**

<table>
<thead>
<tr>
<th>Last Cleared Time</th>
<th>Packets</th>
<th>Octets</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Forwarding Engine Stats**

<table>
<thead>
<tr>
<th>Dropped</th>
<th>Off. HiPrio</th>
<th>Off. LowPrio</th>
<th>Off. Uncolor</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

**Queueing Stats(Ingress QoS Policy 1)**

<table>
<thead>
<tr>
<th>Dro. HiPrio</th>
<th>Dro. LowPrio</th>
<th>For. InProf</th>
<th>For. OutProf</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

**Queueing Stats(Egress QoS Policy 1)**

<table>
<thead>
<tr>
<th>Dro. InProf</th>
<th>Dro. OutProf</th>
<th>For. InProf</th>
<th>For. OutProf</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
Sap per Queue stats

<table>
<thead>
<tr>
<th>Packets</th>
<th>Octets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ingress Queue 1 (Unicast) (Priority)</td>
<td></td>
</tr>
<tr>
<td>Off. HiPrio : 0</td>
<td>0</td>
</tr>
<tr>
<td>Off. LoPrio : 0</td>
<td>0</td>
</tr>
<tr>
<td>Dro. HiPrio : 0</td>
<td>0</td>
</tr>
<tr>
<td>Dro. LoPrio : 0</td>
<td>0</td>
</tr>
<tr>
<td>For. InProf : 0</td>
<td>0</td>
</tr>
<tr>
<td>For. OutProf : 0</td>
<td>0</td>
</tr>
<tr>
<td>Egress Queue 1</td>
<td></td>
</tr>
<tr>
<td>For. InProf : 0</td>
<td>0</td>
</tr>
<tr>
<td>For. OutProf : 0</td>
<td>0</td>
</tr>
<tr>
<td>Dro. InProf : 0</td>
<td>0</td>
</tr>
<tr>
<td>Dro. OutProf : 0</td>
<td>0</td>
</tr>
</tbody>
</table>

Service Interfaces

<table>
<thead>
<tr>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>If Name : to-ce1</td>
</tr>
<tr>
<td>Admin State : Up</td>
</tr>
<tr>
<td>Oper (v4/v6) : Down/Down</td>
</tr>
<tr>
<td>Protocols : None</td>
</tr>
<tr>
<td>IP Addr/mask : 11.1.0.1/24</td>
</tr>
<tr>
<td>Address Type : Primary</td>
</tr>
<tr>
<td>IGP Inhibit : Disabled</td>
</tr>
</tbody>
</table>

Details

| If Index : 2 |
| Virt. If Index : 2 |
| Last Oper Chg : 06/18/2007 10:07:01 |
| Global If Index : 96 |
| SAP Id : 1/1/21:0 |
| TOS Marking : Trusted |
| If Type : VPRN |
| SNTP B.Cast : False |
| MAC Address : 14:30:01:01:00:15 |
| Arp Timeout : 14400 |
| IP MTU : 1500 |
| ICMP Mask Reply : True |
| Arp Populate : Disabled |
| Host Conn Verify : Enabled |

Proxy ARP Details

| Rem Proxy ARP : Disabled |
| Local Proxy ARP : Disabled |
| Policies : none |

Proxy Neighbor Discovery Details

| Local Pxy ND : Disabled |
| Policies : none |

DHCP Details

| Admin State : Up |
| Lease Populate : 1 |
| Gi-Addr : 11.1.0.1* |
| Gi-Addr as Src Ip : Disabled |
| * = inferred gi-address from interface IP address |

Action : Keep |
| Trusted : Enabled |

DHCP Proxy Details

| Admin State : Down |
| Lease Time : N/A |
| Emul. Server : Not configured |

Subscriber Authentication Details

| Auth Policy : None |

DHCP6 Relay Details
VPRN Show Commands

Admin State : Down                  Lease Populate : 0
Oper State : Down                    Nbr Resolution : Disabled
If-Id Option : None                    Remote Id : Disabled
Src Addr : Not configured

DHCP6 Server Details
Admin State : Down                     Max. Lease States : 8000

ICMP Details
Redirects : Number - 100                 Time (seconds) - 10
Unreachables : Number - 100              Time (seconds) - 10
TTL Expired : Number - 100                Time (seconds) - 10

IPCP Address Extension Details
Peer IP Addr : Not configured
Peer Pri DNS Addr : Not configured
Peer Sec DNS Addr : Not configured

Interface
If Name : test
Admin State : Up                        Oper (v4/v6) : Down/Down
Protocols : IGMP PIM

Details
If Index : 3                              Virt. If Index : 3
Last Oper Chg : 06/18/2007 10:07:01         Global If Index : 95
Port Id : n/a
TOS Marking : Trusted                      If Type : VPRN
SNMP B.Cast : False
MAC Address :                                Arp Timeout : 14400
IP MTU : 0                                  ICMP Mask Reply : True
Arp Populate : Disabled                     Host Conn Verify : Disabled

Proxy ARP Details
Rem Proxy ARP : Disabled                   Local Proxy ARP : Disabled
Policies : none

Proxy Neighbor Discovery Details
Local Pxy ND : Disabled                    Policies : none

DHCP Details
Admin State : Down                        Lease Populate : 0
Gi-Addr : Not configured                   Gi-Addr as Src Ip : Disabled
Action : Keep                             Trusted : Disabled

DHCP Proxy Details
Admin State : Down
Lease Time : N/A
Emul. Server : Not configured

Subscriber Authentication Details
Auth Policy : None

DHCP6 Relay Details
Admin State : Down                        Lease Populate : 0
Oper State : Down                          Nbr Resolution : Disabled
If-Id Option : None                        Remote Id : Disabled
Src Addr : Not configured
DHCP6 Server Details
Admin State : Down Max. Lease States : 8000

ICMP Details
Redirects : Number - 100 Time (seconds) - 10
Unreachables : Number - 100 Time (seconds) - 10
TTL Expired : Number - 100 Time (seconds) - 10

IPCP Address Extension Details
Peer IP Addr : Not configured
Peer Pri DNS Addr : Not configured
Peer Sec DNS Addr : Not configured

Interface
If Name : SpokeSDP
Admin State : Up Oper (v4/v6) : Down/Down
Protocols : None

IP Addr/mask : Not Assigned

Details
If Index : 4 Virt. If Index : 4
Last Oper Chg : 06/18/2007 10:07:01 Global If Index : 94
SDP Id : spoke-3:4
TOS Marking : Trusted If Type : VPRN
SNTP B.Cast : False
MAC Address : 14:30:ff:00:00:00 Arp Timeout : 14400
IP MTU : 0 ICMP Mask Reply : True
Arp Populate : Disabled Host Conn Verify : Disabled
Proxy ARP Details
Rem Proxy ARP : Disabled Local Proxy ARP : Disabled
Policies : none

Proxy Neighbor Discovery Details
Local Pxy ND : Disabled Policies : none

DHCP Details
Admin State : Down Lease Populate : 0
Gi-Addr : Not configured Gi-Addr as Src Ip : Disabled
Action : Keep Trusted : Disabled

DHCP Proxy Details
Admin State : Down
Lease Time : N/A
Emul. Server : Not configured

Subscriber Authentication Details
Auth Policy : None

DHCP6 Relay Details
Admin State : Down Lease Populate : 0
Oper State : Down Nbr Resolution : Disabled
If-Id Option : None Remote Id : Disabled
Src Addr : Not configured

DHCP6 Server Details
Admin State : Down Max. Lease States : 8000
ICMP Details
Redirects : Number - 100                     Time (seconds) - 10
Unreachables : Number - 100                    Time (seconds) - 10
TTL Expired : Number - 100                     Time (seconds) - 10

IPCP Address Extension Details
Peer IP Addr : Not configured
Peer Pri DNS Addr : Not configured
Peer Sec DNS Addr : Not configured

<table>
<thead>
<tr>
<th>Interface</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>If Name</td>
<td>gizmo</td>
</tr>
<tr>
<td>Admin State</td>
<td>Up</td>
</tr>
<tr>
<td>Protocols</td>
<td>None</td>
</tr>
<tr>
<td>IP Addr/mask</td>
<td>Not Assigned</td>
</tr>
<tr>
<td>If Index</td>
<td>5</td>
</tr>
<tr>
<td>Last Oper Chg</td>
<td>06/18/2007 10:07:01</td>
</tr>
<tr>
<td>SDP Id</td>
<td>spoke-1:10</td>
</tr>
<tr>
<td>TOS Marking</td>
<td>Trusted</td>
</tr>
<tr>
<td>Egress Filter</td>
<td>none</td>
</tr>
<tr>
<td>SNTP B.Cast</td>
<td>False</td>
</tr>
<tr>
<td>MAC Address</td>
<td>14:30:ff:00:00:00</td>
</tr>
<tr>
<td>IP MTU</td>
<td>0</td>
</tr>
<tr>
<td>ICMP Mask Reply</td>
<td>True</td>
</tr>
<tr>
<td>If Name</td>
<td>test123</td>
</tr>
<tr>
<td>Admin State</td>
<td>Up</td>
</tr>
<tr>
<td>Protocols</td>
<td>None</td>
</tr>
<tr>
<td>IP Addr/mask</td>
<td>Not Assigned</td>
</tr>
<tr>
<td>If Index</td>
<td>6</td>
</tr>
<tr>
<td>Last Oper Chg</td>
<td>06/18/2007 10:07:01</td>
</tr>
<tr>
<td>Port Id</td>
<td>n/a</td>
</tr>
<tr>
<td>TOS Marking</td>
<td>Trusted</td>
</tr>
<tr>
<td>Egress Filter</td>
<td>none</td>
</tr>
<tr>
<td>SNTP B.Cast</td>
<td>False</td>
</tr>
<tr>
<td>MAC Address</td>
<td></td>
</tr>
<tr>
<td>IP MTU</td>
<td>0</td>
</tr>
<tr>
<td>ICMP Mask Reply</td>
<td>True</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Interface</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>If Name</td>
<td>test1</td>
</tr>
<tr>
<td>Admin State</td>
<td>Up</td>
</tr>
<tr>
<td>Protocols</td>
<td>None</td>
</tr>
<tr>
<td>IP Addr/mask</td>
<td>Not Assigned</td>
</tr>
<tr>
<td>If Index</td>
<td>7</td>
</tr>
<tr>
<td>Last Oper Chg</td>
<td>06/18/2007 10:07:01</td>
</tr>
<tr>
<td>Port Id</td>
<td>n/a</td>
</tr>
<tr>
<td>TOS Marking</td>
<td>Trusted</td>
</tr>
<tr>
<td>If Type</td>
<td>VPRN Red</td>
</tr>
</tbody>
</table>
### Interface

<table>
<thead>
<tr>
<th>If Name</th>
<th>bozoclown</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin State</td>
<td>Up</td>
</tr>
<tr>
<td>Oper (v4/v6)</td>
<td>Down/--</td>
</tr>
<tr>
<td>Protocols</td>
<td>None</td>
</tr>
<tr>
<td>IP Addr/mask</td>
<td>Not Assigned</td>
</tr>
</tbody>
</table>

**Details**

<table>
<thead>
<tr>
<th>If Index</th>
<th>8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last Oper Chg</td>
<td>06/18/2007 10:07:01 Global If Index</td>
</tr>
<tr>
<td>Port Id</td>
<td>n/a</td>
</tr>
<tr>
<td>TOS Marking</td>
<td>Trusted</td>
</tr>
<tr>
<td>Egress Filter</td>
<td>none</td>
</tr>
<tr>
<td>Ingress Filter</td>
<td>none</td>
</tr>
<tr>
<td>SNTP B.Cast</td>
<td>False</td>
</tr>
<tr>
<td>QoS Policy</td>
<td>1</td>
</tr>
<tr>
<td>MAC Address</td>
<td></td>
</tr>
<tr>
<td>IP MTU</td>
<td>0</td>
</tr>
<tr>
<td>ICMP Mask Reply</td>
<td>True</td>
</tr>
</tbody>
</table>

### Interface

<table>
<thead>
<tr>
<th>If Name</th>
<th>testabc</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin State</td>
<td>Up</td>
</tr>
<tr>
<td>Oper (v4/v6)</td>
<td>Down/--</td>
</tr>
<tr>
<td>Protocols</td>
<td>None</td>
</tr>
<tr>
<td>IP Addr/mask</td>
<td>Not Assigned</td>
</tr>
</tbody>
</table>

**Details**

<table>
<thead>
<tr>
<th>If Index</th>
<th>9</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last Oper Chg</td>
<td>06/18/2007 10:07:01 Global If Index</td>
</tr>
<tr>
<td>If Type</td>
<td>VPRN Sub</td>
</tr>
</tbody>
</table>

**DHCP Details**

| Gi-Addr | Not configured            |
| Gi-Addr as Src Ip | Disabled                 |

### Interface testabc group-interfaces

<table>
<thead>
<tr>
<th>Interface-Name</th>
<th>Adm</th>
<th>Opr(v4/v6)</th>
<th>Mode</th>
<th>Port/SapId</th>
</tr>
</thead>
<tbody>
<tr>
<td>bozo</td>
<td>Up</td>
<td>Down/--</td>
<td>VPRN G* n/a</td>
<td></td>
</tr>
</tbody>
</table>

Group-Interfaces : 1

* indicates that the corresponding row element may have been truncated.
VPRN Show Commands

Last Oper Chg : 06/18/2007 10:07:01 Global If Index : 88
Port Id : n/a
TOS Marking : Trusted If Type : VPRN Grp
SNTP B.Cast : False
MAC Address : Arp Timeout : 14400
IP MTU : 0 ICMP Mask Reply : True
Arp Populate : Disabled Host Conn Verify : Disabled

Proxy ARP Details
Rem Proxy ARP : Disabled Local Proxy ARP : Enabled
Policies : none

Proxy Neighbor Discovery Details
Local Pxy ND : Disabled
Policies : none

DHCP Details
Admin State : Down
Gi-Addr : Unknown
Action : Keep
Match CircId : Disabled

DHCP Proxy Details
Admin State : Down
Lease Time : N/A
Emul. Server : Not configured

Subscriber Authentication Details
Auth Policy : None

DHCP6 Relay Details
Admin State : Down
Oper State : Down
If-Ip Option : None
Src Addr : Not configured

DHCP6 Server Details
Admin State : Down
Max. Lease States : 8000

ICMP Details
Redirects : Number - 100 Time (seconds) - 10
Unreachables : Number - 100 Time (seconds) - 10
TTL Expired : Number - 100 Time (seconds) - 10

IPCP Address Extension Details
Peer IP Addr : Not configured
Peer Pri DNS Addr : Not configured
Peer Sec DNS Addr : Not configured

PPPoE Details
Last Mgmt Chg: 06/18/2007 10:06:49
Session limit : 1 SAP session limit : 1
PPPoE Policy : N/A
User DB : N/A

Service Access Point(Summary), Service 1 Interface bozo

<table>
<thead>
<tr>
<th>PortId</th>
<th>SvcId</th>
<th>Ing. Ing.</th>
<th>Egr. Egr.</th>
<th>Anti</th>
<th>Adm Opr</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>QoS Fltr</td>
<td>QoS Fltr</td>
<td>Spoof</td>
<td></td>
</tr>
</tbody>
</table>

No Service Access Point found.
If Name: santa  
Admin State: Up  
Oper (v4/v6): Down/--  
Protocols: None  
IP Addr/mask: Not Assigned

Details

If Index: 11  
Virt. If Index: 11  
Last Oper Chg: 06/18/2007 10:07:01  
Global If Index: 87  
If Type: VPRN Sub  

DHCP Details
Gi-Addr: Not configured  
Gi-Addr as Src Ip: Disabled  

Interface santa group-interfaces

Interface-Name                   Adm         Opr(v4/v6)  Mode    Port/SapId  
IP-Address                                                    PfxState  
-------------------------------------------------------------------------------
interface                        Up          Down/--     VPRN G* 1/2/4  
-------------------------------------------------------------------------------
Group-Interfaces : 1

* indicates that the corresponding row element may have been truncated.

Interface

If Name: interface  
Sub If Name: santa  
Red If Name:  
Admin State: Up  
Oper (v4/v6): Down/--  
Protocols: None

Details

If Index: 12  
Virt. If Index: 12  
Last Oper Chg: 06/18/2007 10:07:01  
Global If Index: 86  
Group Port: 1/2/4  
TOS Marking: Trusted  
If Type: VPRN Grp  
SNTP B.Cast: False  
MAC Address: 14:30:01:02:00:04  
Arp Timeout: 14400  
IP MTU: 1500  
ICMP Mask Reply: True  
Arp Populate: Disabled  
Host Conn Verify: Disabled  
Proxy ARP Details
Rem Proxy ARP: Disabled  
Local Proxy ARP: Enabled  
Policies: none

Proxy Neighbor Discovery Details
Local Fxy ND: Disabled  
Policies: none

DHCP Details
Admin State: Down  
Lease Populate: 1  
Gi-Addr: Unknown  
Gi-Addr as Src Ip: Disabled  
Action: Keep  
Trusted: Disabled  
Match CircId: Disabled

DHCP Proxy Details
Admin State: Down  
Lease Time: N/A
Emul. Server : Not configured

Subscriber Authentication Details
Auth Policy : None

DHCP6 Relay Details
Admin State : Down Lease Populate : 0
Oper State : Down Nbr Resolution : Disabled
If-Id Option : None Remote Id : Disabled
Src Addr : Not configured

DHCP6 Server Details
Admin State : Down Max. Lease States : 8000

ICMP Details
Redirects : Number - 100 Time (seconds) - 10
Unreachables : Number - 100 Time (seconds) - 10
TTL Expired : Number - 100 Time (seconds) - 10

IPCP Address Extension Details
Peer IP Addr : Not configured
Peer Pri DNS Addr : Not configured
Peer Sec DNS Addr : Not configured

PPPoE Details
Last Mgmt Chg: 06/18/2007 10:06:49
Session limit : 1 SAP session limit : 1
PPPoE Policy : N/A
User DB : N/A

Service Access Point(Summary), Service 1 Interface interface

<table>
<thead>
<tr>
<th>PortId</th>
<th>SvcId</th>
<th>Ing. QoS</th>
<th>Ing. Fltr</th>
<th>Egr. QoS</th>
<th>Egr. Fltr</th>
<th>Anti</th>
<th>Adm</th>
<th>Opr</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/2/4:0</td>
<td>1</td>
<td>1</td>
<td>none</td>
<td>1</td>
<td>none</td>
<td>ip-mac Up</td>
<td>Down</td>
<td></td>
</tr>
</tbody>
</table>

*A:bksim1618# show service id 2 all

Service Detailed Information

<table>
<thead>
<tr>
<th>Service Id</th>
<th>Vpn Id</th>
<th>Service Type</th>
<th>Name</th>
<th>Description</th>
<th>Customer Id</th>
<th>Creation Origin</th>
<th>Last Status Change</th>
<th>Last Mgmt Change</th>
<th>Admin State</th>
<th>Oper State</th>
<th>Route Dist.</th>
<th>AS Number</th>
<th>ECMP</th>
<th>Max IPV4 Routes</th>
<th>Max IPV6 Routes</th>
<th>Ignore NH Metric</th>
<th>Hash Label</th>
<th>Vrf Target</th>
<th>Vrf Import</th>
<th>Vrf Export</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>0</td>
<td>VPRN</td>
<td>(Not Specified)</td>
<td>(Not Specified)</td>
<td>1</td>
<td>manual</td>
<td>08/21/2013 08:54:14</td>
<td>08/21/2013 08:56:06</td>
<td>Down</td>
<td>Down</td>
<td>None</td>
<td>None</td>
<td>Enabled</td>
<td>No Limit</td>
<td>No Limit</td>
<td>Disabled</td>
<td>Disabled</td>
<td>None</td>
<td>None</td>
<td></td>
</tr>
</tbody>
</table>
authenticaton

Syntax authentication

Context show>service>id

Description This command enables the context to display subscriber authentication information.

statistics

Syntax statistics [policy name] [sap sap-id]

Context show>service>id>authentication

Description This command displays session authentication statistics for this service.

Parameters policy name — Specifies the subscriber authentication policy statistics to display.

sap sap-id — Specifies the SAP ID statistics to display. See Common CLI Command Descriptions on page 1783 for command syntax.

Sample Output

*A:ALA-1# show service id 11 authentication statistics

============================================================================
VPRN Show Commands

Authentication statistics

<table>
<thead>
<tr>
<th>Interface / SAP</th>
<th>Authentication Successful</th>
<th>Authentication Failed</th>
</tr>
</thead>
<tbody>
<tr>
<td>abc-11-90.1.0.254</td>
<td>1582</td>
<td>3</td>
</tr>
</tbody>
</table>

Number of entries: 1

*A:ALA-1#

arp

Syntax arp [ip-address] | [mac ieee-address] | [sap sap-id] | [interface ip-int-name] [sdp sdp-id:vc-id] [summary]

Context show>service>id

Description Displays the ARP table for the IES instance.

Parameters

- **ip-address** — Displays only ARP entries in the ARP table with the specified IP address.
  - **Default** All IP addresses.

- **mac ieee-address** — Displays only ARP entries in the ARP table with the specified 48-bit MAC address.
  - The MAC address can be expressed in the form aa:bb:cc:dd:ee:ff or aa-bb-cc-dd-ee-ff where aa, bb, cc, dd, ee and ff are hexadecimal numbers.
  - **Default** All MAC addresses.

- **sap sap-id** — Displays SAP information for the specified SAP ID. See Common CLI Command Descriptions on page 1783 for command syntax.

- **port id** — Specifies matching service ARP entries associated with the specified IP interface.
  - **Values** 1.0.0.0 — 223.255.255.255

- **ip-int-name** — The IP interface name for which to display matching ARPs.

Output Show Service-ID ARP — The following table describes show service-id ARP output fields.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service ID</td>
<td>The service ID number.</td>
</tr>
<tr>
<td>Interface / SAP</td>
<td>The specified SAP address.</td>
</tr>
<tr>
<td>Source-Identifier</td>
<td>The location the MAC is defined.</td>
</tr>
<tr>
<td>Type</td>
<td>FDB entries created by management.</td>
</tr>
<tr>
<td>Number of entries: 1</td>
<td>Learned — Dynamic entries created by the learning process.</td>
</tr>
<tr>
<td>*A:ALA-1#</td>
<td>OAM — Entries created by the OAM process.</td>
</tr>
<tr>
<td>Age</td>
<td>The time elapsed since the service was enabled.</td>
</tr>
<tr>
<td>Interface</td>
<td>The interface applied to the service.</td>
</tr>
</tbody>
</table>
Service ID | The service ID number.
MAC | The specified MAC address
Source-Identifier | The location the MAC is defined.
Type
Static | FDB entries created by management.
Learned | Dynamic entries created by the learning process.
OAM | Entries created by the OAM process.
Age | The time elapsed since the service was enabled.
Interface | The interface applied to the service.

Sample Output

```
*A:ALA-12# show service id 2 arp
ARP Table
+-------------------+-------------------+-------------------+-------------------+-------------------+-------------------+-------------------+-------------------+
| IP Address        | MAC Address       | Type             | Age              | Interface         | Port              |
|-------------------+-------------------+-------------------+-------------------+-------------------+-------------------+-------------------+
| 190.11.1.1        | 00:03:fa:00:08:22 | Other            | 00:00:00         | ies-100-190.11.1  | 1/1/11:0          |
+-------------------+-------------------+-------------------+-------------------+-------------------+-------------------+-------------------+
*A:ALA-12#
```

arp-host

**Syntax**

```
arp-host [wholesaler service-id] [sap sap-id | interface interface-name | ip-address ip-address[/mask] | mac ieee-address | [(port port-id) [no-inter-dest-id | inter-dest-id inter-dest-id]]] [detail]
arp-host statistics [sap sap-id | interface interface-name]
arp-host summary [interface interface-name]
```

**Context**

show>service>id

**Description**

This command displays ARP host related information.

Sample Output

```
*A:Dut-C# show service id 2 arp-host
ARP host table, service 2
+-------------------+-------------------+-------------------+-------------------+-------------------+-------------------+-------------------+-------------------+
| IP Address        | Mac Address       | Sap Id            | Remaining Time    | MC Stdby          |
|-------------------+-------------------+-------------------+-------------------+-------------------+-------------------+-------------------+-------------------+
| 128.128.1.2       | 00:80:00:00:00:01 | 2/1/5:2           | 00h04m41s         |
| 128.128.1.3       | 00:80:00:00:00:02 | 2/1/5:2           | 00h04m42s         |
| 128.128.1.4       | 00:80:00:00:00:03 | 2/1/5:2           | 00h04m43s         |
| 128.128.1.5       | 00:80:00:00:00:04 | 2/1/5:2           | 00h04m44s         |
| 128.128.1.6       | 00:80:00:00:00:05 | 2/1/5:2           | 00h04m45s         |
| 128.128.1.7       | 00:80:00:00:00:06 | 2/1/5:2           | 00h04m46s         |
| 128.128.1.8       | 00:80:00:00:00:07 | 2/1/5:2           | 00h04m47s         |
| 128.128.1.9       | 00:80:00:00:00:08 | 2/1/5:2           | 00h04m48s         |
```
ARP hosts for service 2

Service ID : 2
IP Address : 128.128.1.2
MAC Address : 00:80:00:00:00:01
SAP : 2/1/5:2
Remaining Time : 00h04m58s

Sub-Ident : "alu_1_2"
Sub-Profile-String : ""
SLA-Profile-String : ""
App-Profile-String : ""
ARP host ANCP-String : ""
ARP host Int Dest Id : ""
RADIUS-User-Name : "128.128.1.2"

Session Timeout (s) : 301
Start Time : 02/09/2009 16:35:07
Last Auth : 02/09/2009 16:36:34
Last Refresh : 02/09/2009 16:36:38
Persistence Key : N/A

Number of ARP hosts : 1

ARP host statistics

Num Active Hosts : 20
Received Triggers : 70
Ignored Triggers : 10
Ignored Triggers (overload) : 0
SHCV Checks Forced : 0
Hosts Created : 20
Hosts Updated : 40
Hosts Deleted : 0
Authentication Requests Sent : 40

ARP host summary, service 2

Sap | Used | Provided | Admin State
-----------------------------
sap:2/1/5:2 | 20 | 8000 | inService

Number of SAPs : 1
**show, clear, debug commands**

---

*A: Dut-C#

**base**

**Syntax**  
`base`

**Context**  
`show > service > id`

**Description**  
Displays basic information about the service ID including service type, description, SAPs and SDPs.

**Output**  
Show Service-ID Base — The following table describes show service-id base output fields:

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Id</td>
<td>The service identifier.</td>
</tr>
<tr>
<td>Vpn Id</td>
<td>Specifies the VPN ID assigned to the service.</td>
</tr>
<tr>
<td>Service Type</td>
<td>Specifies the type of service.</td>
</tr>
<tr>
<td>Description</td>
<td>Generic information about the service.</td>
</tr>
<tr>
<td>Customer Id</td>
<td>The customer identifier.</td>
</tr>
<tr>
<td>Last Mgmt Change</td>
<td>The date and time of the most recent management-initiated change to this customer.</td>
</tr>
<tr>
<td>Adm</td>
<td>The desired state of the service.</td>
</tr>
<tr>
<td>Oper</td>
<td>The operating state of the service.</td>
</tr>
<tr>
<td>Mtu</td>
<td>The largest frame size (in octets) that the service can handle.</td>
</tr>
<tr>
<td>Def. Mesh VC Id</td>
<td>This object is only valid in services that accept mesh SDP bindings. It is used to validate the VC ID portion of each mesh SDP binding defined in the service.</td>
</tr>
<tr>
<td>SAP Count</td>
<td>The number of SAPs defined on the service.</td>
</tr>
<tr>
<td>SDP Bind Count</td>
<td>The number of SDPs bound to the service.</td>
</tr>
<tr>
<td>Identifier</td>
<td>Specifies the service access (SAP) and destination (SDP) points.</td>
</tr>
<tr>
<td>Type</td>
<td>Specifies the signaling protocol used to obtain the ingress and egress labels used in frames transmitted and received on the SDP.</td>
</tr>
<tr>
<td>AdmMTU</td>
<td>Specifies the desired largest service frame size (in octets) that can be transmitted through this SDP to the far-end ESR, without requiring the packet to be fragmented.</td>
</tr>
<tr>
<td>OprMTU</td>
<td>Specifies the actual largest service frame size (in octets) that can be transmitted through this SDP to the far-end ESR, without requiring the packet to be fragmented.</td>
</tr>
</tbody>
</table>

---
Sample Output

*A:SetupCLI# show service id 3 base

Service Basic Information

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Id</td>
<td>3</td>
</tr>
<tr>
<td>Vpn Id</td>
<td>0</td>
</tr>
<tr>
<td>Service Type</td>
<td>VPRN</td>
</tr>
<tr>
<td>Name</td>
<td>(Not Specified)</td>
</tr>
<tr>
<td>Description</td>
<td>(Not Specified)</td>
</tr>
<tr>
<td>Customer Id</td>
<td>1</td>
</tr>
<tr>
<td>Last Status Change</td>
<td>10/08/2009 04:55:01</td>
</tr>
<tr>
<td>Last Mgmt Change</td>
<td>10/08/2009 06:48:38</td>
</tr>
<tr>
<td>Admin State</td>
<td>Down</td>
</tr>
<tr>
<td>Oper State</td>
<td>Down</td>
</tr>
<tr>
<td>Route Dist.</td>
<td>None</td>
</tr>
<tr>
<td>VPRN Type</td>
<td>regular</td>
</tr>
<tr>
<td>AS Number</td>
<td>None</td>
</tr>
<tr>
<td>Router Id</td>
<td>10.20.30.40</td>
</tr>
<tr>
<td>ECMP</td>
<td>Enabled</td>
</tr>
<tr>
<td>ECMP Max Routes</td>
<td>1</td>
</tr>
<tr>
<td>Max IPv4 Routes</td>
<td>No Limit</td>
</tr>
<tr>
<td>Auto Bind</td>
<td>MPLS</td>
</tr>
<tr>
<td>Max IPv6 Routes</td>
<td>No Limit</td>
</tr>
<tr>
<td>Ignore NH Metric</td>
<td>Disabled</td>
</tr>
<tr>
<td>Hash Label</td>
<td>Enabled</td>
</tr>
<tr>
<td>Vrf Target</td>
<td>None</td>
</tr>
<tr>
<td>Vrf Import</td>
<td>None</td>
</tr>
<tr>
<td>Vrf Export</td>
<td>None</td>
</tr>
<tr>
<td>MVPN Vrf Target</td>
<td>None</td>
</tr>
<tr>
<td>MVPN Vrf Import</td>
<td>None</td>
</tr>
<tr>
<td>MVPN Vrf Export</td>
<td>None</td>
</tr>
<tr>
<td>SAP Count</td>
<td>0</td>
</tr>
<tr>
<td>SDP Bind Count</td>
<td>1</td>
</tr>
</tbody>
</table>

Service Access & Destination Points

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Type</th>
<th>AdmMTU</th>
<th>OprMTU</th>
<th>Adm</th>
<th>Opr</th>
</tr>
</thead>
<tbody>
<tr>
<td>sdp:2000:1</td>
<td>TLDP</td>
<td>1500</td>
<td>1500</td>
<td>Up</td>
<td>Down</td>
</tr>
</tbody>
</table>

*A:SetupCLI#
Show, Clear, Debug Commands

Parameters

- **ip-address** — The IP address of the interface for which to display information.
  - **Values**
    - 1.0.0.0 — 223.255.255.255

- **ip-int-name** — The IP interface name for which to display information.

- **family** — Specifies the family to display.
  - **Values**
    - ipv4, ipv6

- **interface-type** — Specifies the interface type.
  - **Values**
    - subscriber, group, redundant

- **detail** — Displays detailed IP interface information.
  - **Default**
    - IP interface summary output.

Output

**Show Service-ID Interface** — The following table describes show service-id interface output fields:

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface-Name</td>
<td>The name used to refer to the interface.</td>
</tr>
<tr>
<td>Type</td>
<td>Specifies the interface type.</td>
</tr>
<tr>
<td>IP-Address</td>
<td>Specifies the IP address/IP subnet/broadcast address of the interface.</td>
</tr>
<tr>
<td>Adm</td>
<td>The desired state of the interface.</td>
</tr>
<tr>
<td>Opr</td>
<td>The operating state of the interface.</td>
</tr>
<tr>
<td>Interface If Name</td>
<td>The name used to refer to the interface.</td>
</tr>
<tr>
<td>Admin State</td>
<td>The desired state of the interface.</td>
</tr>
<tr>
<td>Oper State</td>
<td>The operating state of the interface.</td>
</tr>
<tr>
<td>IP Addr/mask Details</td>
<td>Specifies the IP address/IP subnet/broadcast address of the interface.</td>
</tr>
<tr>
<td>If Index</td>
<td>The index corresponding to this interface. The primary index is 1. For</td>
</tr>
<tr>
<td></td>
<td>example, all interfaces are defined in the Base virtual router context.</td>
</tr>
<tr>
<td>If Type</td>
<td>Specifies the interface type.</td>
</tr>
<tr>
<td>Port Id</td>
<td>Specifies the SAP’s port ID.</td>
</tr>
<tr>
<td>SNTF B.Cast</td>
<td>Specifies whether SNTP broadcast client mode is enabled or disabled.</td>
</tr>
<tr>
<td>Arp Timeout</td>
<td>Specifies the timeout for an ARP entry learned on the interface.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>Specifies the 48-bit IEEE 802.3 MAC address.</td>
</tr>
<tr>
<td>ICMP Mask Reply</td>
<td>Specifies whether ICMP mask reply is enabled or disabled.</td>
</tr>
<tr>
<td>Cflowd</td>
<td>Specifies whether Cflowd collection and analysis on the interface is enabled</td>
</tr>
<tr>
<td>ICMP Details</td>
<td>Specifies the rate for ICMP redirect messages.</td>
</tr>
<tr>
<td>Redirects</td>
<td></td>
</tr>
</tbody>
</table>
Sample Output

*A:ALA-12# show service id 321 interface

Interface Table

<table>
<thead>
<tr>
<th>Interface-Name</th>
<th>Type</th>
<th>IP-Address</th>
<th>Adm</th>
<th>Opr</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>test</td>
<td>Pri</td>
<td>190.11.1.1/24</td>
<td>Up</td>
<td>Up</td>
<td>IES</td>
</tr>
</tbody>
</table>

Interfaces : 1

*A:ALA-12#

A:ALA-49# show service id 88 interface detail

Interface Table

Interface

If Name : Sector A
Admin State : Up
Oper State : Down
Protocols : None

IP Addr/mask : Not Assigned

Details

Description : If Index : 26
Virt. If Index : 26
SAP Id : /1/1.2.2
TOS Marking : Untrusted
If Type : IES
SNTP B.Cast : False
IES ID : 88
MAC Address : Not configured.
Arp Timeout : 14400
IP MTU : 1500
ICMP Mask Reply : True
Arp Populate : Disabled
Cflowd : None

Proxy ARP Details
Proxy ARP : Enabled
Local Proxy ARP : Disabled

Policies : ProxyARP

DHCP Details
Admin State : Up
Lease Populate : 0
Action : Keep
Trusted : Disabled

ICMP Details
Redirects : Number - 100
Time (seconds) : 10
Unreachables : Number - 100
Time (seconds) : 10
TTL Expired : Number - 100
Time (seconds) : 10

Interface

Unreachables
Specifies the rate for ICMP unreachable messages.

TTL Expired
Specifies the rate for ICMP TTL messages.
If Name : test
Admin State : Up
Oper State : Down
Protocols : None
IP Addr/mask : Not Assigned

Details

Description :
If Index : 27
Virt. If Index : 27
SAP Id : /1/2:0
TOS Marking : Untrusted
If Type : IES
SNTP B.Cast : False
IES ID : 88
MAC Address : Not configured.
Arp Timeout : 14400
IP MTU : 1500
ICMP Mask Reply : True
Arp Populate : Disabled
If Type : IES

Proxy ARP Details
Proxy ARP : Disabled
Local Proxy ARP : Disabled

DHCP Details
Admin State : Up
Oper State : Down
Action : Keep
Trusted : Disabled
Lease Populate : 0

ICMP Details
Redirects : Number - 100
Time (seconds) - 10
Unreachable : Number - 100
Time (seconds) - 10
TTL Expired : Number - 100
Time (seconds) - 10

Interfaces : 2

*A:SetupCLI# show service id 3 interface "ab" detail

Interface Table

Interface

If Name : ab
Admin State : Up
Oper (v4/v6) : Down/--
Protocols : None
IP Addr/mask : Not Assigned

Details

Description : (Not Specified)
If Index : 2
Virt. If Index : 2
Last Oper Chg: 10/08/2009 07:07:58
Global If Index : 329
SDP Id : spoke-2000:1

Spoke-SDP Details
Admin State : Up
Oper State : Down
Hash Label : Enabled
Flags : SvcAdminDown SdpOperDown
NoIngVCLabel NoEgrVCLabel

TOS Marking : Trusted
If Type : VPRN
SNTP B.Cast : False
MAC Address : 76:6d:ff:00:00:00                Arp Timeout : 14400
IP Oper MTU : 0                                ICMP Mask Reply : True
Arp Populate : Disabled                         Host Conn Verify : Disabled
Cflowd : None
LdpSyncTimer : None
LSR Load Bal*: system                         uRPF Chk : disabled
uRPF Fail By*: 0                                uRPF Chk Fail Pk*: 0
Proxy ARP Details
Rem Proxy ARP: Disabled                         Local Proxy ARP : Disabled
Policies : none

Proxy Neighbor Discovery Details
Local Pxy ND : Disabled
Policies : none

DHCP no local server

DHCP Details
Description : (Not Specified)
Admin State : Down                            Lease Populate : 0
Gi-Addr : Not configured                     Gi-Addr as Src Ip: Disabled
Action : Keep                                Trusted : Disabled

DHCP Proxy Details
Admin State : Down
Lease Time : N/A
Emul. Server : Not configured

Subscriber Authentication Details
Auth Policy : None

DHCP6 Relay Details
Description : (Not Specified)
Admin State : Down                            Lease Populate : 0
Oper State : Down                             Nbr Resolution : Disabled
If-Id Option : None                           Remote Id : Disabled
Src Addr : Not configured

DHCP6 Server Details
Admin State : Down                            Max. Lease States: 8000

ICMP Details
Redirects : Number - 100                      Time (seconds) - 10
Unreaches : Number - 100                      Time (seconds) - 10
TTL Expired : Number - 100                    Time (seconds) - 10

IPCP Address Extension Details
Peer IP Addr*: Not configured
Peer Pri DNS*: Not configured
Peer Sec DNS*: Not configured

Routed VPLS Details
VPLS Name                           Binding Status : Up
------------------------------------------------------------------------
Interfaces : 1
------------------------------------------------------------------------
* indicates that the corresponding row element may have been truncated.
*A:SetupCLIp#
The Oper Hash Label and Hash Lbl Sig Cap spoke-sdp fields display when signal-capability is enabled and operational state of hash-label in datapath.

--------------------------------------------------
Service Destination Points (SDPs)
--------------------------------------------------

Sdp Id 1:555  -(2.2.2.2)

Description : (Not Specified)
SDP Id             : 1:555                    Type              : Spoke
Spoke Descr     : (Not Specified)
VC Type            : Ether                    VC Tag            : n/a
Admin Path MTU     : 0                        Oper Path MTU     : 1568
Far End            : 2.2.2.2                  Delivery          : MPLS
Tunnel Far End     : n/a                      LSP Types         : RSVP
Hash Label         : Disabled                 Hash Lbl Sig Cap  : Disabled
Oper Hash Label    : Disabled
Admin State        : Up                       Oper State        : Up
Acct. Pol          : None                     Collect Stats     : Disabled
Ingress Label      : 131065                   Egress Label      : 131059
Ingr Mac Fltr-Id   : n/a                      Egr Mac Fltr-Id   : n/a
Ingr IP Fltr-Id    : n/a                      Egr IP Fltr-Id    : n/a
Ingr IPv6 Fltr-Id  : n/a                      Egr IPv6 Fltr-Id  : n/a
Admin ControlWord  : Not Preferred            Oper ControlWord  : False
Admin BW(Kbps)     : 0                        Oper BW(Kbps)     : 0
Last Mgmt Change   : 11/24/2010 13:00:48      Force Vlan-Vc     : Disabled
Endpoint           : N/A                      Precedence        : 4
PW Status Sig      : Enabled
Class Fwding State : Down
Flags              : None
Peer Pw Bits       : None
Peer Fault Ip      : None
Peer Vccv CV Bits  : lspPing
Peer Vccv CC Bits  : mplsRouterAlertLabel
Application Profile: None
Standby Sig Slave  : False

---

**retailers**

**Syntax** retailers

**Context** show>service>id

**Description** This command displays the service ID of the retailer subscriber service to which this DHCP lease belongs.

**Sample Output**
*A:ALA-48#config# show service id 101 retailers*

Retailers for service 101
<table>
<thead>
<tr>
<th>Retailer Svc ID</th>
<th>Num Static Hosts</th>
<th>Num Dynamic Hosts</th>
</tr>
</thead>
<tbody>
<tr>
<td>102</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>105</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

Number of retailers : 2

*A:ALA-48>config#*
Show, Clear, Debug Commands

**sap**

**Syntax**
```
sap sap-id [detail]
```

**Context**
```
show>service?id
```

**Description**
Displays information for the SAPs associated with the service.
If no optional parameters are specified, a summary of all associated SAPs is displayed.

**Parameters**
- `sap-id` — The ID that displays SAPs for the service. See Common CLI Command Descriptions on page 1783 for command syntax.
- `detail` — Displays detailed information for the SAP.

**Output**
**Show Service-ID SAP** — The following table describes show service SAP fields:

**Sample Output**

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Id</td>
<td>The service identifier.</td>
</tr>
<tr>
<td>SAP</td>
<td>The SAP and qtag.</td>
</tr>
<tr>
<td>Encap</td>
<td>The encapsulation type of the SAP.</td>
</tr>
<tr>
<td>Ethertype</td>
<td>Specifies an Ethernet type II Ethertype value.</td>
</tr>
<tr>
<td>Admin State</td>
<td>The administrative state of the SAP.</td>
</tr>
<tr>
<td>Oper State</td>
<td>The operating state of the SAP.</td>
</tr>
<tr>
<td>Flags</td>
<td>Specifies the conditions that affect the operating status of this SAP.</td>
</tr>
<tr>
<td></td>
<td>Display output includes: ServiceAdminDown, SapAdminDown, InterfaceAdminDown,</td>
</tr>
<tr>
<td>Last Status Change</td>
<td>Specifies the time of the most recent operating status change to this SAP</td>
</tr>
<tr>
<td>Last Mgmt Change</td>
<td>Specifies the time of the most recent management-initiated change to this SAP.</td>
</tr>
<tr>
<td>Admin MTU</td>
<td>The desired largest service frame size (in octets) that can be transmitted through the SAP to the far-end router, without requiring the packet to be fragmented.</td>
</tr>
<tr>
<td>Oper MTU</td>
<td>The actual largest service frame size (in octets) that can be transmitted through the SAP to the far-end router, without requiring the packet to be fragmented.</td>
</tr>
<tr>
<td>Label</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Ingress qos-policy</td>
<td>The ingress QoS policy ID assigned to the SAP.</td>
</tr>
<tr>
<td>Egress qos-policy</td>
<td>The egress QoS policy ID assigned to the SAP.</td>
</tr>
<tr>
<td>Ingress Filter-Id</td>
<td>The ingress filter policy ID assigned to the SAP.</td>
</tr>
<tr>
<td>Egress Filter-Id</td>
<td>The egress filter policy ID assigned to the SAP.</td>
</tr>
<tr>
<td>Acct. Pol</td>
<td>The accounting policy ID assigned to the SAP.</td>
</tr>
<tr>
<td>Collect Stats</td>
<td>Specifies whether collect stats is enabled.</td>
</tr>
<tr>
<td>Dropped</td>
<td>The number of packets and octets dropped due to SAP state, ingress MAC or IP filter, same segment discard, bad checksum, etc.</td>
</tr>
<tr>
<td>Off. HiPrio</td>
<td>The number of high priority packets and octets, as determined by the SAP ingress QoS policy, offered by the Pchip to the Qchip.</td>
</tr>
<tr>
<td>Off. LowPrio</td>
<td>The number of low priority packets and octets, as determined by the SAP ingress QoS policy, offered by the Pchip to the Qchip.</td>
</tr>
<tr>
<td>Off. Uncolor</td>
<td>The number of uncolored packets and octets, as determined by the SAP ingress QoS policy, offered by the Pchip to the Qchip.</td>
</tr>
<tr>
<td>Dro. HiPrio</td>
<td>The number of high priority packets and octets, as determined by the SAP ingress QoS policy, dropped by the Qchip due to: MBS exceeded, buffer pool limit exceeded, etc.</td>
</tr>
<tr>
<td>Dro. LowPrio</td>
<td>The number of low priority packets and octets, as determined by the SAP ingress QoS policy, dropped by the Qchip due to: MBS exceeded, buffer pool limit exceeded, etc.</td>
</tr>
<tr>
<td>For. InProf</td>
<td>The number of in-profile packets and octets (rate below CIR) forwarded by the ingress Qchip.</td>
</tr>
<tr>
<td>For. OutProf</td>
<td>The number of out-of-profile packets and octets discarded by the egress Qchip due to MBS exceeded, buffer pool limit exceeded, etc.</td>
</tr>
<tr>
<td>Dro. InProf</td>
<td>The number of in-profile packets and octets discarded by the egress Qchip due to MBS exceeded, buffer pool limit exceeded, etc.</td>
</tr>
<tr>
<td>Dro. OutProf</td>
<td>The number of out-of-profile packets and octets discarded by the egress Qchip due to MBS exceeded, buffer pool limit exceeded, etc.</td>
</tr>
<tr>
<td>For. InProf</td>
<td>The number of in-profile packets and octets (rate below CIR) forwarded by the egress Qchip.</td>
</tr>
<tr>
<td>For. OutProf</td>
<td>The number of out-of-profile packets and octets (rate above CIR) forwarded by the egress Qchip.</td>
</tr>
<tr>
<td>Ingress TD Profile</td>
<td>The profile ID applied to the ingress SAP.</td>
</tr>
<tr>
<td>Egress TD Profile</td>
<td>The profile ID applied to the egress SAP.</td>
</tr>
<tr>
<td>Alarm Cell Handling</td>
<td>The indication that OAM cells are being processed.</td>
</tr>
</tbody>
</table>
Show, Clear, Debug Commands

* A:ALA-12# show service id 321 sap 1/1/4:0

Service Access Points (SAP)

<table>
<thead>
<tr>
<th>Service Id</th>
<th>Encap</th>
<th>Dot1Q Ethertype</th>
<th>QinQ Ethertype</th>
<th>Admin State</th>
<th>Oper State</th>
<th>Flags</th>
</tr>
</thead>
<tbody>
<tr>
<td>321</td>
<td>q-tag</td>
<td>0x8100</td>
<td>0x8100</td>
<td>Up</td>
<td>Down</td>
<td>PortOperDown SapIngressQoSMismatch</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Ingress qos-policy : 100                      Egress qos-policy : 1
Ingress Filter-Id : n/a                      Egress Filter-Id : n/a
Multi Svc Site     : None                     Collect Stats : Disabled
Acct. Pol          : None                      Collect Stats : Disabled

---

*S A:ALA-12# show service id 321 sap 1/1/4:0 detail

Service Access Points (SAP)

<table>
<thead>
<tr>
<th>Service Id</th>
<th>Encap</th>
<th>Dot1Q Ethertype</th>
<th>QinQ Ethertype</th>
<th>Admin State</th>
<th>Oper State</th>
<th>Flags</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1/4:0</td>
<td>q-tag</td>
<td>0x8100</td>
<td>0x8100</td>
<td>Up</td>
<td>Down</td>
<td>PortOperDown SapIngressQoSMismatch</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Ingress qos-policy : 100                      Egress qos-policy : 1
Ingress Filter-Id : n/a                      Egress Filter-Id : n/a
Multi Svc Site     : None                     Collect Stats : Disabled
Acct. Pol          : None                      Collect Stats : Disabled

---

Sap Statistics

<table>
<thead>
<tr>
<th>Packets</th>
<th>Octets</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Forwarding Engine Stats

Dropped : 0
Off. HiPrio : 0
Off. LowPrio : 0
Off. Uncolor : 0

Queueing Stats (Ingress QoS Policy 100)

Dro. HiPrio : 0
Dro. LowPrio : 0
For. InProf : 0
For. OutProf : 0

Queueing Stats (Egress QoS Policy 1)

Dro. InProf : 0
Dro. OutProf : 0

---

Label | Description (Continued)
---|---
AAL-5 Encap | The AAL-5 encapsulation type.

---

Label | Description (Continued)
---|---
AAL-5 Encap | The AAL-5 encapsulation type.

---

Label | Description (Continued)
---|---
AAL-5 Encap | The AAL-5 encapsulation type.

---

Label | Description (Continued)
---|---
AAL-5 Encap | The AAL-5 encapsulation type.

---

Label | Description (Continued)
---|---
AAL-5 Encap | The AAL-5 encapsulation type.

---

Label | Description (Continued)
---|---
AAL-5 Encap | The AAL-5 encapsulation type.

---

Label | Description (Continued)
---|---
AAL-5 Encap | The AAL-5 encapsulation type.

---

Label | Description (Continued)
---|---
AAL-5 Encap | The AAL-5 encapsulation type.

---

Label | Description (Continued)
---|---
AAL-5 Encap | The AAL-5 encapsulation type.

---

Label | Description (Continued)
---|---
AAL-5 Encap | The AAL-5 encapsulation type.

---

Label | Description (Continued)
---|---
AAL-5 Encap | The AAL-5 encapsulation type.

---

Label | Description (Continued)
---|---
AAL-5 Encap | The AAL-5 encapsulation type.

---

Label | Description (Continued)
---|---
AAL-5 Encap | The AAL-5 encapsulation type.

---

Label | Description (Continued)
---|---
AAL-5 Encap | The AAL-5 encapsulation type.

---

Label | Description (Continued)
---|---
AAL-5 Encap | The AAL-5 encapsulation type.

---

Label | Description (Continued)
---|---
AAL-5 Encap | The AAL-5 encapsulation type.
VPRN Show Commands

For. InProf : 0 0
For. OutProf : 0 0

-----------------------------------
Sap per Queue stats
-----------------------------------

<table>
<thead>
<tr>
<th>Packets</th>
<th>Octets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ingress Queue 1 (Unicast) (Priority)</td>
<td></td>
</tr>
<tr>
<td>Off. HiPrio</td>
<td>0</td>
</tr>
<tr>
<td>Off. LoPrio</td>
<td>0</td>
</tr>
<tr>
<td>Dro. HiPrio</td>
<td>0</td>
</tr>
<tr>
<td>Dro. LoPrio</td>
<td>0</td>
</tr>
<tr>
<td>For. InProf</td>
<td>0</td>
</tr>
<tr>
<td>For. OutProf</td>
<td>0</td>
</tr>
</tbody>
</table>

| Ingress Queue 10 (Unicast) (Priority) |
| Off. HiPrio | 0 | 0 |
| Off. LoPrio | 0 | 0 |
| Dro. HiPrio | 0 | 0 |
| Dro. LoPrio | 0 | 0 |
| For. InProf | 0 | 0 |
| For. OutProf | 0 | 0 |

 ATM SAP Configuration Information

Ingress TD Profile : 1 Egress TD Profile : 1
Alarm Cell Handling: Enabled AAL-5 Encap : VC-MUX

*AlA-12#
Show, Clear, Debug Commands

**sdp**

**Syntax**  
```
sdp [sdp-id | far-end ip-addr] [detail]
```

**Context**  
```
show>service>id
```

**Description**  
Displays information for the SDPs associated with the service. If no optional parameters are specified, a summary of all associated SDPs is displayed.

**Parameters**
- `sdp-id` — Displays only information for the specified SDP ID.
  - **Default** All SDPs.
  - **Values** 1 — 17407
- `far-end ip-addr` — Displays only SDPs matching with the specified far-end IP address.
  - **Default** SDPs with any far-end IP address.
- `detail` — Displays detailed SDP information.

**Output**

**Show Service-ID SDP** — The following table describes show service-id SDP output fields:

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sdp Id</td>
<td>The SDP identifier.</td>
</tr>
<tr>
<td>Type</td>
<td>Indicates whether the SDP is a spoke or a mesh.</td>
</tr>
<tr>
<td>Split Horizon Group</td>
<td>Name of the split horizon group that the SDP belongs to.</td>
</tr>
<tr>
<td>VC Type</td>
<td>Displays the VC type: ether or vlan.</td>
</tr>
<tr>
<td>VC Tag</td>
<td>Displays the explicit dot1Q value used when encapsulating to the SDP far end.</td>
</tr>
<tr>
<td>I. Lbl</td>
<td>The VC label used by the far-end device to send packets to this device in this service by the SDP.</td>
</tr>
<tr>
<td>Admin Path MTU</td>
<td>The operating path MTU of the SDP is equal to the admin path MTU (when one is set) or the dynamically computed tunnel MTU, when no admin path MTU is set (the default case.)</td>
</tr>
<tr>
<td>Oper Path MTU</td>
<td>The actual largest service frame size (in octets) that can be transmitted through this SDP to the far-end router, without requiring the packet to be fragmented.</td>
</tr>
<tr>
<td>Far End</td>
<td>Specifies the IP address of the remote end of the GRE or MPLS tunnel defined by this SDP.</td>
</tr>
<tr>
<td>Delivery</td>
<td>Specifies the type of delivery used by the SDP: GRE or MPLS.</td>
</tr>
<tr>
<td>Admin State</td>
<td>The administrative state of this SDP.</td>
</tr>
<tr>
<td>Oper State</td>
<td>The operational state of this SDP.</td>
</tr>
<tr>
<td>Ingress Label</td>
<td>The label used by the far-end device to send packets to this device in this service by this SDP.</td>
</tr>
</tbody>
</table>
Table: SDP Details

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Egress Label</td>
<td>The label used by this device to send packets to the far-end device in this service by the SDP.</td>
</tr>
<tr>
<td>Last Changed</td>
<td>The date and time of the most recent change to the SDP.</td>
</tr>
<tr>
<td>Signaling</td>
<td>Specifies the signaling protocol used to obtain the ingress and egress labels used in frames transmitted and received on this SDP.</td>
</tr>
<tr>
<td>Admin State</td>
<td>The administrative state of the keepalive process.</td>
</tr>
<tr>
<td>Oper State</td>
<td>The operational state of the keepalive process.</td>
</tr>
<tr>
<td>Hello Time</td>
<td>Specifies how often the SDP echo request messages are transmitted on this SDP.</td>
</tr>
<tr>
<td>Max Drop Count</td>
<td>Specifies the maximum number of consecutive SDP echo request messages that can be unacknowledged before the keepalive protocol reports a fault.</td>
</tr>
<tr>
<td>Hello Msg Len</td>
<td>Specifies the length of the SDP echo request messages transmitted on this SDP.</td>
</tr>
<tr>
<td>Hold Down Time</td>
<td>Specifies the amount of time to wait before the keepalive operating status is eligible to enter the alive state.</td>
</tr>
<tr>
<td>I. Fwd. Pkts.</td>
<td>Specifies the number of forwarded ingress packets.</td>
</tr>
<tr>
<td>I. Dro. Pkts.</td>
<td>Specifies the number of dropped ingress packets.</td>
</tr>
<tr>
<td>E. Fwd. Pkts.</td>
<td>Specifies the number of forwarded egress packets.</td>
</tr>
<tr>
<td>Associated LSP List</td>
<td>When the SDP type is MPLS, a list of LSPs used to reach the far-end router displays. All the LSPs in the list must terminate at the IP address specified in the far end field. If the SDP type is GRE, then the following message displays: SDP delivery mechanism is not MPLS.</td>
</tr>
</tbody>
</table>

Sample Output

A:Dut-A# show service id 1 sdp detail

Services: Service Destination Points Details

Sdp Id 1:1 - (10.20.1.2)

<table>
<thead>
<tr>
<th>Description</th>
<th>Default sdp description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SDP Id</td>
<td>1:1</td>
</tr>
<tr>
<td>VC Type</td>
<td>Ether</td>
</tr>
<tr>
<td>Admin Path MTU</td>
<td>0</td>
</tr>
<tr>
<td>Far End</td>
<td>10.20.1.2</td>
</tr>
<tr>
<td>Admin State</td>
<td>Up</td>
</tr>
<tr>
<td>Acct. Pol</td>
<td>None</td>
</tr>
<tr>
<td>Ingress Label</td>
<td>2048</td>
</tr>
<tr>
<td>Egress Label</td>
<td>2048</td>
</tr>
<tr>
<td>Egr mac Fltr</td>
<td>n/a</td>
</tr>
<tr>
<td>Egr ip Fltr</td>
<td>n/a</td>
</tr>
<tr>
<td>Egr ipv6 Fltr</td>
<td>n/a</td>
</tr>
<tr>
<td>Ing ip Fltr</td>
<td>n/a</td>
</tr>
<tr>
<td>Ing ipv6 Fltr</td>
<td>n/a</td>
</tr>
</tbody>
</table>
Admin ControlWord : Not Preferred  Oper ControlWord : False
Last Status Change : 05/31/2007 00:45:43  Signaling : None
Last Mgmt Change : 05/31/2007 00:45:43
Class Fwding State : Up
Flags : None
Peer Pw Bits : None
Peer Fault Ip : None
Peer Vccv CV Bits : None
Peer Vccv CC Bits : None
Max Nbr of MAC Addr: No Limit  Total MAC Addr : 0
Learned MAC Addr : 0  Static MAC Addr : 0
MAC Learning : Enabled  Discard Unkwn Srce: Disabled
MAC Aging : Enabled  BPDU Translation : Disabled
L2PT Termination : Disabled  
MAC Pinning : Disabled
KeepAlive Information :
Admin State : Disabled  Oper State : Disabled
Hello Time : 10  Hello Msg Len : 0
Max Drop Count : 3  Hold Down Time : 10
Statistics :
I. Fwd. Pkts. : 0  I. Dro. Pkts. : 0
I. Fwd. Octs. : 0  I. Dro. Octs. : 0
E. Fwd. Pkts. : 0  E. Fwd. Octets : 0
MCAC Policy Name :
MCAC Max Unconst BW: no limit  MCAC Max Mand BW : no limit
MCAC In use Mand BW: 0  MCAC Avail Mand BW: unlimited
MCAC In use Opnl BW: 0  MCAC Avail Opnl BW: unlimited
Associated LSP LIST :
Lsp Name : A_B_1
Admin State : Up  Oper State : Up
Time Since Last Tr*: 00h26m35s
Lsp Name : A_B_2
Admin State : Up  Oper State : Up
Time Since Last Tr*: 00h26m35s
Lsp Name : A_B_3
Admin State : Up  Oper State : Up
Time Since Last Tr*: 00h26m34s
Lsp Name : A_B_4
Admin State : Up  Oper State : Up
Time Since Last Tr*: 00h26m34s
Lsp Name : A_B_5
Admin State : Up  Oper State : Up
Time Since Last Tr*: 00h26m34s
Lsp Name : A_B_6
Admin State : Up  Oper State : Up
Time Since Last Tr*: 00h26m34s
Lsp Name : A_B_7
Admin State : Up  Oper State : Up
Time Since Last Tr*: 00h26m34s
Lsp Name : A_B_8
Admin State : Up  Oper State : Up
Time Since Last Tr*: 00h26m35s
Lsp Name       : A_B_9
Admin State    : Up                      Oper State      : Up
Time Since Last Tr*: 00h26m34s

Lsp Name       : A_B_10
Admin State    : Up                      Oper State      : Up
Time Since Last Tr*: 00h26m34s

Class-based forwarding :
-------------------------------------------------------------------------------
Class forwarding : enabled
Default LSP      : A_B_10                   Multicast LSP     : A_B_9
===============================================================================

FC Mapping Table
===============================================================================
FC Name             LSP Name
-------------------------------------------------------------------------------
af                  A_B_3
be                  A_B_1
ef                  A_B_6
h1                  A_B_7
h2                  A_B_5
l1                  A_B_4
l2                  A_B_2
nc                  A_B_8
===============================================================================

Stp Service Destination Point specifics
-------------------------------------------------------------------------------
Mac Move           : Blockable
Stp Admin State    : Up                      Stp Oper State    : Down
Core Connectivity  : Down                    Port State       : Forwarding
Port Role          : N/A                      Port Priority     : 128
Port Number        : 2049                     Port Path Cost    : 10
Auto Edge          : Enabled
Admin Edge         : Disabled                  Oper Edge        : N/A
Link Type          : Pt-pt                    BPDU Encap        : Dot1d
Root Guard         : Disabled                  Active Protocol   : N/A
Last BPDUs from    : N/A
Designated Bridge  : N/A                      Designated Port Id: 0
Fwd Transitions    : 0                        Bad BPDUs rcvd   : 0
Cfg BPDUs rcvd     : 0                        Cfg BPDUs tx     : 0
TCN BPDUs rcvd     : 0                        TCN BPDUs tx     : 0
RST BPDUs rcvd     : 0                        RST BPDUs tx     : 0
-------------------------------------------------------------------------------
Number of SDPs : 1
-------------------------------------------------------------------------------
* indicates that the corresponding row element may have been truncated.
-------------------------------------------------------------------------------
A:Dut-A#
Parameters

active — This keyword filters out inactive aggregates.

Output

Show Aggregate Output Fields — The following table describes router aggregate output fields.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prefix</td>
<td>Displays the destination address of the aggregate route in dotted decimal notation.</td>
</tr>
<tr>
<td>Summary</td>
<td>Specifies whether the aggregate or more specific components are advertised.</td>
</tr>
<tr>
<td>AS Set</td>
<td>Displays an aggregate where the path advertised for the route consists of all elements contained in all paths that are being summarized.</td>
</tr>
<tr>
<td>Aggr AS</td>
<td>Displays the aggregator path attribute to the aggregate route.</td>
</tr>
<tr>
<td>Aggr IP-Address</td>
<td>The IP address of the aggregated route.</td>
</tr>
<tr>
<td>State</td>
<td>The operational state of the aggregated route.</td>
</tr>
<tr>
<td>No. of Aggregates</td>
<td>The total number of aggregated routes.</td>
</tr>
</tbody>
</table>

Sample Output

*A:ALA-12# show router 3 aggregate

Aggregates (Service: 3)

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Summary</th>
<th>AS Set</th>
<th>Aggr AS</th>
<th>Aggr IP-Address</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.2.3.0/24</td>
<td>False</td>
<td></td>
<td>0</td>
<td>0.0.0.0</td>
<td>Indirect</td>
</tr>
<tr>
<td>2.2.2.2</td>
<td>False</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.2.0.0/16</td>
<td>False</td>
<td></td>
<td>0</td>
<td>0.0.0.0</td>
<td>Active</td>
</tr>
</tbody>
</table>

No. of Aggregates: 2

*A:CPM133>config>router# show router aggregate

*A:CPM133>config>router# show router aggregate
VPRN Show Commands

Aggregates (Router: Base)

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Aggr IP-Address</th>
<th>Aggr AS</th>
<th>AS Set</th>
<th>State</th>
<th>Community</th>
<th>NextHopType</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.0.0/8</td>
<td>0.0.0.0</td>
<td>0</td>
<td>False</td>
<td>Inactive</td>
<td>False</td>
<td>100:33 Blackhole</td>
</tr>
</tbody>
</table>

No. of Aggregates: 1

arp

Syntax    arp [ip-address | ip-int-name | mac ieee-mac-addr]

Context   show>router

Description This command displays the router ARP table sorted by IP address.

If no command line options are specified, all ARP entries are displayed.

Parameters

* ip-addr — Only displays ARP entries associated with the specified IP address.
* ip-int-name — Only displays ARP entries associated with the specified IP interface name.
* mac ieee-mac-addr — Only displays ARP entries associated with the specified MAC address.

Output ARP Table Output — The following table describes ARP table output fields:

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>The IP address of the ARP entry.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>The MAC address of the ARP entry.</td>
</tr>
<tr>
<td>Expiry</td>
<td>The age of the ARP entry.</td>
</tr>
<tr>
<td>Type</td>
<td>Dyn — The ARP entry is a dynamic ARP entry.</td>
</tr>
<tr>
<td></td>
<td>Inv — The ARP entry is an inactive static ARP entry (invalid).</td>
</tr>
<tr>
<td></td>
<td>Oth — The ARP entry is a local or system ARP entry.</td>
</tr>
<tr>
<td></td>
<td>Sta — The ARP entry is an active static ARP entry.</td>
</tr>
<tr>
<td>Interface</td>
<td>The IP interface name associated with the ARP entry.</td>
</tr>
<tr>
<td>No. of ARP Entries</td>
<td>The number of ARP entries displayed in the list.</td>
</tr>
</tbody>
</table>

Sample Output

*A:ALA-12# show router 3 arp

ARP Table (Service: 3)
### Show, Clear, Debug Commands

<table>
<thead>
<tr>
<th>IP Address</th>
<th>MAC Address</th>
<th>Expiry</th>
<th>Type</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.10.10.103</td>
<td>04:67:ff:00:00:01 00:00:00:00:00:00</td>
<td>00h00m00s</td>
<td>Oth</td>
<td>system</td>
</tr>
<tr>
<td>10.10.4.3</td>
<td>00:00:00:00:00:00</td>
<td>00h00m00s</td>
<td>Oth</td>
<td>ALA-1-2</td>
</tr>
<tr>
<td>10.10.5.3</td>
<td>00:00:00:00:00:00</td>
<td>00h00m00s</td>
<td>Oth</td>
<td>ALA-1-3</td>
</tr>
<tr>
<td>10.10.7.3</td>
<td>00:00:00:00:00:00</td>
<td>00h00m00s</td>
<td>Oth</td>
<td>ALA-1-5</td>
</tr>
<tr>
<td>10.10.0.16</td>
<td>00:00:00:00:00:00</td>
<td>00h00m00s</td>
<td>Oth</td>
<td>bozo</td>
</tr>
<tr>
<td>10.10.3.3</td>
<td>00:00:00:00:00:00</td>
<td>00h00m00s</td>
<td>Oth</td>
<td>gizmo</td>
</tr>
<tr>
<td>10.10.2.3</td>
<td>00:00:00:00:00:00</td>
<td>00h00m00s</td>
<td>Oth</td>
<td>hobo</td>
</tr>
<tr>
<td>10.10.1.17</td>
<td>00:00:00:00:00:00</td>
<td>00h00m00s</td>
<td>Oth</td>
<td>int-cflowd</td>
</tr>
<tr>
<td>10.0.0.92</td>
<td>00:00:00:00:00:00</td>
<td>04h00m00s</td>
<td>Dyn</td>
<td>to-104</td>
</tr>
<tr>
<td>10.0.0.103</td>
<td>04:67:01:01:00:01</td>
<td>00h00m00s</td>
<td>Oth</td>
<td>to-104</td>
</tr>
<tr>
<td>10.0.0.104</td>
<td>04:68:01:01:00:01</td>
<td>03h59m49s</td>
<td>Dyn[I]</td>
<td>to-104</td>
</tr>
<tr>
<td>10.10.36.2</td>
<td>00:00:00:00:00:00</td>
<td>00h00m00s</td>
<td>Oth</td>
<td>tuesday</td>
</tr>
<tr>
<td>192.168.2.98</td>
<td>00:03:47:c8:b4:86 00h14m37s</td>
<td>00h14m37s</td>
<td>Dyn[I]</td>
<td>management</td>
</tr>
<tr>
<td>192.168.2.103</td>
<td>00:03:47:d0:c9:8b</td>
<td>00h00m00s</td>
<td>Oth</td>
<td>management</td>
</tr>
</tbody>
</table>

**No. of ARP Entries: 14**

*A:ALA-12#

*A:ALA-12# show router 3 arp 10.10.0.3

**ARP Table**

<table>
<thead>
<tr>
<th>IP Address</th>
<th>MAC Address</th>
<th>Expiry</th>
<th>Type</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.10.0.3</td>
<td>04:5d:ff:00:00:00</td>
<td>00h00m00s</td>
<td>Oth</td>
<td>system</td>
</tr>
</tbody>
</table>

*A:ALA-12#

*A:ALA-12# show router 3 arp to-ser1

**ARP Table**

<table>
<thead>
<tr>
<th>IP Address</th>
<th>MAC Address</th>
<th>Expiry</th>
<th>Type</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.10.13.1</td>
<td>04:5b:01:01:00:02 03:53:09</td>
<td>03:53:09</td>
<td>Dyn</td>
<td>to-ser1</td>
</tr>
</tbody>
</table>

*A:ALA-12#
**Syntax**

```
damping [ip-prefix/mask | ip-address] [detail]
damping [damp-type] [detail]
```

**Context**

`show>router>bgp`

**Description**

This command displays BGP routes with have been dampened due to route flapping. This command can be entered with or without a route parameter.

When the keyword `detail` is included, more detailed information displays.

When only the command is entered (without any parameters included except `detail`), then all dampened routes are listed.

When a parameter is specified, then the matching route or routes are listed.

When a `decayed`, `history`, or `suppressed` keyword is specified, only those types of dampened routes are listed.

**Parameters**

- `ip-prefix/mask` — Displays damping information for the specified IP prefix and mask length.
- `ip-address` — Displays damping entry for the best match route for the specified IP address.
- `damp-type` — Displays damping type for the specified IP address.
- `decayed` — Displays damping entries that are decayed but are not suppressed.
- `history` — Displays damping entries that are withdrawn but have history.
- `suppressed` — Displays damping entries suppressed because of route damping.
- `detail` — Displays detailed information.

**Output**

**Show Damping Output Fields** — The following table describes BGP damping output fields:

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP Router ID</td>
<td>The local BGP router ID.</td>
</tr>
<tr>
<td>AS</td>
<td>The configured autonomous system number.</td>
</tr>
<tr>
<td>Local AS</td>
<td>The configured or inherited local AS for the specified peer group. If not configured, then it is the same value as the AS.</td>
</tr>
<tr>
<td>Network</td>
<td>Route IP prefix and mask length for the route.</td>
</tr>
<tr>
<td>Flag(s)</td>
<td>Legend:</td>
</tr>
<tr>
<td></td>
<td>Status codes: u- used, s-suppressed, h-history, d-decayed, *-valid. If a * is not present, then the status is invalid.</td>
</tr>
<tr>
<td></td>
<td>Origin codes: i-IGP, e-EGP, ?-incomplete, &gt;-best</td>
</tr>
<tr>
<td>Network</td>
<td>The IP prefix and mask length for the route.</td>
</tr>
<tr>
<td>From</td>
<td>The originator ID path attribute value.</td>
</tr>
<tr>
<td>Reuse time</td>
<td>The time when a suppressed route can be used again.</td>
</tr>
<tr>
<td>AS Path</td>
<td>The BGP AS path for the route.</td>
</tr>
</tbody>
</table>
### Sample Output

*A:ALA-12# show router 3 bgp damping*

<table>
<thead>
<tr>
<th>Flag</th>
<th>Network</th>
<th>From</th>
<th>Reuse</th>
<th>AS-Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>ud*i</td>
<td>12.149.7.0/24</td>
<td>10.0.28.1</td>
<td>00h00m00s</td>
<td>60203 65001 19855 3356</td>
</tr>
<tr>
<td>si</td>
<td>24.155.6.0/23</td>
<td>10.0.28.1</td>
<td>00h43m41s</td>
<td>60203 65001 19855 3356</td>
</tr>
<tr>
<td>si</td>
<td>24.155.8.0/22</td>
<td>10.0.28.1</td>
<td>00h38m31s</td>
<td>60203 65001 19855 3356</td>
</tr>
<tr>
<td>si</td>
<td>24.155.12.0/22</td>
<td>10.0.28.1</td>
<td>00h35m41s</td>
<td>60203 65001 19855 3356</td>
</tr>
<tr>
<td>si</td>
<td>24.155.22.0/23</td>
<td>10.0.28.1</td>
<td>00h35m41s</td>
<td>60203 65001 19855 3356</td>
</tr>
<tr>
<td>si</td>
<td>24.155.24.0/22</td>
<td>10.0.28.1</td>
<td>00h35m41s</td>
<td>60203 65001 19855 3356</td>
</tr>
<tr>
<td>si</td>
<td>24.155.28.0/22</td>
<td>10.0.28.1</td>
<td>00h34m31s</td>
<td>60203 65001 19855 3356</td>
</tr>
<tr>
<td>si</td>
<td>24.155.40.0/21</td>
<td>10.0.28.1</td>
<td>00h28m24s</td>
<td>60203 65001 19855 3356</td>
</tr>
<tr>
<td>si</td>
<td>24.155.48.0/20</td>
<td>10.0.28.1</td>
<td>00h28m24s</td>
<td>60203 65001 19855 3356</td>
</tr>
<tr>
<td>ud*i</td>
<td>61.8.140.0/24</td>
<td>10.0.28.1</td>
<td>00h00m00s</td>
<td>60203 65001 19855 3356</td>
</tr>
</tbody>
</table>

#### Label and Description

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peer</td>
<td>The router ID of the advertising router.</td>
</tr>
<tr>
<td>NextHop</td>
<td>BGP nexthop for the route.</td>
</tr>
<tr>
<td>Peer AS</td>
<td>The autonomous system number of the advertising router.</td>
</tr>
<tr>
<td>Peer Router-Id</td>
<td>The router ID of the advertising router.</td>
</tr>
<tr>
<td>Local Pref</td>
<td>BGP local preference path attribute for the route.</td>
</tr>
<tr>
<td>Age</td>
<td>The time elapsed since the service was enabled.</td>
</tr>
<tr>
<td>Last update</td>
<td>The time when BGP was updated last in second/minute/hour (SS:MM:HH) format.</td>
</tr>
<tr>
<td>FOM Present</td>
<td>The current Figure of Merit (FOM) value.</td>
</tr>
<tr>
<td>Number of Flaps</td>
<td>The number of flaps in the neighbor connection.</td>
</tr>
<tr>
<td>Reuse time</td>
<td>The time when the route can be reused.</td>
</tr>
<tr>
<td>Path</td>
<td>The BGP AS path for the route.</td>
</tr>
<tr>
<td>Applied Policy</td>
<td>The applied route policy name.</td>
</tr>
</tbody>
</table>
### BGP Damped Routes

<table>
<thead>
<tr>
<th>Network</th>
<th>Peer</th>
<th>NextHop</th>
<th>Reuse time</th>
<th>Peer AS</th>
<th>Peer Router-Id</th>
<th>Local Pref</th>
<th>Age</th>
<th>FOM Present</th>
<th>Number of Flaps</th>
<th>Flags</th>
<th>Path</th>
<th>Applied Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.149.7.0/24</td>
<td>10.0.28.1</td>
<td>10.0.28.1</td>
<td>00h00m00s</td>
<td>60203</td>
<td>32.32.27.203</td>
<td>none</td>
<td>00h22m09s</td>
<td>738</td>
<td>2</td>
<td>ud*i</td>
<td>60203 65001 19855 3356 1239 22406</td>
<td>default-damping-profile</td>
</tr>
<tr>
<td>15.142.48.0/20</td>
<td>10.0.28.1</td>
<td>10.0.28.1</td>
<td>00h00m00s</td>
<td>60203</td>
<td>32.32.27.203</td>
<td>none</td>
<td>00h00m38s</td>
<td>738</td>
<td>2</td>
<td>ud*i</td>
<td>60203 65001 19855 3356 3561 5551 1889</td>
<td>default-damping-profile</td>
</tr>
<tr>
<td>15.200.128.0/19</td>
<td>10.0.28.1</td>
<td>10.0.28.1</td>
<td>00h00m00s</td>
<td>60203</td>
<td>32.32.27.203</td>
<td>none</td>
<td>00h00m38s</td>
<td>738</td>
<td>2</td>
<td>ud*i</td>
<td>60203 65001 19855 3356 702 1889</td>
<td>default-damping-profile</td>
</tr>
<tr>
<td>15.203.192.0/18</td>
<td>10.0.28.1</td>
<td>10.0.28.1</td>
<td>00h00m00s</td>
<td>60203</td>
<td>32.32.27.203</td>
<td>none</td>
<td>00h00m38s</td>
<td>738</td>
<td>2</td>
<td>ud*i</td>
<td>60203 65001 19855 3356 702 1889</td>
<td>default-damping-profile</td>
</tr>
</tbody>
</table>
NextHop          : 10.0.28.1            Reuse time       : 00h00m00s
Peer AS          : 60203                Peer Router-Id   : 32.32.27.203
Local Pref       : none
Age              : 00h00m07s            Last update      : 02d01h20m
FOM Present      : 1018                 FOM Last upd.    : 1024
Number of Flaps  : 1                    Flags            : ud*i
Path             : 60203 65001 19855 1299  702   1889
Applied Policy   : default-damping-profile
------------------------------------------------------------------------------
*A:ALA-12#

*A:ALA-12# show router 3 bgp damping 15.203.192.0/18 detail
------------------------------------------------------------------------------
BGP Damped Routes 15.203.192.0/18
------------------------------------------------------------------------------
Network          : 15.203.192.0/18      Peer             : 10.0.28.1
NextHop          : 10.0.28.1            Reuse time       : 00h00m00s
Peer AS          : 60203                Peer Router-Id   : 32.32.27.203
Local Pref       : none
Age              : 00h00m42s            Last update      : 02d01h20m
FOM Present      : 2003                 FOM Last upd.    : 2025
Number of Flaps  : 2                    Flags            : ud*i
Path             : 60203 65001 19855 3356  702   1889
Applied Policy   : default-damping-profile
------------------------------------------------------------------------------
Paths : 1

*A:ALA-12# show router 3 bgp damping suppressed detail
------------------------------------------------------------------------------
BGP Damped Routes (Suppressed)
------------------------------------------------------------------------------
Network          : 15.142.48.0/20
------------------------------------------------------------------------------
Network          : 15.200.128.0/19
------------------------------------------------------------------------------
Network          : 15.200.128.0/19
------------------------------------------------------------------------------
Peer AS : 60203 Peer Router-Id : 32.32.27.203
Local Pref : none
Age : 00h01m28s Last update : 02d01h20m
FOM Present : 2936 FOM Last upd. : 3001
Number of Flaps : 3 Flags : si
Path : 60203 65001 19855 3356 702 1889
Applied Policy : default-damping-profile

--------------------------------
Network : 15.203.240.0/20
--------------------------------
Network : 15.203.240.0/20 Peer : 10.0.28.1
NextHop : 10.0.28.1 Reuse time : 00h29m22s
Peer AS : 60203 Peer Router-Id : 32.32.27.203
Local Pref : none
Age : 00h01m28s Last update : 02d01h20m
FOM Present : 2936 FOM Last upd. : 3001
Number of Flaps : 3 Flags : si
Path : 60203 65001 19855 3356 702 1889
Applied Policy : default-damping-profile

--------------------------------
Network : 15.206.0.0/17
--------------------------------
Network : 15.206.0.0/17 Peer : 10.0.28.1
NextHop : 10.0.28.1 Reuse time : 00h29m22s
Peer AS : 60203 Peer Router-Id : 32.32.27.203
Local Pref : none
Age : 00h01m28s Last update : 02d01h20m
FOM Present : 2936 FOM Last upd. : 3001
Number of Flaps : 3 Flags : si
Path : 60203 65001 19855 3356 702 1889
Applied Policy : default-damping-profile

*A:ALA-12#
Show, Clear, Debug Commands

**group**

**Syntax**  
`group [name] [detail]`

**Context**  
`show>router>bgp`

**Description**  
This command displays group information for a BGP peer group. This command can be entered with or without parameters.

When this command is entered without a group name, information about all peer groups displays.

When the command is issued with a specific group name, information only pertaining to that specific peer group displays.

The ‘State’ field displays the BGP group’s operational state. Other valid states are:

- **Up** - BGP global process is configured and running.
- **Down** - BGP global process is administratively shutdown and not running.
- **Disabled** - BGP global process is operationally disabled. The process must be restarted by the operator.

**Parameters**

- **name** — Displays information for the BGP group specified.
- **detail** — Displays detailed information.

**Output**

**Standard and Detailed Group Output** — The following table describes the standard and detailed command output fields for a BGP group:

**Sample Output**

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Group</strong></td>
<td>BGP group name</td>
</tr>
<tr>
<td><strong>Group Type</strong></td>
<td><strong>No Type</strong> — Peer type not configured.</td>
</tr>
<tr>
<td></td>
<td><strong>External</strong> — Peer type configured as external BGP peers.</td>
</tr>
<tr>
<td></td>
<td><strong>Internal</strong> — Peer type configured as internal BGP peers.</td>
</tr>
<tr>
<td><strong>State</strong></td>
<td><strong>Disabled</strong> — The BGP peer group has been operationally disabled.</td>
</tr>
<tr>
<td></td>
<td><strong>Down</strong> — The BGP peer group is operationally inactive.</td>
</tr>
<tr>
<td></td>
<td><strong>Up</strong> — The BGP peer group is operationally active.</td>
</tr>
<tr>
<td><strong>Peer AS</strong></td>
<td>The configured or inherited peer AS for the specified peer group.</td>
</tr>
<tr>
<td><strong>Local AS</strong></td>
<td>The configured or inherited local AS for the specified peer group.</td>
</tr>
<tr>
<td><strong>Local Address</strong></td>
<td>The configured or inherited local address for originating peering for the specified peer group.</td>
</tr>
<tr>
<td><strong>Loop Detect</strong></td>
<td>The configured or inherited loop detect setting for the specified peer group.</td>
</tr>
<tr>
<td><strong>Connect Retry</strong></td>
<td>The configured or inherited connect retry timer value.</td>
</tr>
<tr>
<td><strong>Authentication</strong></td>
<td></td>
</tr>
<tr>
<td>Label</td>
<td>Description (Continued)</td>
</tr>
<tr>
<td>-----------------------</td>
<td>----------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>None</td>
<td>No authentication is configured.</td>
</tr>
<tr>
<td>MD5</td>
<td>MD5 authentication is configured.</td>
</tr>
<tr>
<td>Local Pref</td>
<td>The configured or inherited local preference value.</td>
</tr>
<tr>
<td>MED Out</td>
<td>The configured or inherited MED value assigned to advertised routes without a MED attribute.</td>
</tr>
<tr>
<td>Min Route Advt.</td>
<td>The minimum amount of time that must pass between route updates for the same IP prefix.</td>
</tr>
<tr>
<td>Min AS Originate</td>
<td>The minimum amount of time that must pass between updates for a route originated by the local router.</td>
</tr>
<tr>
<td>Multihop</td>
<td>The maximum number of router hops a BGP connection can traverse.</td>
</tr>
<tr>
<td>Multipath</td>
<td>The configured or inherited multipath value, determining the maximum number of ECMP routes BGP can advertise to the RTM.</td>
</tr>
<tr>
<td>Prefix Limit</td>
<td>No Limit — No route limit assigned to the BGP peer group.</td>
</tr>
<tr>
<td></td>
<td>1 - 4294967295 — The maximum number of routes BGP can learn from a peer.</td>
</tr>
<tr>
<td>Passive</td>
<td>Disabled — BGP attempts to establish BGP connections with neighbors in the specified peer group.</td>
</tr>
<tr>
<td></td>
<td>Enabled — BGP will not actively attempt to establish BGP connections with neighbors in the specified peer group.</td>
</tr>
<tr>
<td>Next Hop Self</td>
<td>Disabled — BGP is not configured to send only its own IP address as the BGP nexthop in route updates to neighbors in the peer group.</td>
</tr>
<tr>
<td></td>
<td>Enabled — BGP sends only its own IP address as the BGP nexthop in route updates to neighbors in the specified peer group.</td>
</tr>
<tr>
<td>Aggregator ID 0</td>
<td>Disabled — BGP is not configured to set the aggregator ID to 0.0.0.0 in all originated route aggregates sent to the neighbor in the peer group.</td>
</tr>
<tr>
<td></td>
<td>Enabled — BGP is configured to set the aggregator ID to 0.0.0.0 in all originated route aggregates sent to the neighbor in the peer group.</td>
</tr>
<tr>
<td>Remove Private</td>
<td>Disabled — BGP will not remove all private AS numbers from the AS path attribute in updates sent to the neighbor in the peer group.</td>
</tr>
<tr>
<td></td>
<td>Enabled — BGP removes all private AS numbers from the AS path attribute in updates sent to the neighbor in the peer group.</td>
</tr>
<tr>
<td>Damping</td>
<td>Disabled — The peer group is configured not to dampen route flaps.</td>
</tr>
<tr>
<td></td>
<td>Enabled — The peer group is configured to dampen route flaps.</td>
</tr>
<tr>
<td>Export Policy</td>
<td>The configured export policies for the peer group.</td>
</tr>
</tbody>
</table>
### BGP Groups

<table>
<thead>
<tr>
<th>Label</th>
<th>Description (Continued)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Import Policy</td>
<td>The configured import policies for the peer group.</td>
</tr>
<tr>
<td>Hold Time</td>
<td>The configured hold time setting.</td>
</tr>
<tr>
<td>Keep Alive</td>
<td>The configured keepalive setting.</td>
</tr>
<tr>
<td>Cluster Id</td>
<td>None — No cluster ID has been configured.</td>
</tr>
<tr>
<td>Client Reflect</td>
<td>Disabled — The BGP route reflector will not reflect routes to this neighbor.</td>
</tr>
<tr>
<td></td>
<td>Enabled — The BGP route reflector is configured to reflect routes to this neighbor.</td>
</tr>
<tr>
<td>NLRI</td>
<td>The type of NLRI information that the specified peer group can accept.</td>
</tr>
<tr>
<td>Preference</td>
<td>The configured route preference value for the peer group.</td>
</tr>
<tr>
<td>List of Peers</td>
<td>A list of BGP peers configured under the peer group.</td>
</tr>
<tr>
<td>Total Peers</td>
<td>The total number of peers configured under the peer group.</td>
</tr>
<tr>
<td>Established</td>
<td>The total number of peers that are in an established state.</td>
</tr>
</tbody>
</table>

*A:ALA-12# `show router 3 bgp group`

<table>
<thead>
<tr>
<th>Group</th>
<th>To_AS_40000</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Not Available</td>
</tr>
<tr>
<td>Group Type</td>
<td>No Type</td>
</tr>
<tr>
<td>Peer AS</td>
<td>40000</td>
</tr>
<tr>
<td>Local Address</td>
<td>n/a</td>
</tr>
<tr>
<td>Export Policy</td>
<td>direct2bgp</td>
</tr>
<tr>
<td>Hold Time</td>
<td>90</td>
</tr>
<tr>
<td>Cluster Id</td>
<td>None</td>
</tr>
<tr>
<td>NLRI</td>
<td>Unicast</td>
</tr>
<tr>
<td>Preference</td>
<td>Unicast</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>List of Peers</th>
<th>Established</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.0.1</td>
<td>To_Jukebox</td>
</tr>
<tr>
<td>10.0.0.12</td>
<td>Not Available</td>
</tr>
<tr>
<td>10.0.0.13</td>
<td>Not Available</td>
</tr>
<tr>
<td>10.0.0.14</td>
<td>To_ALA-1</td>
</tr>
<tr>
<td>10.0.0.15</td>
<td>To_H-215</td>
</tr>
<tr>
<td>Total Peers</td>
<td>5</td>
</tr>
<tr>
<td>Established</td>
<td>2</td>
</tr>
</tbody>
</table>

*A:ALA-12#

**neighbor**

**Syntax**

```
neighbor [ip-address [[family family] filter1]]
```
neighbor \[as-number \[\[family family \] filter2]\]

**Context**
show>router>bgp

**Description**
This command displays BGP neighbor information. This command can be entered with or without any parameters.

When this command is issued without any parameters, information about all BGP peers displays.

When the command is issued with a specific IP address or ASN, information regarding only that specific peer or peers with the same AS display.

When either received-routes or advertised-routes is specified, then the routes received from or sent to the specified peer is listed (see second output example).

Note: This information is not available by SNMP.

When either history or suppressed is specified, then the routes learned from those peers that either have a history or are suppressed (respectively) are listed.

The ‘State’ field displays the BGP peer’s protocol state. In addition to the standard protocol states, this field can also display the ‘Disabled’ operational state which indicates the peer is operationally disabled and must be restarted by the operator.

**Parameters**

- **ip-addr** — Displays the BGP neighbor with the specified IP address.

- **family family** — Specifies the type of routing information to be distributed by the BGP instance.
  
  **Values**
  ipv4, vpn-ipv4

- **filter1** — Specifies route criteria.
  
  **Values**
  received-routes, advertised-routes, history, suppressed, detail

- **filter2** — Specifies route criteria.
  
  **Values**
  history, suppressed, detail

**Output**

**Standard and Detailed Neighbor** — The following table describes the standard and detailed command output fields for a BGP neighbor:

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peer</td>
<td>The IP address of the configured BGP peer.</td>
</tr>
<tr>
<td>Group</td>
<td>The BGP peer group to which this peer is assigned.</td>
</tr>
<tr>
<td>Peer AS</td>
<td>The configured or inherited peer AS for the peer group.</td>
</tr>
<tr>
<td>Peer Address</td>
<td>The configured address for the BGP peer.</td>
</tr>
<tr>
<td>Peer Port</td>
<td>The TCP port number used on the far-end system.</td>
</tr>
<tr>
<td>Local AS</td>
<td>The configured or inherited local AS for the peer group.</td>
</tr>
<tr>
<td>Local Address</td>
<td>The configured or inherited local address for originating peering for the peer group.</td>
</tr>
<tr>
<td>Local Port</td>
<td>The TCP port number used on the local system.</td>
</tr>
<tr>
<td>Peer Type</td>
<td><strong>External</strong> — Peer type configured as external BGP peers.</td>
</tr>
<tr>
<td>Label</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>---------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>State</strong></td>
<td></td>
</tr>
<tr>
<td>Internal</td>
<td>Peer type configured as internal BGP peers.</td>
</tr>
<tr>
<td>Idle</td>
<td>The BGP peer is not accepting connections.</td>
</tr>
<tr>
<td>Active</td>
<td>BGP is listening for and accepting TCP connections from this peer.</td>
</tr>
<tr>
<td>Connect</td>
<td>BGP is attempting to establish a TCP connection from this peer.</td>
</tr>
<tr>
<td>Open Sent</td>
<td>BGP has sent an OPEN message to the peer and is waiting for an OPEN message from the peer.</td>
</tr>
<tr>
<td>Open Confirm</td>
<td>BGP has received a valid OPEN message from the peer and is awaiting a KEEPALIVE or NOTIFICATION.</td>
</tr>
<tr>
<td>Established</td>
<td>BGP has successfully established a peering and is exchanging routing information.</td>
</tr>
<tr>
<td><strong>Last State</strong></td>
<td></td>
</tr>
<tr>
<td>Idle</td>
<td>The BGP peer is not accepting connections.</td>
</tr>
<tr>
<td>Active</td>
<td>BGP is listening for and accepting TCP connections from this peer.</td>
</tr>
<tr>
<td>Connect</td>
<td>BGP is attempting to establish a TCP connection with this peer.</td>
</tr>
<tr>
<td>Connect</td>
<td>BGP is attempting to establish a TCP connections from this peer.</td>
</tr>
<tr>
<td>Open Sent</td>
<td>BGP has sent an OPEN message to the peer and is waiting for an OPEN message from the peer.</td>
</tr>
<tr>
<td>Open Confirm</td>
<td>BGP has received a valid OPEN message from the peer and is awaiting a KEEPALIVE or NOTIFICATION.</td>
</tr>
<tr>
<td>Open Confirm</td>
<td>BGP has received a valid OPEN message from the peer and is awaiting a KEEPALIVE or NOTIFICATION.</td>
</tr>
<tr>
<td><strong>Last Event</strong></td>
<td></td>
</tr>
<tr>
<td>start</td>
<td>BGP has initialized the BGP neighbor.</td>
</tr>
<tr>
<td>stop</td>
<td>BGP has disabled the BGP neighbor.</td>
</tr>
<tr>
<td>open</td>
<td>BGP transport connection opened.</td>
</tr>
<tr>
<td>close</td>
<td>BGP transport connection closed.</td>
</tr>
<tr>
<td>openFail</td>
<td>BGP transport connection failed to open.</td>
</tr>
<tr>
<td>error</td>
<td>BGP transport connection error.</td>
</tr>
<tr>
<td>connectRetry</td>
<td>Connect retry timer expired.</td>
</tr>
<tr>
<td>holdTime</td>
<td>Hold time timer expired.</td>
</tr>
<tr>
<td>keepAlive</td>
<td>Keepalive timer expired.</td>
</tr>
<tr>
<td>Label</td>
<td>Description (Continued)</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>recvOpen</td>
<td>Receive an OPEN message.</td>
</tr>
<tr>
<td>revKeepalive</td>
<td>Receive an KEEPALIVE message.</td>
</tr>
<tr>
<td>recvUpdate</td>
<td>Receive an UPDATE message.</td>
</tr>
<tr>
<td>recvNotify</td>
<td>Receive an NOTIFICATION message.</td>
</tr>
<tr>
<td>None</td>
<td>No events have occurred.</td>
</tr>
<tr>
<td>Last Error</td>
<td>Displays the last BGP error and sub-code to occur on the BGP neighbor.</td>
</tr>
<tr>
<td>Connect Retry</td>
<td>The configured or inherited connect retry timer value.</td>
</tr>
<tr>
<td>Local Pref.</td>
<td>The configured or inherited local preference value.</td>
</tr>
<tr>
<td>Min Route Advt.</td>
<td>The minimum amount of time that must pass between route updates for the same IP prefix.</td>
</tr>
<tr>
<td>Min AS Originate</td>
<td>The minimum amount of time that must pass between updates for a route originated by the local router.</td>
</tr>
<tr>
<td>Multihop</td>
<td>The maximum number of router hops a BGP connection can traverse.</td>
</tr>
<tr>
<td>Multipath</td>
<td>The configured or inherited multipath value, determining the maximum number of ECMP routes BGP can advertise to the RTM.</td>
</tr>
<tr>
<td>Damping</td>
<td>Disabled — BGP neighbor is configured not to dampen route flaps.</td>
</tr>
<tr>
<td></td>
<td>Enabled — BGP neighbor is configured to dampen route flaps.</td>
</tr>
<tr>
<td>Loop Detect</td>
<td>Ignore — The BGP neighbor is configured to ignore routes with an AS loop.</td>
</tr>
<tr>
<td></td>
<td>Drop — The BGP neighbor is configured to drop the BGP peering if an AS loop is detected.</td>
</tr>
<tr>
<td></td>
<td>Off — AS loop detection is disabled for the neighbor.</td>
</tr>
<tr>
<td>MED Out</td>
<td>The configured or inherited MED value assigned to advertised routes without a MED attribute.</td>
</tr>
<tr>
<td>Authentication</td>
<td>None — No authentication is configured.</td>
</tr>
<tr>
<td></td>
<td>MD5 — MD5 authentication is configured.</td>
</tr>
<tr>
<td>Next Hop Self</td>
<td>Disabled — BGP is not configured to send only its own IP address as the BGP nexthop in route updates to the specified neighbor.</td>
</tr>
<tr>
<td></td>
<td>Enabled — BGP will send only its own IP address as the BGP next-hop in route updates to the neighbor.</td>
</tr>
<tr>
<td>AggregatorID Zero</td>
<td>Disabled — The BGP Neighbor is not configured to set the aggregator ID to 0.0.0.0 in all originated route aggregates.</td>
</tr>
<tr>
<td>Label</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Remove Private       | Disabled — BGP will not remove all private AS numbers from the AS path attribute, in updates sent to the specified neighbor.  
|                      | Enabled — BGP will remove all private AS numbers from the AS path attribute, in updates sent to the specified neighbor. |
| Passive              | Disabled — BGP will actively attempt to establish a BGP connection with the specified neighbor.  
|                      | Enabled — BGP will not actively attempt to establish a BGP connection with the specified neighbor. |
| Prefix Limit         | No Limit — No route limit assigned to the BGP peer group.  
|                      | 1 - 4294967295 — The maximum number of routes BGP can learn from a peer. |
| Hold Time            | The configured hold time setting.                                           |
| Keep Alive           | The configured keepalive setting.                                           |
| Active Hold Time     | The negotiated hold time, if the BGP neighbor is in an established state.   |
| Active Keep Alive    | The negotiated keepalive time, if the BGP neighbor is in an established state. |
| Cluster Id           | The configured route reflector cluster ID.                                  
|                      | None — No cluster ID has been configured                                    |
| Client Reflect       | Disabled — The BGP route reflector is configured not to reflect routes to this neighbor.  
|                      | Enabled — The BGP route reflector is configured to reflect routes to this neighbor. |
| Preference           | The configured route preference value for the peer group.                   |
| Num of Flaps         | The number of flaps in the neighbor connection.                             |
| Recd. Prefixes       | The number of routes received from the BGP neighbor.                        |
| Active Prefixes      | The number of routes received from the BGP neighbor and active in the forwarding table. |
| Recd. Paths          | The number of unique sets of path attributes received from the BGP neighbor. |
| Suppressed Paths     | The number of unique sets of path attributes received from the BGP neighbor and suppressed due to route damping. |
| Input Queue          | The number of BGP messages to be processed.                                  |
| Output Queue         | The number of BGP messages to be transmitted.                               |
Sample Output

*A:ALA-12# show router 3 bgp neighbor
detail

<table>
<thead>
<tr>
<th>Label</th>
<th>Description (Continued)</th>
</tr>
</thead>
<tbody>
<tr>
<td>i/p Messages</td>
<td>Total number of packets received from the BGP neighbor.</td>
</tr>
<tr>
<td>o/p Messages</td>
<td>Total number of packets sent to the BGP neighbor.</td>
</tr>
<tr>
<td>i/p Octets</td>
<td>Total number of octets received from the BGP neighbor.</td>
</tr>
<tr>
<td>o/p Octets</td>
<td>Total number of octets sent to the BGP neighbor.</td>
</tr>
<tr>
<td>i/p Updates</td>
<td>Total number of BGP updates received from the BGP neighbor.</td>
</tr>
<tr>
<td>o/p Updates</td>
<td>Total number of BGP updates sent to the BGP neighbor.</td>
</tr>
<tr>
<td>Export Policy</td>
<td>The configured export policies for the peer group.</td>
</tr>
<tr>
<td>Import Policy</td>
<td>The configured import policies for the peer group.</td>
</tr>
</tbody>
</table>
Peer Type : External
State : Active
Last Event : openFail
Last Error : Hold Timer Expire
Connect Retry : 20
Min Route Advrt. : 30
Min Route Advt. : 30
Multipath : 1
Loop Detect : Ignore
MED Out : No MED Out
Next Hop Self : Disabled
Damping : Disabled
MED Out : No MED Out
Next Hop Self : Disabled
Remove Private : Disabled
Prefix Limit : No Limit
Hold Time : 90
Keep Alive : 30
Active Hold Time : 0
Active Keep Alive : 0
Cluster Id : None
Client Reflect : Enabled
Preference : 170
Num of Flaps : 0
Recd. Prefixes : 0
Active Prefixes : 0
Recd. Paths : 0
Suppressed Paths : 0
Input Queue : 0
Output Queue : 0
i/p Messages : 0
o/p Messages : 0
i/p Octets : 0
o/p Octets : 0
i/p Updates : 0
o/p Updates : 0
Export Policy : direct2bgp

*A:ALA-12#

Output

Show Advertised and Received Routes Output — The following table describes the command output fields for both the standard and detailed information for a neighbor:

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP Router ID</td>
<td>The local BGP router ID.</td>
</tr>
<tr>
<td>AS</td>
<td>The configured autonomous system number.</td>
</tr>
<tr>
<td>Local AS</td>
<td>The configured local AS setting. If not configured, then it is the same value as the AS.</td>
</tr>
<tr>
<td>Flag</td>
<td>u - used</td>
</tr>
<tr>
<td></td>
<td>s - suppressed</td>
</tr>
<tr>
<td></td>
<td>h - history</td>
</tr>
<tr>
<td></td>
<td>d - decayed</td>
</tr>
<tr>
<td></td>
<td>* - valid</td>
</tr>
<tr>
<td></td>
<td>i - igp</td>
</tr>
<tr>
<td></td>
<td>? - incomplete</td>
</tr>
<tr>
<td></td>
<td>&gt; - best</td>
</tr>
<tr>
<td>Network</td>
<td>Route IP prefix and mask length for the route.</td>
</tr>
<tr>
<td>Next Hop</td>
<td>BGP nexthop for the route.</td>
</tr>
</tbody>
</table>
Sample Output

*A:ALA-12# show router 3 bgp neighbor 10.0.0.16 received-routes

BGP Router ID : 10.0.0.16         AS : 65206   Local AS : 65206

Legend -
Status codes : u - used, s - suppressed, h - history, d - decayed, * - valid
Origin codes : i - IGP, e - EGP, ? - incomplete, > - best

BGP Neighbor

<table>
<thead>
<tr>
<th>Flag</th>
<th>Network</th>
<th>Nexthop</th>
<th>LocalPref</th>
<th>MED</th>
<th>As-Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>?</td>
<td>10.0.0.16/32</td>
<td>10.0.0.16</td>
<td>100</td>
<td>none</td>
<td>No As-Path</td>
</tr>
<tr>
<td>?</td>
<td>10.0.6.0/24</td>
<td>10.0.0.16</td>
<td>100</td>
<td>none</td>
<td>No As-Path</td>
</tr>
<tr>
<td>?</td>
<td>10.0.8.0/24</td>
<td>10.0.0.16</td>
<td>100</td>
<td>none</td>
<td>No As-Path</td>
</tr>
<tr>
<td>?</td>
<td>10.0.12.0/24</td>
<td>10.0.0.16</td>
<td>100</td>
<td>none</td>
<td>No As-Path</td>
</tr>
<tr>
<td>?</td>
<td>10.0.13.0/24</td>
<td>10.0.0.16</td>
<td>100</td>
<td>none</td>
<td>No As-Path</td>
</tr>
<tr>
<td>?</td>
<td>10.0.204.0/24</td>
<td>10.0.0.16</td>
<td>100</td>
<td>none</td>
<td>No As-Path</td>
</tr>
</tbody>
</table>

*A:ALA-12#
paths

Syntax

paths

Context

show>router>bgp

Description

This command displays a summary of BGP path attributes.

Output

Show Path Output — The following table describes the command output fields for a BGP path.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP Router ID</td>
<td>The local BGP router ID.</td>
</tr>
<tr>
<td>AS</td>
<td>The configured autonomous system number.</td>
</tr>
<tr>
<td>Local AS</td>
<td>The configured local AS setting. If not configured, then the value is the</td>
</tr>
<tr>
<td></td>
<td>same as the AS.</td>
</tr>
<tr>
<td>Path</td>
<td>The AS path attribute.</td>
</tr>
<tr>
<td>Origin</td>
<td>EGP — The NLRI is learned by an EGP protocol.</td>
</tr>
<tr>
<td></td>
<td>IGP — The NLRI is interior to the originating AS.</td>
</tr>
<tr>
<td></td>
<td>INCOMPLETE — NLRI was learned another way.</td>
</tr>
<tr>
<td>Next Hop</td>
<td>The advertised BGP nexthop.</td>
</tr>
<tr>
<td>MED</td>
<td>The Multi-Exit Discriminator value.</td>
</tr>
<tr>
<td>Local Preference</td>
<td>The local preference value.</td>
</tr>
<tr>
<td>Refs</td>
<td>The number of routes using a specified set of path attributes.</td>
</tr>
<tr>
<td>ASes</td>
<td>The number of autonomous system numbers in the AS path attribute.</td>
</tr>
<tr>
<td>Segments</td>
<td>The number of segments in the AS path attribute.</td>
</tr>
<tr>
<td>Flags</td>
<td>EBGP-learned — Path attributes learned by an EBGP peering.</td>
</tr>
<tr>
<td></td>
<td>IBGP-Learned — Path attributes learned by an IBGP peering.</td>
</tr>
<tr>
<td>Aggregator</td>
<td>The route aggregator ID.</td>
</tr>
<tr>
<td>Community</td>
<td>The BGP community attribute list.</td>
</tr>
<tr>
<td>Originator ID</td>
<td>The originator ID path attribute value.</td>
</tr>
<tr>
<td>Cluster List</td>
<td>The route reflector cluster list.</td>
</tr>
</tbody>
</table>

Sample Output

*A:ALA-12# show router 3 bgp paths

BGP Router ID : 10.0.0.14     AS : 65206   Local AS : 65206

BGP Paths
Path: 60203 65001 19855 3356 15412

Origin           : IGP                  Next Hop         : 10.0.28.1
MED              : 60203                Local Preference : none
Refs             : 4                    ASes             : 5
Segments         : 1
Flags            : EBGP-learned
Aggregator       : 15412  62.216.140.1

Path: 60203 65001 19855 3356 1236 1236 1236 1236

Origin           : IGP                  Next Hop         : 10.0.28.1
MED              : 60203                Local Preference : none
Refs             : 2                    ASes             : 9
Segments         : 1
Flags            : EBGP-learned

*A:ALA-12#
routes

**Syntax**

routes [family family] [prefix [detail | longer]]
routes [family family] [prefix [hunt | brief]]
routes [family family] [community comm-id]
routes [family family] [aspath-regex reg-exp]
routes [family family] [ipv6-prefix[/prefix-length] [detail | longer] | [hunt [brief]]]

**Context**
show>router>bgp

**Description**
This command displays BGP route information.
When this command is issued without any parameters, then the entire BGP routing table displays.
When this command is issued with an IP prefix/mask or IP address, then the best match for the parameter displays.

**Parameters**

*family family* — Specifies the type of routing information to be distributed by the BGP instance.

*Values*

- ipv4 — Displays only those BGP peers that have the IPv4 family enable and not those capable of exchanging IP-VPN routes.
- vpn-ipv4 — Displays the BGP peers that are IP-VPN capable.
- ipv6 — Displays the BGP peers that are IPv6 capable.
- mcast-ipv4 — Displays the BGP peers that are mcast-ipv4 capable.

*prefix* — Specifies the type of routing information to display.

*Values*

- rd[/ip-address[mask]]
  - rd
    - ip-address
      - number1: 1 — 65535
      - as-number1: 1 — 65535
      - number2: 0 — 4294967295
      - as-number2: 1 — 4294967295
      - number3: 0 — 65535
      - ip-address: a.b.c.d
      - mask: 0 — 32

- ipv6-prefix[/prefix-length] — Specifies the type of IPv6 routing information to display.

*Values*

- ipv6-prefix: x:x:x:x:x:x:x:x (eight 16-bit pieces)
  - x:x:x:x:x:x:d.d.d.d
  - x: [0 — FFFF]H
  - d: [0 — 255]D
  - prefix-length: 0 — 128

*filter* — Specifies route criteria.

*Values*

- hunt — Displays entries for the specified route in the RIB-In, RIB-Out, and RTM.
- longer — Displays the specified route and subsets of the route.
- detail — Display the longer, more detailed version of the output.

*aspath-regex “reg-exp”* — Displays all routes with an AS path matching the specified regular expression *reg-exp*.

*community comm.-id* — Displays all routes with the specified BGP community.
Values

\[ \text{as-number1:comm-val1} | \text{ext-comm} | \text{well-known-comm} \]

- ext-comm
  - type: \{ip-address:comm-val1 | as-number1:comm-val2 | as-number2:comm-val1\}
  - as-number1: 0..65535
  - comm-val1: 0..65535
  - type: keywords: target, origin
  - ip-address: a.b.c.d
  - comm-val2: 0 — 4294967295
  - as-number2: 0 — 4294967295
  - well-known-comm: no-export, no-export-subconfed, no-advertise

Output

Show BGP Routes — The following table describes the command output fields for BGP routes.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP Router ID</td>
<td>The local BGP router ID.</td>
</tr>
<tr>
<td>AS</td>
<td>The configured autonomous system number.</td>
</tr>
<tr>
<td>Local AS</td>
<td>The configured local AS setting, if not configured it is the same as the system AS.</td>
</tr>
<tr>
<td>Network</td>
<td>The IP prefix and mask length.</td>
</tr>
<tr>
<td>Nexthop</td>
<td>The BGP nexthop.</td>
</tr>
<tr>
<td>From</td>
<td>The advertising BGP neighbor’s IP address.</td>
</tr>
<tr>
<td>Res. Nexthop</td>
<td>The resolved nexthop.</td>
</tr>
<tr>
<td>Local Pref.</td>
<td>The local preference value.</td>
</tr>
<tr>
<td>Flag</td>
<td>u — used</td>
</tr>
<tr>
<td></td>
<td>s — suppressed</td>
</tr>
<tr>
<td></td>
<td>h — history</td>
</tr>
<tr>
<td></td>
<td>d — decayed</td>
</tr>
<tr>
<td></td>
<td>* — valid</td>
</tr>
<tr>
<td></td>
<td>i — igp</td>
</tr>
<tr>
<td></td>
<td>e — egp</td>
</tr>
<tr>
<td></td>
<td>? — incomplete</td>
</tr>
<tr>
<td></td>
<td>&gt; — best</td>
</tr>
<tr>
<td>Aggregator AS</td>
<td>The aggregator AS value.</td>
</tr>
<tr>
<td></td>
<td>none — No aggregator AS attributes are present.</td>
</tr>
<tr>
<td>Aggregator</td>
<td>The aggregator attribute value.</td>
</tr>
<tr>
<td></td>
<td>none — no Aggregator attributes are present.</td>
</tr>
<tr>
<td>Atomic Aggr.</td>
<td>Atomic — The atomic aggregator flag is set.</td>
</tr>
</tbody>
</table>
Sample Output

*A:ALA-12>config>router>bgp# show router 3 bgp routes family ipv4

<table>
<thead>
<tr>
<th>Flag</th>
<th>Network</th>
<th>Nexthop</th>
<th>LocalPref</th>
<th>MED</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>100.0.0.0/31</td>
<td>10.20.1.2</td>
<td>100</td>
<td>131070</td>
</tr>
</tbody>
</table>

*A:ALA-12>config>router>bgp#

A:SR-12# show router bgp routes 100.0.0.0/31 hunt

<table>
<thead>
<tr>
<th>Network</th>
<th>Nexthop</th>
<th>Route Dist.</th>
<th>VPN Label</th>
<th>Interface Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>100.0.0.0/31</td>
<td>10.20.1.2</td>
<td>10.20.1.2:1</td>
<td>131070</td>
<td>to-sr7</td>
</tr>
</tbody>
</table>

### Table

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MED</td>
<td>The MED metric value.</td>
</tr>
<tr>
<td>none</td>
<td>No MED metric is present.</td>
</tr>
<tr>
<td>Community</td>
<td>The BGP community attribute list.</td>
</tr>
<tr>
<td>Cluster</td>
<td>The route reflector cluster list.</td>
</tr>
<tr>
<td>Originator Id</td>
<td>The originator ID path attribute value.</td>
</tr>
<tr>
<td>none</td>
<td>The originator ID attribute is not present.</td>
</tr>
<tr>
<td>Peer Router Id</td>
<td>The router ID of the advertising router.</td>
</tr>
<tr>
<td>AS-Path</td>
<td>The BGP AS path attribute.</td>
</tr>
<tr>
<td>VPNN Imported</td>
<td>Displays the VPRNs where a particular BGP-VPN received route has been imported and installed.</td>
</tr>
</tbody>
</table>
ecmp

**Syntax**

cemp

**Context**

show>router

**Description**

This command displays the ECMP settings for the router.

**Output**

*Show ECMP Settings Output* — The following table describes the output fields for the router ECMP settings.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instance</td>
<td>The router instance number.</td>
</tr>
<tr>
<td>Router Name</td>
<td>The name of the router instance.</td>
</tr>
</tbody>
</table>
| ECMP                          | False — ECMP is disabled for the instance.  
                                    | True — ECMP is enabled for the instance. |
| Configured-ECMP-Routes        | The number of ECMP routes configured for path sharing. |

**Sample Output**

*A:ALA-12# show router 3 ecmp

-----------------------------------------------------------------------------------------------

<table>
<thead>
<tr>
<th>Instance</th>
<th>Router Name</th>
<th>ECMP</th>
<th>Configured-ECMP-Routes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Base</td>
<td>True</td>
<td>8</td>
</tr>
</tbody>
</table>

*A:ALA-12#
interface

Syntax  interface  [[ip-address | ip-int-name] [detail]] | [summary] | [exclude-services]

Context  show>router

Description  This command displays the router IP interface table sorted by interface index.

Parameters  
ip-address — Only displays the interface information associated with the specified IP address.

ip-int-name — Only displays the interface information associated with the specified IP interface name.

detail — Displays detailed IP interface information.

summary — Displays summary IP interface information for the router.

exclude-services — Displays IP interface information, excluding IP interfaces configured for customer services. Only core network IP interfaces are displayed.

Output  Standard IP Interface Output — The following table describes the standard output fields for an IP interface:

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface-Name</td>
<td>The IP interface name.</td>
</tr>
<tr>
<td>Type</td>
<td>n/a — No IP address has been assigned to the IP interface, so the IP address type is not applicable.</td>
</tr>
<tr>
<td></td>
<td>Pri — The IP address for the IP interface is the Primary address on the IP interface.</td>
</tr>
<tr>
<td></td>
<td>Sec — The IP address for the IP interface is a secondary address on the IP interface.</td>
</tr>
<tr>
<td>IP-Address</td>
<td>The IP address and subnet mask length of the IP interface.</td>
</tr>
<tr>
<td></td>
<td>n/a — Indicates no IP address has been assigned to the IP interface.</td>
</tr>
<tr>
<td>Adm</td>
<td>Down — The IP interface is administratively disabled.</td>
</tr>
<tr>
<td></td>
<td>Up — The IP interface is administratively enabled.</td>
</tr>
<tr>
<td>Opr</td>
<td>Down — The IP interface is operationally disabled.</td>
</tr>
<tr>
<td></td>
<td>Up — The IP interface is operationally enabled.</td>
</tr>
<tr>
<td>Mode</td>
<td>Network — The IP interface is a network/core IP interface.</td>
</tr>
<tr>
<td></td>
<td>Service — The IP interface is a service IP interface.</td>
</tr>
</tbody>
</table>

Sample Output

*A:ALA-12#  show router 3 interface

===============================================================================
<p>| Interface Table |</p>
<table>
<thead>
<tr>
<th>Interface-Name</th>
<th>Type</th>
<th>IP-Address</th>
<th>Adm</th>
<th>Opr</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
VPRN Show Commands

```c
*ALA-12# show router 3 interface 10.1.1.3/24

*A:ALA-12#
```

```c
*ALA-12# show router 3 interface exclude-services

*A:ALA-12#
```

**Detailed IP Interface Output** — The following table describes the detailed output fields for an IP interface.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>If Name</td>
<td>The IP interface name.</td>
</tr>
<tr>
<td>Admin State</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Down</strong> — The IP interface is administratively disabled.</td>
</tr>
</tbody>
</table>
### Show, Clear, Debug Commands

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
</table>
| Oper State          | Down — The IP interface is operationally disabled.  
                         Up — The IP interface is operationally disabled.  |
| IP Addr/mask        | The IP address and subnet mask length of the IP interface.  
                         Not Assigned — Indicates no IP address has been assigned to the IP interface.  |
| Address Type        | Primary — The IP address for the IP interface is the Primary address on the IP interface.  
                         Secondary — The IP address for the IP interface is a Secondary address on the IP interface.  |
| IGP Inhibit         | Disabled — The secondary IP address on the interface will be recognized as a local interface by the IGP.  
                         Enabled — The secondary IP address on the interface will not be recognized as a local interface by the IGP.  |
| Broadcast Address   | All-ones — The broadcast format on the IP interface is all ones.  
                         Host-ones — The broadcast format on the IP interface is host ones.  |
| If Index            | The interface index of the IP router interface.  |
| If Type             | Network — The IP interface is a network/core IP interface.  
                         Service — The IP interface is a service IP interface.  |
| Port Id             | The port ID of the IP interface.  |
| Egress Filter       | The egress IP filter policy ID associated with the IP interface.  
                         none — Indicates no egress filter policy is associated with the interface.  |
| Ingress Filter      | The ingress IP filter policy ID associated with the IP interface.  
                         none — Indicates no ingress filter policy is associated with the interface.  |
| QoS Policy          | The QoS policy ID associated with the IP interface.  |
| SNTP Broadcast      | False — Receipt of SNTP broadcasts on the IP interface is disabled.  
                         True — Receipt of SNTP broadcasts on the IP interface is enabled.  |
| MAC Address         | The MAC address of the IP interface.  |
| Arp Timeout         | The ARP timeout for the interface, in seconds, which is the time an ARP entry is maintained in the ARP cache without being refreshed.  |
| IP MTU              | The IP Maximum Transmission Unit (MTU) for the IP interface.  |
| ICMP Mask Reply     | False — The IP interface will not reply to a received ICMP mask request.  
                         True — The IP interface will reply to a received ICMP mask request.  |
### Interface Table

<table>
<thead>
<tr>
<th>Interface</th>
<th>Admin State</th>
<th>Oper State</th>
<th>IP Addr/mask</th>
<th>Address Type</th>
<th>IGP Inhibit</th>
<th>Broadcast Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>to-ser1</td>
<td>Up</td>
<td>Up</td>
<td>10.10.13.3/24</td>
<td>Primary</td>
<td>Disabled</td>
<td>Host-ones</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>10.200.0.1/16</td>
<td>Secondary</td>
<td>Enabled</td>
<td>Host-ones</td>
</tr>
</tbody>
</table>

### Details

- **If Index**: 2
- **Port Id**: 1/1/2
- **Egress Filter**: none
- **QoS Policy**: 1
- **MAC Address**: 04:5d:01:01:00:02
- **IP MTU**: 1500
- **Cflowd**: none

### ICMP Details

- **Redirects**: Disabled
- **Unreachables**: Number - 100, Time (seconds) - 10
- **TTL Expired**: Number - 100, Time (seconds) - 10

---

**Summary IP Interface Output** — The following table describes the summary output fields for the router IP interfaces.
**Show, Clear, Debug Commands**

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instance</td>
<td>The router instance number.</td>
</tr>
<tr>
<td>Router Name</td>
<td>The name of the router instance.</td>
</tr>
<tr>
<td>Interfaces</td>
<td>The number of IP interfaces in the router instance.</td>
</tr>
<tr>
<td>Admin-Up</td>
<td>The number of administratively enabled IP interfaces in the router instance.</td>
</tr>
<tr>
<td>Oper-Up</td>
<td>The number of operationally enabled IP interfaces in the router instance.</td>
</tr>
</tbody>
</table>

**Sample Output**

```
*A:AL-C# show router 3 interface summary
===============================================================================
Router Summary (Interfaces)
===============================================================================
Instance  Router Name                       Interfaces    Admin-Up   Oper-Up
-------------------------------------------------------------------------------
1         Base                              7             7          5
===============================================================================
*A:AL-C#
```

**mvpn**

**Syntax**

mvpn

**Context**

show>router router-instance

**Description**

This command displays Multicast VPN related information. The router instance must be specified.

**Sample Output**

```
*A:Dut-C# show router 1 mvpn
===============================================================================
MVPN 1 configuration data
===============================================================================
signaling          : Bgp                  auto-discovery     : Enabled
UMH Selection      : Highest-Ip           intersite-shared   : Enabled
vrf-import         : N/A                  vrf-export         : N/A
vrf-target         : target:1:1          C-Mcast Import RT  : target:10.20.1.3:2
ipmsi              : pim-asm 224.1.1.1    admin status       : Up                   three-way-hello : N/A
admin status       : N/A                  hello-interval     : N/A                  hello-multiplier : 35 * 0.1
tracking support   : Disabled             tracking support   : Disabled             Improved Assert : N/A
spmsi              : pim-ssm 225.0.0.0/32   data-delay-interval: 3 seconds
join-tlv-packing   : N/A                  data-threshold     : 224.0.0.0/4 --> 1 kbps
```
route-table

Syntax: `route-table [ip-prefix [mask] [longer] | [protocol protocol] | [summary]]`

Context: `show>router`

Description: This command displays the active routes in the routing table. If no command line arguments are specified, all routes are displayed, sorted by prefix.

Parameters:
- `ip-prefix[|mask]` — Displays routes only matching the specified `ip-prefix` and optional `mask`.
- `longer` — Displays routes matching the `ip-prefix/mask` and routes with longer masks.
- `protocol protocol` — Displays routes learned from the specified protocol.

Values: `bgp, isis, local, ospf, rip, static, aggregate`

summary — Displays a route table summary information.

Output:

Standard Show Route Table Output — The following table describes the standard output fields for the route table.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dest Address</td>
<td>The route destination address and mask.</td>
</tr>
<tr>
<td>Next Hop</td>
<td>The next hop IP address for the route destination.</td>
</tr>
<tr>
<td>Type</td>
<td>Local — The route is a local route.</td>
</tr>
<tr>
<td></td>
<td>Remote — The route is a remote route.</td>
</tr>
<tr>
<td>Protocol</td>
<td>The protocol through which the route was learned.</td>
</tr>
<tr>
<td>Age</td>
<td>The route age in seconds for the route.</td>
</tr>
<tr>
<td>Metric</td>
<td>The route metric value for the route.</td>
</tr>
<tr>
<td>Pref</td>
<td>The route preference value for the route.</td>
</tr>
<tr>
<td>No. of Routes:</td>
<td>The number of routes displayed in the list.</td>
</tr>
</tbody>
</table>

Sample Output

```
*ALA-12# show router 3 route-table
```

<table>
<thead>
<tr>
<th>Dest Address</th>
<th>Next Hop</th>
<th>Type</th>
<th>Protocol</th>
<th>Age</th>
<th>Metric</th>
<th>Pref</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.10.0.1/32</td>
<td>10.10.13.1</td>
<td>Remote</td>
<td>OSPF</td>
<td>65844</td>
<td>1001</td>
<td>10</td>
</tr>
<tr>
<td>10.10.0.2/32</td>
<td>10.10.13.1</td>
<td>Remote</td>
<td>OSPF</td>
<td>65844</td>
<td>2001</td>
<td>10</td>
</tr>
<tr>
<td>10.10.0.3/32</td>
<td>0.0.0.0</td>
<td>Local</td>
<td>Local</td>
<td>1329261</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>10.10.0.4/32</td>
<td>10.10.34.4</td>
<td>Remote</td>
<td>OSPF</td>
<td>3523</td>
<td>1001</td>
<td>10</td>
</tr>
<tr>
<td>10.10.0.5/32</td>
<td>10.10.35.5</td>
<td>Remote</td>
<td>OSPF</td>
<td>1084022</td>
<td>1001</td>
<td>10</td>
</tr>
</tbody>
</table>
### Show, Clear, Debug Commands

#### 10.10.12.0/24  10.10.13.1  Remote  OSPF  65844  2000  10
#### 10.10.15.0/24  10.10.13.1  Remote  OSPF  58836  2000  10
#### 10.10.24.0/24  10.10.34.4  Remote  OSPF  3523   2000  10
#### 10.10.25.0/24  10.10.35.5  Remote  OSPF  399059 2000  10
#### 10.10.34.0/24  0.0.0.0      Local   Local   3543    0       0
#### 10.10.35.0/24  0.0.0.0      Local   Local   1329259 0       0
#### 10.10.45.0/24  10.10.34.4  Remote  OSPF  3523   2000  10
#### 10.200.0.0/16  0.0.0.0      Local   Local   4513    0       0
#### 192.168.0.0/20 0.0.0.0      Local   Local   1329264 0       0
#### 192.168.254.0/24 0.0.0.0     Remote  Static 11     1       5

<table>
<thead>
<tr>
<th>Dest Address</th>
<th>Next Hop</th>
<th>Type</th>
<th>Protocol</th>
<th>Age</th>
<th>Metric</th>
<th>Pref</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.10.0.4/32</td>
<td>10.10.34.4</td>
<td>Remote</td>
<td>OSPF</td>
<td>3523</td>
<td>1001</td>
<td>10</td>
</tr>
<tr>
<td>10.10.0.5/32</td>
<td>10.10.35.5</td>
<td>Remote</td>
<td>OSPF</td>
<td>1084022</td>
<td>1001</td>
<td>10</td>
</tr>
<tr>
<td>10.10.12.0/24</td>
<td>10.10.13.1</td>
<td>Remote</td>
<td>OSPF</td>
<td>65844</td>
<td>2001</td>
<td>10</td>
</tr>
<tr>
<td>10.10.15.0/24</td>
<td>10.10.13.1</td>
<td>Remote</td>
<td>OSPF</td>
<td>58836</td>
<td>2000</td>
<td>10</td>
</tr>
<tr>
<td>10.10.24.0/24</td>
<td>10.10.34.4</td>
<td>Remote</td>
<td>OSPF</td>
<td>3523</td>
<td>2000</td>
<td>10</td>
</tr>
<tr>
<td>10.10.25.0/24</td>
<td>10.10.35.5</td>
<td>Remote</td>
<td>OSPF</td>
<td>399059</td>
<td>2000</td>
<td>10</td>
</tr>
<tr>
<td>10.10.45.0/24</td>
<td>10.10.34.4</td>
<td>Remote</td>
<td>OSPF</td>
<td>3523</td>
<td>2000</td>
<td>10</td>
</tr>
</tbody>
</table>

*A:ALA-12# show router 3 route-table 10.10.0.4

Route Table

<table>
<thead>
<tr>
<th>Dest Address</th>
<th>Next Hop</th>
<th>Type</th>
<th>Protocol</th>
<th>Age</th>
<th>Metric</th>
<th>Pref</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.10.0.4/32</td>
<td>10.10.34.4</td>
<td>Remote</td>
<td>OSPF</td>
<td>3523</td>
<td>1001</td>
<td>10</td>
</tr>
</tbody>
</table>

*A:ALA-12# show router 3 route-table 10.10.0.4/32 longer

Route Table

<table>
<thead>
<tr>
<th>Dest Address</th>
<th>Next Hop</th>
<th>Type</th>
<th>Protocol</th>
<th>Age</th>
<th>Metric</th>
<th>Pref</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.10.0.4/32</td>
<td>10.10.34.4</td>
<td>Remote</td>
<td>OSPF</td>
<td>3523</td>
<td>1001</td>
<td>10</td>
</tr>
</tbody>
</table>

No. of Routes: 1

+ : indicates that the route matches on a longer prefix

*A:ALA-12# show router 3 route-table protocol ospf

Route Table

<table>
<thead>
<tr>
<th>Dest Address</th>
<th>Next Hop</th>
<th>Type</th>
<th>Protocol</th>
<th>Age</th>
<th>Metric</th>
<th>Pref</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.10.10.0/24</td>
<td>10.10.13.1</td>
<td>Remote</td>
<td>OSPF</td>
<td>65844</td>
<td>2001</td>
<td>10</td>
</tr>
<tr>
<td>10.10.10.1/24</td>
<td>10.10.13.1</td>
<td>Remote</td>
<td>OSPF</td>
<td>65844</td>
<td>2001</td>
<td>10</td>
</tr>
<tr>
<td>10.10.0.4/32</td>
<td>10.10.34.4</td>
<td>Remote</td>
<td>OSPF</td>
<td>3523</td>
<td>1001</td>
<td>10</td>
</tr>
<tr>
<td>10.10.10.0/32</td>
<td>10.10.35.5</td>
<td>Remote</td>
<td>OSPF</td>
<td>1084022</td>
<td>1001</td>
<td>10</td>
</tr>
<tr>
<td>10.10.15.0/24</td>
<td>10.10.13.1</td>
<td>Remote</td>
<td>OSPF</td>
<td>65844</td>
<td>2000</td>
<td>10</td>
</tr>
<tr>
<td>10.10.24.0/24</td>
<td>10.10.13.1</td>
<td>Remote</td>
<td>OSPF</td>
<td>58836</td>
<td>2000</td>
<td>10</td>
</tr>
<tr>
<td>10.10.25.0/24</td>
<td>10.10.35.5</td>
<td>Remote</td>
<td>OSPF</td>
<td>399059</td>
<td>2000</td>
<td>10</td>
</tr>
<tr>
<td>10.10.45.0/24</td>
<td>10.10.34.4</td>
<td>Remote</td>
<td>OSPF</td>
<td>3523</td>
<td>2000</td>
<td>10</td>
</tr>
</tbody>
</table>

*A:ALA-12# show router 3 route-table summary

Route Table Summary
service-prefix

Syntax  service-prefix

Context  show>router

Description  This command displays service-prefix information.

Output  Show Service Prefix Output — The following table describes the service prefix output fields.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Prefix</td>
<td>Displays information for the specified IP prefix.</td>
</tr>
<tr>
<td>Mask</td>
<td>Displays information for the specified mask length.</td>
</tr>
</tbody>
</table>

Sample Output

*A:ALA-12# show router 3 service-prefix

Address Ranges Reserved for Services (Service: 3)

<table>
<thead>
<tr>
<th>IP Prefix</th>
<th>Mask</th>
<th>Exclusive</th>
</tr>
</thead>
<tbody>
<tr>
<td>No Matching Entries Found</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*A:ALA-12#show>router#
static-arp

Syntax  static-arp [ip-address | ip-int-name | mac ieee-mac-addr]

Context  show>router

Description  This command displays the router static ARP table sorted by IP address. If no options are present, all ARP entries are displayed.

Parameters  
ip-address — Only displays static ARP entries associated with the specified IP address.
ip-int-name — Only displays static ARP entries associated with the specified IP interface name.
mac ieee-mac-addr — Only displays static ARP entries associated with the specified MAC address.

Output  Static ARP Table Output — The following table describes the output fields for the ARP table.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>The IP address of the static ARP entry.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>The MAC address of the static ARP entry.</td>
</tr>
<tr>
<td>Age</td>
<td>The age of the ARP entry. Static ARPs always have 00:00:00 for the age.</td>
</tr>
<tr>
<td>Type</td>
<td>Inv — The ARP entry is an inactive static ARP entry (invalid).</td>
</tr>
<tr>
<td></td>
<td>Sta — The ARP entry is an active static ARP entry.</td>
</tr>
<tr>
<td>Interface</td>
<td>The IP interface name associated with the ARP entry.</td>
</tr>
<tr>
<td>No. of ARP Entries</td>
<td>The number of ARP entries displayed in the list.</td>
</tr>
</tbody>
</table>

Sample Output

*A:ALA-12# show router 3 static-arp

ARP Table

<table>
<thead>
<tr>
<th>IP Address</th>
<th>MAC Address</th>
<th>Age</th>
<th>Type</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.200.0.253</td>
<td>00:00:5a:40:00:01 00:00:00</td>
<td>Sta</td>
<td></td>
<td>to-ser1</td>
</tr>
<tr>
<td>12.200.1.1</td>
<td>00:00:5a:01:00:33 00:00:00</td>
<td>Inv</td>
<td></td>
<td>to-ser1 a</td>
</tr>
</tbody>
</table>

No. of ARP Entries: 2

*A:ALA-12#

*A:ALA-12# show router 3 static-arp 12.200.1.1

ARP Table

<table>
<thead>
<tr>
<th>IP Address</th>
<th>MAC Address</th>
<th>Age</th>
<th>Type</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.200.1.1</td>
<td>00:00:5a:01:00:33 00:00:00</td>
<td>Inv</td>
<td></td>
<td>to-ser1 a</td>
</tr>
</tbody>
</table>

*A:ALA-12#
static-route

Syntax  static-route [ip-prefix [mask]] | [preference preference] | [next-hop ip-addr] [detail]

Context  show>router

Description  This command displays the static entries in the routing table.
If no options are present, all static routes are displayed sorted by prefix.

Parameters  ip-prefix [mask] — Displays static routes only matching the specified ip-prefix and mask.
preference preference — Only displays static routes with the specified route preference.
Values  0 — 65535
next-hop ip-addr — Only displays static routes with the specified next hop IP address.
detail — Displays detailed information about the static route.

Output  Show Static Route Output — The following table describes the output fields for the static route table:

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Addr/mask</td>
<td>The static route destination address and mask.</td>
</tr>
<tr>
<td>Pref</td>
<td>The route preference value for the static route.</td>
</tr>
<tr>
<td>Metric</td>
<td>The route metric value for the static route.</td>
</tr>
<tr>
<td>Type</td>
<td>BH — The static route is a black hole route. The Next hop for this type of route is black-hole.</td>
</tr>
<tr>
<td></td>
<td>ID — The static route is an indirect route, where the Next hop for this type of route is the non-directly connected next hop.</td>
</tr>
</tbody>
</table>
Show, Clear, Debug Commands

<table>
<thead>
<tr>
<th>Label</th>
<th>Description (Continued)</th>
</tr>
</thead>
<tbody>
<tr>
<td>NH</td>
<td>The route is a static route with a directly connected next hop. The Nexthop for this type of route is either the next hop IP address or an egress IP interface name.</td>
</tr>
<tr>
<td>Next Hop</td>
<td>The next hop for the static route destination.</td>
</tr>
<tr>
<td>Interface</td>
<td>The egress IP interface name for the static route. n/a — indicates there is no current egress interface because the static route is inactive or a black hole route.</td>
</tr>
<tr>
<td>Active</td>
<td>N — The static route is inactive; for example, the static route is disabled or the next hop IP interface is down. Y — The static route is active.</td>
</tr>
</tbody>
</table>

No. of Routes: The number of routes displayed in the list.

Sample Output

*A:ALA-12# show router 3 static-route

Route Table

<table>
<thead>
<tr>
<th>IP Addr/mask</th>
<th>Pref Metric</th>
<th>Type</th>
<th>Nexthop</th>
<th>Interface</th>
<th>Active</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.250.0/24</td>
<td>5 1</td>
<td>ID</td>
<td>10.200.10.1</td>
<td>to-ser1</td>
<td>Y</td>
</tr>
<tr>
<td>192.168.252.0/24</td>
<td>5 1</td>
<td>NH</td>
<td>10.10.0.254</td>
<td>n/a</td>
<td>N</td>
</tr>
<tr>
<td>192.168.253.0/24</td>
<td>5 1</td>
<td>NH</td>
<td>to-ser1</td>
<td>n/a</td>
<td>N</td>
</tr>
<tr>
<td>192.168.253.0/24</td>
<td>5 1</td>
<td>NH</td>
<td>10.10.0.254</td>
<td>n/a</td>
<td>N</td>
</tr>
<tr>
<td>192.168.254.0/24</td>
<td>4 1</td>
<td>BH</td>
<td>black-hole</td>
<td>n/a</td>
<td>Y</td>
</tr>
</tbody>
</table>

*A:ALA-12#

*A:ALA-12# show router 3 static-route 192.168.250.0/24

Route Table

<table>
<thead>
<tr>
<th>IP Addr/mask</th>
<th>Pref Metric</th>
<th>Type</th>
<th>Nexthop</th>
<th>Interface</th>
<th>Active</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.250.0/24</td>
<td>5 1</td>
<td>ID</td>
<td>10.200.10.1</td>
<td>to-ser1</td>
<td>Y</td>
</tr>
</tbody>
</table>

*A:ALA-12#

*A:ALA-12# show router 3 static-route preference 4

Route Table

<table>
<thead>
<tr>
<th>IP Addr/mask</th>
<th>Pref Metric</th>
<th>Type</th>
<th>Nexthop</th>
<th>Interface</th>
<th>Active</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.254.0/24</td>
<td>4 1</td>
<td>BH</td>
<td>black-hole</td>
<td>n/a</td>
<td>Y</td>
</tr>
</tbody>
</table>

*A:ALA-12#

*A:ALA-12# show router 3 static-route next-hop 10.10.0.254

Route Table

<table>
<thead>
<tr>
<th>IP Addr/mask</th>
<th>Pref Metric</th>
<th>Type</th>
<th>Nexthop</th>
<th>Interface</th>
<th>Active</th>
</tr>
</thead>
</table>

A:ALA-12#
### Route Table

<table>
<thead>
<tr>
<th>IP Addr/mask</th>
<th>Pref</th>
<th>Metric</th>
<th>Type</th>
<th>Nexthop</th>
<th>Interface</th>
<th>Active</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.253.0/24</td>
<td>5</td>
<td>1</td>
<td>NH</td>
<td>10.10.0.254</td>
<td>n/a</td>
<td>N</td>
</tr>
</tbody>
</table>

*A:ALA-12#

*A:Dut-B# show router static-route

```plaintext
Static Route Table (Router: Base)  Family: IPv4

Prefix                  Tag     Met    Pref  Type  Act
Next Hop                Interface
---------------------------------------------------
1.2.3.4/32            0  1  5    NH    Y
                      10.11.25.6
                      ip-10.11.25.5_base_to_cpe_static
10.11.15.0/24         0  1  5    NH    Y
                      10.11.25.6
                      ip-10.11.25.5_base_to_cpe_static
```

No. of Static Routes: 2

*A:Dut-B# show router static-route detail

```plaintext
Static Route Table (Router: Base)  Family: IPv4

Network          : 1.2.3.4/32
Nexthop          : 10.11.25.6
Type             : Nexthop
Interface        : ip-10.11.25.5_base_to_cpe_static
Metric           : 1
Admin State      : Up
BFD              : disabled
CPE-check        : enabled
Target           : 10.11.18.6
Interval         : 1
Log              : N
CPE Host Up Time : 0d 00:00:02
CPE Echo Req Tx  : 3
CPE Up Trans     : 1
CPE TTL          : 2

Network          : 10.11.15.0/24
Nexthop          : 10.11.25.6
Type             : Nexthop
Interface        : ip-10.11.25.5_base_to_cpe_static
Metric           : 1
Admin State      : Up
BFD              : disabled
CPE-check        : disabled
```

No. of Static Routes: 2

*A:CPM133>config>router# show router static-route 3.3.3.3/32 detail

```plaintext
Static Route Table (Router: Base)  Family: IPv4

Network          : 3.3.3.3/32
```

*A:CPM133>config>router# show router static-route 3.3.3.3/32 detail
Static Route Table (Router: Base)  Family: IPv4
===============================================================================
Prefix           : 3.3.3.3/32
Nexthop          : n/a
Type             : Blackhole       Nexthop Type      : IP
Interface        : n/a                             Active            : Y
Prefix List      : n/a                             Prefix List Type  : n/a
Metric           : 1                               Preference        : 5
Admin  State     : Up                              Tag               : 0
BFD              : disabled                        Community         : 100:33
CPE-check        : disabled
-------------------------------------------------------------------------------
No. of Static Routes: 1
===============================================================================

tunnel-table

Syntax          tunnel-table [ip-address[/mask] | protocol protocol | sdp sdp-id]
tunnel-table [summary]

Context         show>router

Description     This command displays tunnel table information.

Note that auto-bind GRE tunnels are not displayed in show command output. GRE tunnels are not the same as SDP tunnels that use the GRE encapsulation type. When the auto-bind command is used when configuring a VPRN service, it means the MP-BGP NH resolution is referring to core routing instance for IP reachability. For a VPRN service this object specifies the lookup to be used by the routing instance if no SDP to the destination exists.

Parameters      ip-address[/mask] — Displays the specified tunnel table’s destination IP address and mask.

               protocol protocol — Displays LDP protocol information.

               sdp sdp-id — Displays information pertaining to the specified SDP.

               summary — Displays summary tunnel table information.

Output          Show Tunnel Table Output — The following table describes tunnel table output fields:

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination</td>
<td>The route’s destination address and mask.</td>
</tr>
<tr>
<td>Owner</td>
<td>Specifies the tunnel owner.</td>
</tr>
<tr>
<td>Encap</td>
<td>Specifies the tunnel’s encapsulation type.</td>
</tr>
<tr>
<td>Tunnel ID</td>
<td>Specifies the tunnel (SDP) identifier.</td>
</tr>
<tr>
<td>Pref</td>
<td>Specifies the route preference for routes learned from the configured peer(s).</td>
</tr>
<tr>
<td>Nexthop</td>
<td>The next hop for the route’s destination.</td>
</tr>
<tr>
<td>Metric</td>
<td>The route metric value for the route.</td>
</tr>
</tbody>
</table>
Sample Output

*A:ALA-12>config>service# show router 3 tunnel-table

Tunnel Table

<table>
<thead>
<tr>
<th>Destination</th>
<th>Owner</th>
<th>Encap</th>
<th>Tunnel Id</th>
<th>Pref</th>
<th>NexthopMetric</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.0.1/32</td>
<td>sdp</td>
<td>GRE</td>
<td>10</td>
<td>5</td>
<td>10.0.0.1</td>
</tr>
<tr>
<td>10.0.0.1/32</td>
<td>sdp</td>
<td>GRE</td>
<td>21</td>
<td>5</td>
<td>10.0.0.1</td>
</tr>
<tr>
<td>10.0.0.1/32</td>
<td>sdp</td>
<td>GRE</td>
<td>31</td>
<td>5</td>
<td>10.0.0.1</td>
</tr>
<tr>
<td>10.0.0.1/32</td>
<td>sdp</td>
<td>GRE</td>
<td>41</td>
<td>5</td>
<td>10.0.0.1</td>
</tr>
</tbody>
</table>

*A:ALA-12>config>service#

*A:ALA-12>config>service#  show router 3 tunnel-table summary

Tunnel Table Summary (Router: Base)

<table>
<thead>
<tr>
<th></th>
<th>Active</th>
<th>Available</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDP</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>SDP</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

*A:ALA-12>config>service#
VPRN Clear Commands

apr

Syntax: 
```
arp
```

Context: `clear>service>id`

Description: This command clears ARP host data.

arp-host

Syntax: 
```
arp-host
arp-host { mac ieee-address | sap sap-id | ip-address ip-address[/mask] }  
arp-host [port port-id] [inter-dest-id intermediate-destination-id | no-inter-dest-id]  
arp-host statistics [sap sap-id | interface interface-name]
```

Context: `clear>service>id`

Description: This command clears ARP host data.

interface

Syntax: 
```
interface [ip-int-name | ip-addr] [icmp]
```

Context: `clear>router`

Description: This command clears IP interface statistics.

Parameters: `ip-int-name | ip-addr` — The IP interface name or IP interface address.

Default: All IP interfaces.

`icmp` — Specifies to reset the ICMP statistics for the IP interface(s) used for ICMP rate limit.

damping

Syntax: 
```
damping [[ip-prefix/mask] [neighbor ip-address]] | [group name]
```

Context: `clear>router>bgp`

Description: This command clears or resets the route damping information for received routes.

Parameters: `ip-prefix/mask` — Clears damping information for entries that match the IP prefix and mask length.
**neighbor** *ip-address* — Clears damping information for entries received from the BGP neighbor.

**group** *name* — Clears damping information for entries received from any BGP neighbors in the peer group.

---

**flap-statistics**

**Syntax**

```
flap-statistics [ip-prefix/mask] [neighbor ip-addr] [group group-name] [regex reg-exp] [policy policy-name]
```

**Context**

```
clear>router>bgp
```

**Description**

This command clears route flap statistics.

**Parameters**

- **ip-prefix/mask** — Clears route flap statistics for entries that match the specified IP prefix and mask length.
- **neighbor ip-addr** — Clears route flap statistics for entries received from the specified BGP neighbor.
- **group group-name** — Clears route flap statistics for entries received from any BGP neighbors in the specified peer group.
- **regex reg-exp** — Clears route flap statistics for all entries which have the regular expression and the AS path that matches the regular expression.
- **policy policy-name** — Clears route flap statistics for entries that match the specified route policy.

---

**neighbor**

**Syntax**

```
neighbor {ip-addr | as as-number | external | all} [soft | soft-inbound | statistics]
```

**Context**

```
clear>router>bgp
```

**Description**

This command resets the specified BGP peer or peers. This can cause existing BGP connections to be shutdown and restarted.

**Parameters**

- **ip-addr** — Resets the BGP neighbor with the specified IP address.
- **as as-number** — Resets all BGP neighbors with the specified peer AS.
- **external** — Resets all EBGP neighbors.
- **all** — Resets all BGP neighbors.
- **soft** — The specified BGP neighbor(s) re-evaluates all routes in the Local-RIB against the configured export policies.
- **soft-inbound** — The specified BGP neighbor(s) re-evaluates all routes in the RIB-In against the configured import policies.
- **statistics** — The BGP neighbor statistics.

---

**protocol**

**Syntax**

```
protocol
```

**Context**

```
clear>router>bgp
```
**Show, Clear, Debug Commands**

**Description**
This command resets the entire BGP protocol. If the AS number was previously changed, the BGP AS number does not inherit the new value.

### id

**Syntax**
id service-id

**Context**
clear>service
clear>service>statistics

**Description**
This command clears commands for a specific service.

**Parameters**

- **service-id** — The ID that uniquely identifies a service.

  **Values**
  
  1 — 2147483648

### sap

**Syntax**
sap sap-id {all | counters | stp}

**Context**
clear>service>statistics

**Description**
Clears SAP statistics for a SAP.

**Parameters**

- **sap-id** — Specifies the physical port identifier portion of the SAP definition. See Common CLI Command Descriptions on page 1783 for command syntax.

### site

**Syntax**
site service-id

**Context**
clear>service>id

**Description**
This command clears site-specific information for the service.

**Parameters**

- **service-id** — Specifies the service ID or service name up to 64 characters in length.

  **Values**
  
  1 — 2147483648

### spoke-sdp

**Syntax**
spoke-sdp sdp-id:vc-id ingress-vc-label

**Context**
clear>service>id

**Description**
This command clears and resets the spoke SDP bindings for the service.

**Parameters**

- **sdp-id** — The spoke SDP ID to be reset.

  **Values**
  
  1 — 17407

- **vc-id** — The virtual circuit ID on the SDP ID to be reset.
VPRN Show Commands

Values 1 — 4294967295

sdp

Syntax sdp sdp-id keep-alive
Context clear>service>statistics
Description This command clears keepalive statistics associated with the SDP ID.
Parameters sdp-id — The SDP ID for which to clear keepalive statistics.
  Values 1 — 17407

counters

Syntax counters
Context clear>service>statistics>id
Description Clears all traffic queue counters associated with the service ID.

spoke-sdp

Syntax spoke-sdp sdp-id[:vc-id] {all | counters | stp}
Context clear>service>statistics>id
Description This command clears statistics for the spoke SDP bound to the service.
Parameters sdp-id — The spoke SDP ID for which to clear statistics.
  Values 1 — 17407
  vc-id — The virtual circuit ID on the SDP ID to be reset.
  Values 1 — 4294967295
  all — Clears all queue statistics and STP statistics associated with the SDP.
  counters — Clears all queue statistics associated with the SDP.
  stp — Clears all STP statistics associated with the SDP.

stp

Syntax stp
Context clear>service>statistics>id
Description Clears all spanning tree statistics for the service ID.
VPRN Debug Commands

id

Syntax  

[no] id service-id

Context  

default > service

Description  

This command debugs commands for a specific service.

The no form of the command disables debugging.

Parameters  

service-id — The ID that uniquely identifies a service.

arp-host

Syntax  

[no] arp-host

Context  

default > service > id

Description  

This command enables and configures ARP host debugging.

The no form of the command disables ARP host debugging.

host-connectivity-verify

Syntax  

[no] host-connectivity-verify

Context  

default > service > id

Description  

This command enables Subscriber Host Connectivity Verification (SHCV) debugging.

The no form of the command disables the SHCV debugging.

ip

Syntax  

[no] ip ip-address

Context  

default > service > id > host-connectivity-verify

Description  

This command displays Subscriber Host Connectivity Verification (SHCV) events for a particular IP address.

Parameters  

ip-address — The IP address of the IP interface. The ip-address portion of the address command specifies the IP host address that will be used by the IP interface within the subnet. This address must be unique within the subnet and specified in dotted decimal notation. Allowed values are IP addresses in the range 1.0.0.0 – 223.255.255.255 (with support of /31 subnets).
mac

Syntax: \[no\] mac ieee-address

Context: debug>service>id>host-connectivity-verify

Description: This command displays Subscriber Host Connectivity Verification (SHCV) events for a particular MAC address.

Parameters:

mac-address — Specifies the 48-bit MAC address for the static ARP in the form aa:bb:cc:dd:ee:ff or aa-bb-cc-dd-ee-ff where aa, bb, cc, dd, ee, and ff are hexadecimal numbers. Allowed values are any non-broadcast, non-multicast MAC and non-IEEE reserved MAC addresses.

sap

Syntax: \[no\] sap sap-id

Context: debug>service>id>host-connectivity-verify

Description: This command displays Subscriber Host Connectivity Verification (SHCV) events for a particular SAP.

Parameters:

sap-id — Specifies the physical port identifier portion of the SAP definition. See Common CLI Command Descriptions on page 1783 for command syntax.

sap

Syntax: \[no\] sap sap-id

Context: debug>service>id
debug>service>stp

Description: This command enables STP debugging for a specific SAP. The no form of the command disables debugging.

Parameters:

sap-id — Specifies the physical port identifier portion of the SAP definition. See Common CLI Command Descriptions on page 1783 for command syntax.

sdp

Syntax: \[no\] sdp sdp-id:vc-id

Context: debug>service>id
debug>service>stp

Description: This command enables STP debugging for a specific SDP. The no form of the command disables debugging.
event-type

Syntax  
[no] event-type {config-change | svc-oper-status-change | sap-oper-status-change | sdpbind-oper-status-change}

Context  
debug>service>id

Description  
This command enables debugging for a particular event type. The no form of the command disables debugging.

event-type

Syntax  
[no] event-type {config-change | oper-status-change}

Context  
debug>service>id>sap

Description  
This command enables debugging for a particular event type. The no form of the command disables debugging.

stp

Syntax  
[no] stp

Context  
debug>service>id

Description  
This command enables the context for debugging STP. The no form of the command disables debugging.

all-events

Syntax  
all-events

Context  
debug>service>id>event-type

Description  
This command enables STP debugging for all events. The no form of the command disables debugging.

bpdu

Syntax  
[no] bpdu

Context  
debug>service>stp

Description  
This command enables STP debugging for received and transmitted BPDUs. The no form of the command disables debugging.
core-connectivity

Syntax  [no] core-connectivity
Context  debug>service>stp
Description  This command enables STP debugging for core connectivity.
The no form of the command disables debugging.

exception

Syntax  [no] exception
Context  debug>service>stp
Description  This command enables STP debugging for exceptions.
The no form of the command disables debugging.

fsm-state-changes

Syntax  [no] fsm-state-changes
Context  debug>service>stp
Description  This command enables STP debugging for FSM state changes.
The no form of the command disables debugging.

fsm-timers

Syntax  [no] fsm-timers
Context  debug>service>stp
Description  This command enables STP debugging for FSM timer changes.
The no form of the command disables debugging.

port-role

Syntax  [no] port-role
Context  debug>service>stp
Description  This command enables STP debugging for changes in port roles.
The no form of the command disables debugging.
Show, Clear, Debug Commands

port-state

Syntax  [no] port-state
Context  debug>service>stp
Description  This command enables STP debugging for port states.
The no form of the command disables debugging.

igmp

Syntax  [no] igmp
Context  debug>router
Description  This command enables debugging for IGMP.
The no form of the command disables debugging.

interface

Syntax  [no] interface [ip-int-name | ip-address]
Context  debug>router>igmp
Description  This command enables debugging on the IGMP interface.
The no form of the command disables debugging.
Parameters  
ip-int-name — Only displays the information associated with the specified IP interface name.
ip-address — Only displays the information associated with the specified IP address.

Sample Output

A:FA# debug router 100 igmp interface
A:FA#
A:FA# show debug
debug
    router "100"
    igmp
    interface
    exit
exit
exit
"A:FA#
38397 2007/02/01 11:46:40.94 UTC MINOR: DEBUG #2001 vprn100 IGMP[85]
"IGMP[85]: INTF
Querier Timer expired on i/f 2"

38398 2007/02/01 11:46:40.94 UTC MINOR: DEBUG #2001 vprn100 IGMP[85]
"IGMP[85]: INTF
Sending query on i/f 2 to 0.0.0.0"

38399 2007/02/01 11:46:40.94 UTC MINOR: DEBUG #2001 vprn100 IGMP[85]
"IGMP[85]: INTF
Interface 2 already UP, ignoring event"

38400 2007/02/01 11:46:41.64 UTC MINOR: DEBUG #2001 vprn100 IGMP[85]
"IGMP[85]: INTF
Process received group rec MODE_IS_EXCL for i/f 2 group 225.1.1.1 in mode EXCLUD
E. Num srcs 0"

38401 2007/02/01 11:46:41.64 UTC MINOR: DEBUG #2001 vprn100 IGMP[85]
"IGMP[85]: INTF
Process received group rec MODE_IS_EXCL for i/f 2 group 225.1.1.2 in mode EXCLUD
E. Num srcs 0"

38402 2007/02/01 11:46:41.64 UTC MINOR: DEBUG #2001 vprn100 IGMP[85]
"IGMP[85]: INTF
Process received group rec MODE_IS_EXCL for i/f 2 group 225.1.1.3 in mode EXCLUD
E. Num srcs 0"

38403 2007/02/01 11:46:41.64 UTC MINOR: DEBUG #2001 vprn100 IGMP[85]
"IGMP[85]: INTF
Process received group rec MODE_IS_EXCL for i/f 2 group 225.1.1.4 in mode EXCLUD
E. Num srcs 0"

38404 2007/02/01 11:46:41.64 UTC MINOR: DEBUG #2001 vprn100 IGMP[85]
"IGMP[85]: INTF
Process received group rec MODE_IS_EXCL for i/f 2 group 225.1.1.5 in mode EXCLUD
E. Num srcs 0"

38405 2007/02/01 11:46:48.93 UTC MINOR: DEBUG #2001 vprn100 IGMP[85]
"IGMP[85]: INTF
Process received group rec MODE_IS_EXCL for i/f 2 group 225.1.1.1 in mode EXCLUD
E. Num srcs 0"

38408 2007/02/01 11:46:48.93 UTC MINOR: DEBUG #2001 vprn100 IGMP[85]
"IGMP[85]: INTF
Process received group rec MODE_IS_EXCL for i/f 2 group 225.1.1.4 in mode EXCLUD
E. Num srcs 0"

38409 2007/02/01 11:46:48.93 UTC MINOR: DEBUG #2001 vprn100 IGMP[85]
"IGMP[85]: INTF
Process received group rec MODE_IS_EXCL for i/f 2 group 225.1.1.5 in mode EXCLUD
E. Num srcs 0"

38410 2007/02/01 11:46:48.93 UTC MINOR: DEBUG #2001 vprn100 IGMP[85]
"IGMP[85]: INTF
Interface 2 already UP, ignoring event"

A:FA#

**MCS**

**Syntax**  
[no] mcs [ip-int-name]

**Context**  
debug>router>igmp

**Description**  
This command enables debugging for IGMP MCS. The no form of the command disables debugging.

**Parameters**  
*ip-int-name* — Only displays the information associated with the specified IP interface name.

**Sample Output**
misc

Syntax  [no] misc

Context  debug>router>igmp

Description  This command enables debugging for IGMP miscellaneous. The no form of the command disables debugging.

Sample Output

A:BA# debug router 100 igmp misc
A:BA# show debug
debug
    router "100"
    igmp
    misc
    exit
    exit
    exit
A:BA#

packet

Syntax  [no] packet [query|v1-report|v2-report|v3-report|v2-leave] [ip-int-name | ip-address]

Context  debug>router>igmp

Description  This command enables debugging for IGMP packets. The no form of the command disables debugging.

Parameters  query v1/v2/v3-report, v2-leave — Select the type of packet to debug.
            ip-int-name — Only displays the information associated with the specified IP interface name.
            ip-address — Only displays the information associated with the specified IP address.

Sample Output

A:BA# debug router 100 igmp packet
A:BA#
A:BA# show debug
debug
router "100"
  igmp
    packet
  exit
exit

5 2006/09/03 22:20:05.73 UTC MINOR: DEBUG #2001 vprn100 IGMP[2]
"IGMP[2]: TX-PKT
[000 18:25:24.480] ifId:2 fName:IGMP_to_CE IGMP V3 PDU: 11.1.1.1 -> 224.0.0.1 pduLen 12
  Type: QUERY maxrespCode 0xa checkSum 0xec78
  GroupAddr: 0.0.0.0
    S bit 0, QRV 2, QQIC 125, NumSources 0
  Source Address List:
"n
6 2006/09/03 22:20:05.96 UTC MINOR: DEBUG #2001 vprn100 IGMP[2]
"IGMP[2]: RX-PKT
[000 18:25:24.710] ifId:2 fName:IGMP_to_CE IGMP V3 PDU: 11.1.1.20 -> 224.0.0.22 pduLen 48
  Type: V3 REPORT maxrespCode 0x0 checkSum 0x5fe2
  Num Group Records: 4
  Group Record 0
    Type: CHG_TO_EXCL, AuxDataLen 0, Num Sources 0
    Mcast Addr: 225.1.1.1
    Source Address List
  Group Record 1
    Type: CHG_TO_EXCL, AuxDataLen 0, Num Sources 0
    Mcast Addr: 225.1.1.2
    Source Address List
  Group Record 2
    Type: CHG_TO_EXCL, AuxDataLen 0, Num Sources 0
    Mcast Addr: 225.1.1.3
    Source Address List
  Group Record 3
    Type: CHG_TO_EXCL, AuxDataLen 0, Num Sources 0
    Mcast Addr: 225.1.1.4
    Source Address List
A:BA#
*A:BA# no debug
Trace disabled for all existing and future clients
*A:BA# show debug
debug
exit
Show, Clear, Debug Commands
Common CLI Command Descriptions

In This Chapter

This section provides information about common Command Line Interface (CLI) syntax and command usage.

Topics in this chapter include:

• SAP syntax on page 1784
Common Service Commands

sap

Syntax  
[no] sap sap-id

Description  
This command specifies the physical port identifier portion of the SAP definition.

Parameters  
sap-id — Specifies the physical port identifier portion of the SAP definition.

The sap-id can be configured in one of the following formats:

<table>
<thead>
<tr>
<th>Type</th>
<th>Syntax</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>port-id</td>
<td>slot/mda/port[.channel]</td>
<td>1/1/5</td>
</tr>
<tr>
<td>null</td>
<td>[port-id</td>
<td>lag-id ]</td>
</tr>
<tr>
<td>dot1q</td>
<td>[port-id</td>
<td>lag-id]:qtag1</td>
</tr>
<tr>
<td>qinq</td>
<td>[port-id</td>
<td>lag-id]:qtag1.qtag2</td>
</tr>
</tbody>
</table>

The values depend on the encapsulation type configured for the interface. The following table describes the allowed values for the port and encapsulation types.

<table>
<thead>
<tr>
<th>Port Type</th>
<th>Encap-Type</th>
<th>Allowed Values</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet</td>
<td>Null</td>
<td>0</td>
<td>The SAP is identified by the port.</td>
</tr>
<tr>
<td>Ethernet</td>
<td>Dot1q</td>
<td>0 — 4094</td>
<td>The SAP is identified by the 802.1Q tag on the port. Note that a 0 qtag1 value also accepts untagged packets on the dot1q port.</td>
</tr>
<tr>
<td>Ethernet</td>
<td>QinQ</td>
<td>qtag1: 0 — 4094 qtag2: 0 — 4094</td>
<td>The SAP is identified by two 802.1Q tags on the port. Note that a 0 qtag1 value also accepts untagged packets on the Dot1q port.</td>
</tr>
<tr>
<td>SONET/SDH</td>
<td>IPCP</td>
<td>-</td>
<td>The SAP is identified by the channel. No BCP is deployed and all traffic is IP.</td>
</tr>
<tr>
<td>SONET/SDH</td>
<td>BCP-Null</td>
<td>0</td>
<td>The SAP is identified with a single service on the channel. Tags are assumed to be part of the customer packet and not a service delimiter.</td>
</tr>
</tbody>
</table>
SONET/SDH  BCP-Dot1q  0 — 4094

The SAP is identified by the 802.1Q tag on the channel.
Standards and Protocol Support

**Ethernet Standards**

IEEE 802.1ab-REV/D3 Station and Media Access Control Connectivity Discovery
IEEE 802.1d Bridging
IEEE 802.1p/Q VLAN Tagging
IEEE 802.1s Multiple Spanning Tree
IEEE 802.11w Rapid Spanning Tree Protocol
IEEE 802.1x Port Based Network Access Control
IEEE 802.1ad Provider Bridges
IEEE 802.1ah Provider Backbone Bridges
IEEE 802.1ag Service Layer OAM
IEEE 802.3ah Ethernet in the First Mile
IEEE 802.1ak Multiple MAC Registration Protocol
IEEE 802.3 10BaseT
IEEE 802.3ad Link Aggregation
IEEE 802.3ae 10Gbps Ethernet
IEEE 802.3ah Ethernet OAM
IEEE 802.3u 100BaseTX
IEEE 802.3x Flow Control
IEEE 802.3z 100BaseSX/LX
ITU-T G.1731 OAM functions and mechanisms for Ethernet based networks
ITU-T G.8031 Ethernet linear protection switching
ITU-T G.8032 Ethernet Ring Protection Switching (version 2)

**BGP**

RFC 1397 BGP Default Route Advertisement
RFC 1772 Application of BGP in the Internet
RFC 1965 Confederations for BGP
RFC 1997 BGP Communities Attribute
RFC 2385 Protection of BGP Sessions via MD5
RFC 2439 BGP Route Flap Dampening
RFC 2558 Multiprotocol Extensions for BGP-4
RFC 2918 Route Refresh Capability for BGP-4
RFC 3107 Carrying Label Information in BGP-4
RFC 3392 Capabilities Advertisement with BGP4
RFC 4271 BGP-4 (previously RFC 1771)
RFC 4360 BGP Extended Communities Attribute
RFc 4364 BGP/MPLS IP Virtual Private Networks (VPNs)(previously RFC 2547bis BGP/MPLS VPNs)
RFC 4456 BGP Route Reflection: Alternative to Full-mesh IBGP (previously RFC 1966 & 2796)
RFC 4486 Subcodes for BGP Cease Notification Message
RFC 4577 BGP as the Provider/ Customer Edge Protocol for BGP/ MPLS IP Virtual Private Networks (VPNs)
RFC 4659 BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN
RFC 4684 Constrained Route Distribution for Border Gateway Protocol/MultiProtocol Label Switching (BGP/MPLS) Internet Protocol (IP) Virtual Private Networks (VPNs)
RFC 4724 Graceful Restart Mechanism for BGP – GR helper
RFC 4760 Multi-protocol Extensions for BGP
RFC 4798 Connecting IPv6 Islands over IPv4 MPLS Using IPv6 Provider Edge Routers (6PE)
RFC 4893 BGP Support for Four-octet AS Number Space
RFC 5004 Avoid BGP Best Path Transitions from One External to Another
RFC 5065 Confederations for BGP (obsoletes 3065)
RFC 5291 Outbound Route Filtering Capability for BGP-4
RFC 5575 Dissemination of Flow Specification Rules
RFC 5668 4-Octet AS Specific BGP Extended Community
draft-ietf-idr-add-paths
draft-ietf-idr-best-external

**IS-IS**

RFC 1195 Use of OSI IS-IS for Routing in TCP/IP and Dual Environments
RFC 2973 IS-IS Mesh Groups
RFC 3359 Reserved Type, Length and Value (TLV) Codepoints in Intermediate System to Intermediate System
RFC 3719 Recommendations for Interoperable Networks using Intermediate System to Intermediate System (IS-IS)
RFC 3787 Recommendations for Interoperable IP Networks using
RFC 5120 M-ISIS: Multi Topology (MT) Routing in IS-IS (Partial)
RFC 5301 Dynamic Hostname Exchange Mechanism for IS-IS
RFC 5302 Domain-wide Prefix Distribution with Two-Level IS-IS
RFC 5303 Three-Way Handshake for IS-IS Point-to-Point Adjacencies
RFC 5304 IS-IS Cryptographic Authentication
RFC 5305 IS-IS Extensions for Traffic Engineering TE
RFC 5306 Restart Signaling for IS-IS
RFC 5307 IS-IS Extensions in Support of Generalized Multi-Protocol Label Switching (GMPLS)
RFC 5308 IS-IS Extensions over LAN in Link State Routing
RFC 6329 IS-IS Extensions Supporting IEEE 802.1aq Shortest Path Bridging (Partial)
draft-ietf-isis-mi IS-IS Multi-Instance

IPSec
RFC 2401 Security Architecture for the Internet Protocol
RFC 2406 IP Encapsulating Security Payload (ESP)
RFC 2409 The Internet Key Exchange (IKE)
RFC 2560 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP
RFC 3706 IKE Dead Peer Detection
RFC 3947 Negotiation of NAT-Traversal in the IKE
RFC 3948 UDP Encapsulation of IPsec ESP Packets
RFC 4210 Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)
RFC 4211 Internet X.509 Public Key Infrastructure Certificate Request Message Format (CRMF)
RFC 5996 Internet Key Exchange Protocol Version 2 (IKEv2)
RFC 5998 An Extension for EAP-Only Authentication in IKEv2
draft-ietf-ipsec-isakmp-xauth-06.txt – Extended Authentication within ISAKMP/Oakley (XAUTH)
draft-ietf-ipsec-isakmp-modecfg-05.txt – The ISAKMP Configuration Method

IPv6
RFC 1981 Path MTU Discovery for IPv6
RFC 2375 IPv6 Multicast Address Assignments
RFC 2460 Internet Protocol, Version 6 (IPv6) Specification
RFC 2461 Neighbor Discovery for IPv6
RFC 2462 IPv6 Stateless Address Auto configuration
RFC 2463 Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 Specification
RFC 2464 Transmission of IPv6 Packets over Ethernet Networks
RFC 2529 Transmission of IPv6 over IPv4 Domains without Explicit Tunnels
RFC 2545 Use of BGP-4 Multiprotocol Extension for IPv6 Inter-Domain Routing
RFC 2710 Multicast Listener Discovery (MLD) for IPv6
RFC 2740 OSPF for IPv6
RFC 3306 Unicast-Prefix-based IPv6 Multicast Addresses
RFC 3315 Dynamic Host Configuration Protocol for IPv6
RFC 3587 IPv6 Global Unicast Address Format
RFC3590 Source Address Selection for the Multicast Listener Discovery (MLD) Protocol
RFC 3810 Multicast Listener Discovery Version 2 (MLDv2) for IPv6
RFC 4007 IPv6 Scoped Address Architecture
RFC 4193 Unique Local IPv6 Unicast Addresses
RFC 4291 IPv6 Addressing Architecture
RFC 4552 Authentication/Confidentiality for OSPFv3
RFC 4659 BGP/MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN

Multicast
RFC 1112 Host Extensions for IP Multicasting (Snooping)
RFC 2236 Internet Group Management Protocol, (Snooping)
RFC 3376 Internet Group Management Protocol, Version 3 (Snooping)
RFC 2362 Protocol Independent Multicast-Sparse Mode (PIMSM)
RFC 3618 Multicast Source Discovery Protocol (MSDP)
RFC 3446 Anycast Rendezvous Point (RP) mechanism using Protocol Independent Multicast (PIM) and Multicast Source Discovery Protocol (MSDP)
RFC 4604 Using IGMPv3 and MLDv2 for Source-Specific Multicast
RFC 4607 Source-Specific Multicast for IP
RFC 4608 Source-Specific Protocol Independent Multicast in 232/8
RFC 4610 Anycast-IP Using Protocol Independent Multicast (PIM)
draft-ietf-pim-sm-bsr-06.txt
draft-rosen-vpn-mcast-15.txt Multicast in MPLS/BGP IP VPNs
draft-ietf-mboned-msdp-mib-01.txt
draft-ietf-l3vpn-2547bis-mcast-07: Multicast in MPLS/BGP IP VPNs
draft-ietf-l3vpn-2547bis-mcast-bgp-05: BGP Encodings and Procedures for Multicast in MPLS/BGP IP VPNs
RFC 3956: Embedding the Rendezvous Point (RP) Address in an IPv6 Multicast Address

MPLS
RFC 2430 A Provider Architecture DiffServ & TE
RFC 2474 Definition of the DS Field the IPv4 and IPv6 Headers (Rev)
RFC 2597 Assured Forwarding PHB Group (rev3260)
RFC 2598 An Expedited Forwarding PHB
RFC 3031 MPLS Architecture
RFC 3032 MPLS Label Stack Encoding
RFC 3443 Time To Live (TTL) Processing in Multi-Protocol Label Switching (MPLS) Networks
RFC 4182 Removing a Restriction on the use of MPLS Explicit NULL
RFC 3140 Per-Hop Behavior Identification Codes
RFC 5332 MPLS Multicast Encapsulations

MPLS — LDP
RFC 3037 LDP Applicability
RFC 3478 Graceful Restart Mechanism for LDP – GR helper
RFC 5036 LDP Specification
RFC 5283 LDP extension for Inter-Area LSP
RFC 5443 LDP IGP Synchronization
RFC 6388 LDP Extensions for Point-to-Multipoint and Multipoint-to-Multipoint LSP
RFC 6826 Multipoint LDP in-band signaling for Point-to-Multipoint and Multipoint-to-Multipoint Label Switched Paths
draft-pdutta-mls-ldp-hello-reduce-04.txt, Targeted LDP Hello Reduction

MPLS/RSVP-TE
RFC 2702 Requirements for Traffic Engineering over MPLS
RFC 2747 RSVP Cryptographic Authentication
RFC 2961 RSVP Refresh Overhead Reduction Extensions
RFC 3097 RSVP Cryptographic Authentication - Updated Message Type Value
RFC 3209 Extensions to RSVP for Tunnels
RFC 3477 Signalling Unnumbered Links in Resource ReSerVation Protocol - Traffic Engineering (RSVP-TE)
RFC 3564 Requirements for Diff-Serv-aware TE
RFC 3906 Calculating Interior Gateway Protocol (IGP) Routes Over Traffic Engineering Tunnels
RFC 4090 Fast reroute Extensions to RSVP-TE for LSP Tunnels
RFC 4124 Protocol Extensions for Support of DiffServ-aware MPLS Traffic Engineering
RFC 4125 Maximum Allocation Bandwidth Constraints Model for DiffServ-aware MPLS Traffic Engineering
RFC 4127 Russian Dolls Bandwidth Constraints Model for DiffServ-aware MPLS Traffic Engineering
draft-newton-mps-to-dynamic-overbooking-00 A DiffServ-TE Implementation Model to dynamically change booking factors during failure events
RFC 4561 Definition of a RRO Node-Id Sub-Object
RFC 4875 Extensions to Resource Reservation Protocol - Traffic Engineering (RSVP-TE) for Point-to-Multipoint TE Label Switched Paths (LSPs)
RFC 5151 Inter-domain MPLS and GMPLS Traffic Engineering – RSVP-TE Extensions
RFC 5712 MPLS Traffic Engineering Soft Preemption
RFC 5817 Graceful Shutdown in GMPLS Traffic Engineering Networks

MPLS — OAM
RFC 4379 Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures
RFC 6425 Detecting Data Plane Failures in Point-to-Multipoint Multiprotocol

MPLS-TP
RFC 5586 MPLS Generic Associated Channel
RFC 5921 A Framework for MPLS in Transport Networks
RFC 5960 MPLS Transport Profile Data Plane Architecture
RFC 6370 MPLS-TP Identifiers
RFC 6378 MPLS-TP Linear Protection
RFC 6428 Proactive Connectivity Verification, Continuity Check and Remote Defect indication for MPLS Transport Profile
RFC 6426 MPLS On-Demand Connectivity and Route Tracing
RFC 6478 Pseudowire Status for Static Pseudowires
draft-ietf-mpls-tp-ethernet-addressing-02 MPLS-TP Next-Hop Ethernet Addressing

RIP
RFC 1058 RIP Version 1
RFC 2082 RIP-2 MD5 Authentication
RFC 2453 RIP Version 2

TCP/IP
RFC 768 UDP
RFC 1350 The TFTP Protocol (Rev.
RFC 791 IP
RFC 792 ICMP
RFC 793 TCP
RFC 826 ARP
RFC 854 Telnet
RFC 951 BootP (rev)
RFC 1519 CIDR
RFC 1542 Clarifications and Extensions for the Bootstrap Protocol
RFC 1812 Requirements for IPv4 Routers
RFC 2347 TFT option Extension
RFC 2328 TFT Blocksize Option
RFC 2349 TFT Timeout Interval and Transfer Size option
RFC 2401 Security Architecture for Internet Protocol
RFC 2428 FTP Extensions for IPv6 and NATs
RFC 3596 DNS Extensions to Support IP version 6
Standards and Protocols

draft-ietf-bfd-mib-00.txt Bidirectional Forwarding Detection Management Information Base
RFC 5880 Bidirectional Forwarding Detection
RFC 5881 BFD IPv4 and IPv6 (Single Hop)
RFC 5883 BFD for Multihop Paths
RFC 5286 Basic Specification for IP Fast Reroute: Loop-Free Alternates

VRRP
RFC 2787 Definitions of Managed Objects for the Virtual Router Redundancy Protocol
RFC 3768 Virtual Router Redundancy Protocol

PPP
RFC 1332 PPP IPCP
RFC 1377 PPP OSINLCP
RFC 1638/2878PPP BCP
RFC 1661 PPP (rev RFC2151)
RFC 1662 PPP in HDLC-like Framing
RFC 1877 PPP Internet Protocol Control Protocol Extensions for Name Server Addresses
RFC 1989 PPP Link Quality Monitoring
RFC 1990 The PPP Multilink Protocol (MP)
RFC 1994 "PPP Challenge Handshake Authentication Protocol (CHAP)
RFC 2516 A Method for Transmitting PPP Over EthernetRFC 2615 PPP over SONET/SDH
RFC 2686 The Multi-Class Extension to Multi-Link PPP

Frame Relay
FRF.1.2 - PVC User-to-Network Interface (UNI) Implementation Agreement
FRF.5 - Frame Relay/ATM PVC Network Interworking Implementation
FRF2.2 - PVC Network-to-Network Interface (NNI) Implementation Agreement.
FRF.12 Frame Relay Fragmentation Implementation Agreement
FRF.16.1 Multilink Frame Relay UNI/NNI Implementation Agreement
ITU-T Q.933 Annex A- Additional procedures for Permanent Virtual Connection (PVC) status management

ATM
RFC 1626 Default IP MTU for use over ATM AAL5
RFC 2514 Definitions of Textual Conventions and OBJECT_IDENTITIES for ATM Management
RFC 2515 Definition of Managed Objects for ATM Management RFC 2684 Multiprotocol Encapsulation over ATM Adaptation Layer 5
AF-TM-0121.000 Traffic Management Specification Version 4.1
ITU-T Recommendation I.610 - B-ISDN Operation and Maintenance Principles and Functions version 11/95
ITU-T Recommendation I.432.1 – BISDN user-network interface – Physical layer specification: General characteristics
GR-1248-CORE - Generic Requirements for Operations of ATM Network Elements (NEs). Issue 3
GR-1113-CORE - Bellcore, Asynchronous Transfer Mode (ATM) and ATM Adaptation Layer (AAL) Protocols Generic Requirements, Issue 1
AF-ILMI-0065.000 Integrated Local Management Interface (ILMI) Version 4.0
AF-TM-0150.00 Addendum to Traffic Management v4.1 optional minimum desired cell rate indication for UBR
AF-PHY-0086.001, Inverse Multiplexing for ATM (IMA) Specification Version 1.1

DHCP
RFC 2131 Dynamic HostConfiguration Protocol (REV)
RFC 3046 DHCP Relay Agent Information Option (Option 82)

RFC 1534 Interoperation between DHCP and BOOTP

Policy Management and Credit Control
3GPP TS 29.212 - Policy and Charging Control (PCC) over Gx/Sd Reference Point (Release 11) - Gx support as it applies to wireline environment (BNG)
RFC 3588 – Diameter Base Protocol
RFC 4006 – Diameter Credit Control Application

NAT
RFC 6333 Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion
RFC 6334 Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Option for Dual-Stack Lite
RFC 6888 Common Requirements For Carrier-Grade NATs (CGNs)
RFC 5508 NAT Behavioral Requirements for ICMP
RFC 5382 NAT Behavioral Requirements for TCP
RFC 6146 Statefull NAT64

VPLS
RFC 4762 Virtual Private LAN Services Using LDP
RFC 5501: Requirements for Multicast Support in Virtual Private LAN Services (previously draft-ietf-l2vpn-vpls-mcast-reqts-04)
RFC 6074: Provisioning, Auto-Discovery, and Signaling in Layer 2 Virtual Private Networks (L2VPNs) (previously draft-ietf-l2vpn-signaling-08)
draft-ietf-l2vpn-vpls-mcast-13.txt Multicast in VPLS
RFC 7041 Extensions to the Virtual Private LAN Service (VPLS) Provider Edge (PE) Model for Provider Backbone Bridging
RFC 7117 Multicast in Virtual Private LAN Service (VPLS)

Pseudowire
RFC 3985 Pseudo Wire Emulation Edge-to-Edge (PWE3)
RFC 4385 Pseudo Wire Emulation Edge-to-Edge (PWE3) Control Word for Use over an MPLS PSN
RFC 3916 Requirements for Pseudo-Wire Emulation Edge-to-Edge (PWE3)
RFC 4717 Encapsulation Methods for Transport ATM over MPLS Networks (draft-ietf-pwe3-atm-encap-10.txt)
RFC 4816 PWE3 ATM Transparent Cell Transport Service (draft-ietf-pwe3-cell-transport-04.txt)
RFC 4448 Encapsulation Methods for Transport of Ethernet over MPLS Networks (draft-ietf-pwe3-ethernet-encap-11.txt)
RFC 4619 Encapsulation Methods for Transport of Frame Relay over MPLS Networks (draft-ietf-pwe3-frame-relay-10.txt)
RFC 5085, Pseudowire Virtual Circuit Connectivity Verification (VCCV): A Control Channel for Pseudowires
RFC 5659 An Architecture for Multi-Segment Pseudowire Emulation Edge-to-Edge
draft-ietf-ancp-protocol-02.txt ANCP Protocol
MFA Forum 12.0.0 Multiservice Interworking - Ethernet over MPLS
MFA forum 13.0.0 - Fault Management for Multiservice Interworking v1.0
MFA Forum 16.0.0 – Multiservice Interworking - IP over MPLS
RFC5851 ANCP framework
draft-ietf-ancp-protocol-02.txt ANCP Protocol
VOICE / VIDEO PERFORMANCE:
ITU-T Rec. P.564 - Conformance testing for voice over IP transmission quality assessment models
ITU-T G1020 - Appendix I- Performance Parameter Definitions for Quality of Speech and other Voiceband Applications Utilizing IP Networks- Mean Absolute Packet Delay Variation & Markov Models.
RFC 4553 Structure-Agnostic Time Division Multiplexing (TDM) over Packet (SAToP)
RFC 5086 Structure-Aware Time Division Multiplexed (TDM) Circuit Emulation Service over Packet Switched Network (CESoPSN)
MFA Forum 9.0.0 The Use of Virtual trunks for ATM/MPLS Control Plane Interworking
SONET/SDH
ITU-G841 Telecommunication Standardization Section of ITU, Types and Characteristics of SDH Networks Protection Architecture, issued in October 1998 and as augmented by Corrigendum1 issued in July 2002
AAA
RFC 2865 Remote Authentication Dial In User Service
RFC 2866 RADIUS Accounting
draft-grant-tacacs-02.txt
SSH
RFC 4250 The Secure Shell (SSH) Protocol Assigned Numbers
RFC 4251 The Secure Shell (SSH) Protocol Architecture
RFC 4254 The Secure Shell (SSH) Connection Protocol
OpenFlow
ONF OpenFlow Switch Specification version 1.3.1 (Hybrid-switch/FlowTable)
Timing
ITU-T G781 Telecommunication Standardization Section of ITU, Synchronization layer functions, issued 09/2008
ITU-T G813 Telecommunication Standardization Section of ITU, Timing characteristics of SDH equipment slave clocks (SEC), issued 03/2003.

Standards and Protocols

ITU-T G.8265.1 Telecommunication Standardization Section of ITU, Precision time protocol telecom profile for frequency synchronization, issued 10/2010.


Network Management
ITU-T X.721: Information technology-OSI-Structure of Management Information
ITU-T X.734: Information technology-OSI-Systems Management: Event Report Management Function
M.3100/3120 Equipment and Connection Models
TMF 509/613 Network Connectivity Model
RFC 1157 SNMPv1
RFC 1215 A Convention for Defining Traps for use with the SNMP
RFC 1657 BGP4-MIB
RFC 1724 RIPv2-MIB
RFC 1850 OSPF-MIB
RFC 1907 SNMPv2-MIB
RFC 2011 IP-MIB
RFC 2138 RADIUS
RFC 2206 RSVP-MIB
RFC 2452 IPv6 Management Information Base for the Transmission Control Protocol
RFC 2465 Management Information Base for IPv6: Textual Conventions and General Group
RFC 2558 SONET-MIB
RFC 2571 SNMP-FRAMEWORKMIB
RFC 2572 SNMP-MPD-MIB
RFC 2573 SNMP-TARGET-&-NOTIFICATION-MIB
RFC 2574 SNMP-USER-BASED-SNMP
RFC 2575 SNMP-VIEW-BASED-ACM-MIB
RFC 2576 SNMP-COMMUNITY-MIB
RFC 2578 Structure of Management Information Version 2 (SMIv2)
RFC 2665 EtherLike-MIB
RFC 2819 RMON-MIB
RFC 2863 IF-MIB
RFC 2864 INVERTED-STACK-MIB
RFC 2987 VRRP-MIB
RFC 3014 NOTIFICATION-LOGMIB
RFC 3019 IP Version 6 Management Information Base for The Multicast Listener Discovery Protocol
RFC 3164 Syslog
RFC 3273 HRMON-MIB
RFC 3412 - Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
RFC 3413 - Simple Network Management Protocol (SNMP) Applications
RFC 3414 - User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)
RFC 3418 - SNMP MIB
RFC 3826 The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model
RFC 4113 Management Information Base for the User Datagram Protocol (UDP)
RFC 4292 IP-FORWARD-MIB
RFC 4293 MIB for the Internet Protocol
RFC 6241: NETCONF Configuration Protocol
RFC 6242 Using the NETCONF Protocol over Secure Shell (SSH)

draft-ietf-ospf-mib-update-04.txt
draft-ietf-mpls-lsr-mib-06.txt
draft-ietf-mpls-te-mib-04.txt
draft-ietf-mpls-ldp-mib-07.txt
draft-ietf-isis-wg-mib-06 Management Information Base for Intermediate System to Intermediate System (IS-
Index

A

Apipe
283
configuring 430
overview 283
SAP 433
SDP 437
traffic management support 287

C

circuit emulation services
parameters 293
configuration
basic service 101
control words 464
Cpipe
configuring
create a service 439
creating a service 439
payload 299
SAP 442
customers 44, 103

D
default SAP 49
DEI in IEEE 802.1ad 736
deploying and provisioning services 97
DHCP
CLI 1028

E
egress multicast groups 757
encapsulation types
Ethernet 46
SAPs 46

Epipe
overview 301
SAPs
filter policies 426
MAC Resources 426
QoS policies 426
SDPs 420
configuring 444
creating a service 444
SDPs 452
SAP 445
distributed 448
local 446
SDP 452
with PBB 303
ETH-CFM 112
Ethernet Ring Sub-Rings 84
EVPN 683
configuring 707
overview 684
VXLAN 685, 687

F

Fpipe
309
overview 309
SAP 456
SDP 458
traffic management support 313

G

G.8031 Protected Ethernet Tunnels 70
G.8032 Ethernet Ring Protection Switching 77

I

IEEE 802.1ah PBB 1189
access MH for native PBB 1250
deploying and provisioning services 97
example network configuration 1215
features 1191
ISID policies 1211
ISID policy control 1213
MAC flush 1240
MRRP 1223
overview 1190
   SPBM to non-SPBM interworking 1209
packet walkthrough 1198
PBB and BGP-AD 1230
PBB and IGMP snooping 1263
PBB eline 1230
PBB OAM 1280
PBB using G.8031p Protected Ethernet tunnels 1231
SAP and SDP support 1196
SPBM 1200

IES
overview 1348
   filter policies 1377
   IP interfaces 1349, 1625
   QoS policies 1377
   routing protocols 1376
   SAP encapsulation 1367
configuring
   creating a service 1396
   IES interface 1398
management tasks 1406
SAPs on IES interface 1400
VRRP on IES interface 1403

Ipipe
314
configuring 460
creating
   management tasks 484
overview 314
SAP 460
SDP 463

IPv6 Support on IP Interworking VLL 324

M
MAC flush message processing 789
MC-APS and MC-LAG 405
multi-service sites 105

P
PBB
   Epipe configuration 450
pseudowire
   configurations 467
   control word 738
   redundancy 356
   redundancy service models 397
   switching 335
   switching behavior 339

R
routed VPLS 824

S
SAPs
   overview 44
   configuration considerations 51
   encapsulation and pseudowire types 422
   encapsulation types
      Ethernet 46
      SONET/SDH
         BCP-dot1q 46, 47
         BCP-null 46, 47
         IPCP 46, 47
SDPs
   overview
      keepalives 57
      spoke and mesh 56
service
   access points (SAP) 44
   distribution points (SDPs) 53
   types 35
Services
   Epipe 301
   IES 1348
   multi-service sites 69
   VPLS 727
   VPRN 1607
   Apipe 283
configuring
   SDPs 107
Cpipe (CES) 289
entities
    multi-service sites 69
Fpipe 309
Ipipe 314

Services command reference
    Apipe 503
    Cpipe 509
    Epipe 512
    Fpipe 523
    Internet Enhances Service (IES) 1411
    Ipipe 526
    Provider Backbone Bridging (PBB) 1317
    Virtual Leased Line (VLL) 503
    Virtual Private LAN Service (VPLS) 711, 935
    Virtual Private Routed Network 1725

split horizon groups 731, 747, 880, 897

SRRP 1380
    instance 1389
    messaging 1386
    multi-chassis synchronization 1388

T

T-LDP 401

V

VLL
    Ethernet Interworking 305
    G.8031 protected Ethernet tunnels 408
    ingress VLAN swapping 342
    MC-LAG and pseudowire redundancy 392
    pseudowire redundancy 344
    pseudowire switching 335
    resilience 363

VPLS
    overview 727
        MAC learning 733
        packet walkthrough 728
        STP 748
        VPLS over MPLS 732
    access redundancy 785
    configuring

basic 854
creating a service 859
management tasks 930
SAP 870
    distributed 871
    local 870
SDP bindings 885
TSTP bridge parameters 864

BGP 806
BGP multi-homing 813
G.8031 protected Ethernet tunnels 737
multicast-aware 818
redundancy 769

VPRN
    overview
        BGP support 1610
        IP filter policies 1640
        QoS policies 1640
        route distinguishers 1611
        route redistribution 1615
        route reflectors 1614
        routing prerequisites 1609
        SAP encapsulations 1639
tunneling mechanisms 1644
    configuring
        basic 1698
        create a service 455, 1701
        interface 1713, 1717
            SAP 1719
        management tasks 1721
        protocols
            BGP 1706
            RIP 1710
IP-VPNs 1648
    cflowd 1650
    MDTs 1670
    multicast 1668
    OSPF 1648
    Option-C 1651
    RIP 1663
    SAPs 1639
    spoke SDPs 1645