## Table of Contents

**Preface** ................................................................. 11

**ISA-MS Hardware**
- ISA-MS Overview ....................................................... 16
- Application Assurance Hardware Features .......................... 17
  - AA ISA Host System Support ....................................... 17
  - IOM Support for AA ISA ........................................... 18

**Application Assurance**
- Application Assurance (AA) Overview ............................... 22
  - Application Assurance: Inline Policy Enforcement ............ 23
  - AA for Residential Subscriber Edge and VPN PE ............... 24
  - Fixed Residential Broadband Services .......................... 26
  - Application-Aware Business VPN Services ....................... 27
  - AA in Dual Stack Residential Deployment ........................ 29
    - AA in Dual Stack Business VPN Deployment .................... 30
  - Adjunct Off-line Content Processing ............................. 31
- Application Assurance System Architecture ....................... 33
  - AA ISA Resource Configuration ................................. 33
  - AA ISA Groups and Partitions .................................. 33
    - Multiple AA ISA Groups .................................... 33
    - AA Group Partitions ......................................... 35
    - Bypass Modes ................................................. 36
  - Redundancy .......................................................... 37
    - No AA ISA Group Redundancy .................................. 37
    - Failure to Fabric .............................................. 37
    - N+1 AA ISA Card Warm Redundancy ............................. 37
- ISA Load Balancing .................................................... 39
  - Transit Prefix Policy .............................................. 40
    - static-remote-aa-sub Command ................................ 40
    - Transit AA-sub Persistence .................................... 42
    - Policers for Prefix Transit AAsubs ........................... 42
- ISA Overload Detection ................................................ 43
- AA Packet Processing .................................................. 45
  - Divert of Traffic and Subscribers ............................... 46
    - Services and AA Subscribers .................................. 47
    - Spoke SDPs ..................................................... 49
    - Transit AA Subs ................................................ 49
    - AA Subscriber Application Service Definition ................ 49
  - Application Identification ........................................ 64
    - Application Assurance Identification Components ............ 66
      - Protocol Signatures ........................................... 68
      - Custom Protocols ............................................. 69
      - Protocol Shutdown ............................................ 70
      - Supported Protocol Signatures ............................... 71
      - Application Groups .......................................... 71
# Table of Contents

Applications .................................................................................................................. 71
Application Filters ......................................................................................................... 72
Statistics and Accounting ............................................................................................... 73
  Per-AA-Subscriber Special Study .................................................................................. 73
  System Aspects .............................................................................................................. 74
  Configurable AA-Subscriber Statistics Collection ...................................................... 80
  AA-Performance Record for ISA Load ......................................................................... 81
  Cflowd AA Records .................................................................................................... 83
Policy Actions .................................................................................................................. 85
  Application Assurance Policers .................................................................................... 86
  Application Assurance HTTP Redirect ...................................................................... 89
  Application QoS Policy (AQP) ..................................................................................... 91
  AQP Match Criteria ..................................................................................................... 92
  CLI Batch: Begin, Commit and Abort Commands ........................................................ 94
  Per AA Subscriber Service Monitoring and Debugging ............................................. 95
CPU Utilization .............................................................................................................. 95
Configuring Application Assurance with CLI ................................................................. 97
  Provisioning AA ISA ................................................................................................... 97
  Configuring AA ISA .................................................................................................... 99
  Configuring Watermark Parameters .......................................................................... 101
  Configuring a Group Policy ......................................................................................... 102
  Beginning and Committing a Policy Configuration .................................................... 102
  Aborting a Policy Configuration ................................................................................ 102
  Configuring an Application Filter ................................................................................ 103
  Configuring an Application Group ............................................................................. 104
  Configuring AA Volume, TCP and RTP Performance Reporting ............................... 105
  Configuring an Application ......................................................................................... 107
  Configuring an Application Profile ............................................................................ 108
  Configuring a Policier ................................................................................................. 109
  Configure an HTTP Redirect ...................................................................................... 110
  Configuring an Application QoS Policy ..................................................................... 111
  Configuring Application Service Options .................................................................. 113
  Configuring AA Volume Accounting and Statistics .................................................... 114
  Configuring Cflowd Collector ..................................................................................... 116
  Configuring AA Volume, TCP and RTP Performance Reporting ............................... 118
Application Assurance Command Reference ................................................................. 121

## IP Tunnels

IP Tunnels Overview ..................................................................................................... 240
Tunnel ISAs ..................................................................................................................... 243
  Public Tunnel SAPs ..................................................................................................... 243
  Private Tunnel SAPs ................................................................................................... 244
  IP Interface Configuration .......................................................................................... 245
  Unprotected GRE Tunnel Configuration .................................................................... 245
  GRE Tunnel Protection Using IPSec Tunnel Mode ...................................................... 247
Operational Conditions ................................................................................................. 250
QoS Interactions ............................................................................................................ 251
OAM Interactions ........................................................................................................... 251
### Table of Contents

- **Redundancy** ........................................................................................................... 251
- **Statistics Collection** ............................................................................................. 252
- **Security** ................................................................................................................ 252
- **IKEv2** .................................................................................................................... 253
- **X.509v3 Certificate Overview** .................................................................................. 254
  - **Key Generation** .................................................................................................. 254
  - **Formats and Local Storage** .................................................................................. 255
  - **Import and Export** ............................................................................................... 255
  - **Certificate Enrollment** .......................................................................................... 256
  - **CA Profile** ............................................................................................................ 256
- **Use Certificate Authentication for IKEv2 Static Lan-to-Lan tunnel** ......................... 256
- **Video Wholesale Example** ....................................................................................... 257
- **Configuring IPSec with CLI** ..................................................................................... 259
- **Provisioning an IPSec ISA** ...................................................................................... 259
- **Configuring IPSec ISA** ............................................................................................ 260
- **Configuring Router Interfaces for IPSec** .................................................................. 261
- **Configuring IPSec Parameters** ................................................................................ 262
- **Configuring IPSec in Services** ................................................................................ 263
- **Configuring X.509v3 Certificate Parameters** ............................................................ 263
- **IP Security Command Reference** ............................................................................. 267

### Video Services

- **Video Services** ........................................................................................................ 348
- **Video Groups** ......................................................................................................... 348
- **Video SAP** ............................................................................................................... 349
- **Video Interface** ....................................................................................................... 349
- **Multicast Information Policies** .................................................................................. 350
- **Duplicate Stream Protection** ................................................................................... 352
- **Duplicate Stream Selection** .................................................................................... 353
  - **Stream Identification** .......................................................................................... 353
  - **Initial Sequence Identification** ............................................................................. 354
  - **Packet Selection** .................................................................................................. 354
  - **Clock Recovery** .................................................................................................... 355
  - **Playout** .................................................................................................................. 356
  - **Loss of Transport** .................................................................................................. 356
- **Video Quality Monitoring** ........................................................................................ 357
  - **VoIP/Video/Teleconferencing Performance Measurements** .................................. 363
  - **Mean Opinion Score (MOS) Performance Measurements Solution Architecture** ...... 364
- **Retransmission and Fast Channel Change** ................................................................. 365
- **RET and FCC Overview** .......................................................................................... 365
  - **Retransmission** ....................................................................................................... 365
  - **Fast Channel Change (FCC)** .................................................................................. 366
    - **Retransmission Client** ....................................................................................... 370
    - **Retransmission Server** ..................................................................................... 371
  - **Fast Channel Change Server** .................................................................................. 372
  - **Logging and Accounting for RET and FCC** ............................................................ 373
  - **RET Server Session Stats** ..................................................................................... 373
  - **RET and FCC Server Concurrency** ........................................................................ 374
  - **Prerequisites and Restrictions** ............................................................................... 375
- **Multi-Service ISA Support in the IOM-3 for Video Services** ........................................ 376
# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prioritization Mechanism for RET vs. FCC</td>
<td>376</td>
</tr>
<tr>
<td>RET Features</td>
<td>377</td>
</tr>
<tr>
<td>Statistics ALU SQM MIB Additions</td>
<td>377</td>
</tr>
<tr>
<td>RET Server Multicast Tuning Parameters</td>
<td>378</td>
</tr>
<tr>
<td>FCC Features</td>
<td>379</td>
</tr>
<tr>
<td>FCC Hybrid Mode Support</td>
<td>379</td>
</tr>
<tr>
<td>Ad Insertion</td>
<td>380</td>
</tr>
<tr>
<td>Local/Zoned Ad Insertion</td>
<td>380</td>
</tr>
<tr>
<td>Transport Stream Ad Splicing</td>
<td>380</td>
</tr>
<tr>
<td>Ad Zones</td>
<td>383</td>
</tr>
<tr>
<td>Local/Zoned ADI Prerequisites and Restrictions</td>
<td>384</td>
</tr>
<tr>
<td>Configuring Video Service Components with CLI</td>
<td>385</td>
</tr>
<tr>
<td>Video Services Overview</td>
<td>385</td>
</tr>
<tr>
<td>Configuring an ISA-MS Module</td>
<td>387</td>
</tr>
<tr>
<td>Configuring a Video Group</td>
<td>388</td>
</tr>
<tr>
<td>Configuring a Video SAP and Video Interface in a Service</td>
<td>389</td>
</tr>
<tr>
<td>Basic Multicast Information Policy Configuration</td>
<td>390</td>
</tr>
<tr>
<td>Sample Configurations</td>
<td>391</td>
</tr>
<tr>
<td>Configuring RET/FCC Video Components with CLI</td>
<td>397</td>
</tr>
<tr>
<td>Configuring RET/FCC Video Features in the CLI</td>
<td>398</td>
</tr>
<tr>
<td>Configuring the RET Client</td>
<td>398</td>
</tr>
<tr>
<td>Configuring the RET Server</td>
<td>402</td>
</tr>
<tr>
<td>Configuring the FCC Server</td>
<td>406</td>
</tr>
<tr>
<td>Logging and Accounting Collection for Video Statistics</td>
<td>410</td>
</tr>
<tr>
<td>Configuring ADI Components with CLI</td>
<td>411</td>
</tr>
<tr>
<td>Configuring ADI in CLI</td>
<td>412</td>
</tr>
<tr>
<td>Configuring the RET Client</td>
<td>412</td>
</tr>
<tr>
<td>Configuring a Video Group</td>
<td>413</td>
</tr>
<tr>
<td>Configuring NTP</td>
<td>414</td>
</tr>
<tr>
<td>Configuring Channel Parameters</td>
<td>414</td>
</tr>
<tr>
<td>Configuring Service Entities</td>
<td>415</td>
</tr>
<tr>
<td>Video Command Reference</td>
<td>417</td>
</tr>
<tr>
<td>IP-TV Command Hierarchies</td>
<td>418</td>
</tr>
<tr>
<td>Show Commands</td>
<td>425</td>
</tr>
<tr>
<td>Clear Commands</td>
<td>425</td>
</tr>
<tr>
<td>Debug Commands</td>
<td>426</td>
</tr>
<tr>
<td>Video Services Commands</td>
<td>427</td>
</tr>
<tr>
<td>Generic Commands</td>
<td>427</td>
</tr>
<tr>
<td>Configuring NAT</td>
<td>485</td>
</tr>
<tr>
<td>ISA Redundancy</td>
<td>485</td>
</tr>
<tr>
<td>NAT Layer 2-Aware Configurations</td>
<td>488</td>
</tr>
<tr>
<td>Large Scale NAT Configuration</td>
<td>490</td>
</tr>
<tr>
<td>NAT Command Reference</td>
<td>493</td>
</tr>
<tr>
<td><strong>Appendix A: Common CLI Command Descriptions</strong></td>
<td></td>
</tr>
<tr>
<td>Common Service Commands</td>
<td>534</td>
</tr>
<tr>
<td><strong>Glossary</strong></td>
<td>537</td>
</tr>
<tr>
<td><strong>Index</strong></td>
<td>541</td>
</tr>
</tbody>
</table>
List of Figures

ISA-MS Hardware
Figure 1: AA ISA on Host IOM 2-20G Example .......................................................... 18

Application Assurance
Figure 2: AA ISA Inline Identification, Classification and Control ................................. 23
Figure 3: AA Deployment Topologies ................................................................. 24
Figure 4: AA BVS Services integrated into the Provider Edge ........................................ 28
Figure 5: AA in Dual Stack Residential Deployment ..................................................... 29
Figure 6: AA for Dual Stack Business VPN ............................................................. 30
Figure 7: AA Mirroring for Off-Line Specialized Appliance Processing ......................... 32
Figure 8: Transit Subscribers ..................................................................................... 41
Figure 9: Application Assurance Functional Components .......................................... 45
Figure 10: Application Assurance Ingress Datapath ...................................................... 46
Figure 11: Determining the Subscriber Profile, SLA Profile and Application Profile of a Host ................................................................. 51
Figure 12: Configuration Example ............................................................................ 52
Figure 13: AQP Definition Example ....................................................................... 53
Figure 14: Single ASO Example .............................................................................. 54
Figure 15: RADIUS COA Example ....................................................................... 61
Figure 16: Policy Structure .................................................................................... 66
Figure 17: From-AA-Sub Application-Aware Bandwidth Policing ................................ 88
Figure 18: To-AA-Sub Application-Aware Bandwidth Policing ................................ 88
Figure 19: AQP Actions ......................................................................................... 90

IP Tunnels
Figure 20: 7750 IPSec Implementation Architecture .................................................. 240
Figure 21: Example GRE over IPSec Tunnel Configuration ......................................... 248
Figure 22: Video Wholesale Configuration .................................................................. 257

Video Services
Figure 23: RTP Header Extension .......................................................................... 362
Figure 24: Voice/Voice Monitoring Deployment Example .......................................... 363
Figure 25: RET Server Retransmission of a Missing Frame ........................................ 365
Figure 26: FCC Client/Server Protocol .................................................................... 367
Figure 27: FCC Bursting Sent Faster Than Nominal Rate ........................................... 368
Figure 28: FCC Denting Removing Less Important Frames ......................................... 368
Figure 29: Ad Insertion Model ................................................................................ 380
Figure 30: Transport Stream Ad Splicing .................................................................. 381
Figure 31: Splicer Model ......................................................................................... 381
Figure 32: Transport Stream Flow Example ................................................................ 382
Figure 33: Video Services Configuration Elements .................................................. 386
## List of Tables

### ISA-MS Hardware
- **Table 1:** Application Assurance AA ISA System Support .................................................. 17
- **Table 2:** MS-ISA Host IOM Support Matrix ................................................................. 17

### Application Assurance
- **Table 3:** Traffic Diversion to the ISA ........................................................................... 25
- **Table 4:** Spoke SDP Divert ............................................................................................. 49
- **Table 5:** AA Flows and Sessions ..................................................................................... 67
- **Table 6:** Application Assurance Statistics Fields Generated per Record (Accounting File) ........................................................ 75
- **Table 7:** AA Performance Planning Record Fields ....................................................... 81
- **Table 8:** Policer’s Hardware Rate Steps for AA ISA ..................................................... 86

### IP Tunnels
- **Table 9:** Bottom Position QinQ and TopQ SAP Dot1P Evaluation ................................. 324
About This Guide

This guide describes details pertaining to Integrated Services Adapters (ISAs) and the services they provide.

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 7750 SR and 7450 ESS routers. It is assumed that the network administrators have an understanding of networking principles and configurations.

List of Technical Publications

The documentation set is composed of the following books:

- 7750 SR OS Basic System Configuration Guide
  7450 ESS OS Basic System Configuration Guide
  These guides describe basic system configurations and operations.

- 7750 SR OS System Management Guide
  7450 ESS OS System Management Guide
  These guides describe system security and access configurations as well as event logging and accounting logs.

- 7750 SR OS Interface Configuration Guide
  7450 ESS OS Interface Configuration Guide
  These guides describe card, Media Dependent Adapter (MDA), and port provisioning.
Preface

- 7750 SR OS Router Configuration Guide
  7450 ESS OS Router Configuration Guide
  These guides describe logical IP routing interfaces and associated attributes such as an IP
  address, port, link aggregation group (LAG) as well as IP and MAC-based filtering, and
  VRRP, and Cflowd.

- 7750 SR OS Routing Protocols Guide
  7450 ESS OS Routing Protocols Guide
  These guides provide an overview of routing concepts and provides configuration
  examples for RIP, OSPF, IS-IS, Multicast, BGP, and route policies.

- 7750 SR OS MPLS Guide
  7450 ESS OS MPLS Guide
  These guides describe how to configure Multiprotocol Label Switching (MPLS) and Label
  Distribution Protocol (LDP).

- 7750 SR OS Services Guide
  7450 ESS OS Services Guide
  These guides describe how to configure service parameters such as service distribution
  points (SDPs), customer information, and user services.

- 7750 SR OS OAM and Diagnostic Guide
  7450 ESS OS OAM and Diagnostic Guide
  These guides describe how to configure features such as service mirroring and Operations,
  Administration and Management (OAM) tools.

- 7750 SR OS Triple Play Guide
  7450 ESS OS Triple Play Guide
  These guides describe Triple Play services and support provided by the router and presents
  examples to configure and implement various protocols and services.

- 7750 SR OS Quality of Service Guide
  7450 ESS OS Quality of Service Guide
  These guides describe how to configure Quality of Service (QoS) policy management.

- OS Multi-Service Integrated Services Adapter Guide
  These guides describe services provided by integrated service Adapters such as
  Application Assurance, IPSec.

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 welcome center.
Web: http://www1.alcatel-lucent.com/comps/pages/carrier_support.jhtml
ISA-MS Hardware

In This Section

This section provides an overview of Alcatel-Lucent’s implementation of the ISA MS hardware.

Topics include:

- ISA-MS Overview on page 16
- Application Assurance Hardware Features on page 17
ISA-MS Overview

The ISA-MS is a resource module within the router providing packet buffering and packet processing in support of IPTV video features.

ISA-MS fits in an MDA/ISA slot on an IOM and has no external ports, so all communication passes through the IOM, making use of the network processor complex on the carrier IOM for queuing and filtering functions like other MDAs and ISAs.

The actual ingress and egress throughput will vary depending on the buffering and processing demands of a given video application, but the ISA hardware connector can support slightly more than 10 Gbps of throughput ingress and egress.
Application Assurance Hardware Features

AA ISA Host System Support

The Application Assurance Integrated Services Adapter (AA ISA) is a resource adapter, which means that there are no external interface ports on the AA ISA itself. Instead, any other Input Output Modules on a system in which the AA ISA is installed are used to switch traffic internally MS ISA to the AA ISA. Table 1 describes Application Assurance ISA support on products. Table 2 shows platform, IOM model, and feature matrix.

A key strength of Application Assurance features is the complete integration into the family of products. Common interfaces and operational familiarity reduce the effort to integrate the Application Assurance into existing networks.

Table 2: MS-ISA Host IOM Support Matrix

<table>
<thead>
<tr>
<th>Feature</th>
<th>7450 ESS: ESS-6, ESS-6v, ESS-7, ESS-12</th>
<th>7750 SR: SR-7, SR-12</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Assurance</td>
<td>IOM-20G-B, IOM3-XP</td>
<td>IOM-20G-B, IOM2-20G, IOM3-XP</td>
</tr>
<tr>
<td>Video: Ad Insertion</td>
<td>n/a</td>
<td>IOM-20G-B, IOM2-20G, IOM3-XP</td>
</tr>
<tr>
<td>NAT</td>
<td>n/a</td>
<td>IOM3-XP</td>
</tr>
</tbody>
</table>
IOM Support for AA ISA

The AA ISA is supported on IOM-20G-B, and IOM3-XP. Each IOM can support a maximum of two AA ISA modules. To maximize AA ISA redundancy, deployment of AA ISAs on separate host IOMs is recommended as it provides IOM resilience. Traffic from any supported IOM (for example IOM-20G-B, and IOM3-XP, fixed port IOMs (IMMs)) can be diverted to AA ISA hosted by either an IOM-20G-B, and IOM3-XP. The AA ISA is field replaceable and supports hot insertion and removal. See Figure 1. A system can support up to 7 active AA ISA cards providing up to 70 G of processing capacity.

AA ISA software upgrades are part of the ISSU functionality. Upgrades to AA ISA software, for example to activate new protocol signatures, do not impact the second MDA slot for the IOM carrying the AA ISA, nor do upgrades impact the router itself (for example, a new AA ISA software image can be downloaded without a need to upgrade other software images).

![Figure 1: AA ISA on Host IOM 2-20G Example](image-url)
Application Assurance

In This Section

This section provides an overview of Alcatel-Lucent’s implementation of the Application Assurance service model.

Topics include:

• Application Assurance (AA) Overview on page 22
  → Application Assurance: Inline Policy Enforcement on page 23
  → AA for Residential Subscriber Edge and VPN PE on page 24
  → Fixed Residential Broadband Services on page 26
  → Application-Aware Business VPN Services on page 27
  → Adjunct Off-line Content Processing on page 31
• Application Assurance System Architecture on page 33
  → AA ISA Resource Configuration on page 33
    – AA ISA Groups and Partitions on page 33
      • Multiple AA ISA Groups on page 33
      • AA Group Partitions on page 35
      • Bypass Modes on page 36
    – Redundancy on page 37
      • No AA ISA Group Redundancy on page 37
      • Failure to Fabric on page 37
      • N+1 AA ISA Card Warm Redundancy on page 37
    – ISA Load Balancing on page 39
    – ISA Overload Detection on page 43
AA Packet Processing on page 45
  - Divert of Traffic and Subscribers on page 46
  - Services and AA Subscribers on page 47
    • Spoke SDPs on page 49
    • Transit AA Subs on page 49
    • AA Subscriber Application Service Definition on page 49
    • Application Profile on page 50
    • Application Profile Map on page 51
    • Application Service Options (ASOs) on page 52
    • ASO Overrides on page 56
    • AA-Sub Scale Mode on page 57
  - Application Identification on page 64
    • Application Assurance Identification Components on page 66
    • Protocol Signatures on page 68
    • Custom Protocols on page 69
    • Protocol Shutdown on page 70
    • Supported Protocol Signatures on page 71
    • Application Groups on page 71
    • Applications on page 71
    • Application Filters on page 72
  - Statistics and Accounting on page 73
    • Per-AA-Subscriber Special Study on page 73
    • System Aspects on page 74
    • Application Assurance Volume Statistics and Accounting on page 75
    • AA-Performance Record for ISA Load on page 81
    • Cflowd AA Records on page 83
    • TCP Application Performance on page 83
    • Volume Statistics on page 83
• Audio/Video (A/V) Application Performance on page 84
  – Policy Actions on page 85
  – Application Assurance Policers on page 86
  – Application Assurance HTTP Redirect on page 89
  – Application QoS Policy (AQP) on page 91
  – AQP Match Criteria on page 92
  – AQP Actions on page 92
  – Time of Day Policing Adjustments on page 93
  → CLI Batch: Begin, Commit and Abort Commands on page 94
  → Per AA Subscriber Service Monitoring and Debugging on page 95
  → CPU Utilization on page 95
Application Assurance (AA) Overview

Network operators are transforming broadband network infrastructures to accommodate unified architecture for IPTV, fixed and mobile voice services, business services, and High Speed Internet (HSI), all with a consistent, integrated awareness and policy capability for the applications using these services.

As bandwidth demand grows and application usage shifts, the network must provide consistent application performance that satisfies the end customer requirements for deterministic, managed quality of experience (QoE), according to the business objectives for each service and application. Application Assurance (AA) is the enabling network technology for this evolution in the service router operating system.

Application Assurance, coupled with subscriber and/or VPN access policy control points enables any broadband network to provide application-based services. For service providers, this unlocks:

- The opportunity for new revenue sources.
- Content control varieties of service.
- Control over network costs incurred by various uses of HSI.
- Complementary security aspects to the existing network security.
- Improved quality of service (QoS) sophistication and granularity of the network.
- The ability to understand and apply policy control on the transactions traversing the network.
The integrated solution approach for Application Assurance recognizes that a per-AA-subscriber and per-service capable QoS infrastructure is a pre-condition for delivering application-aware QoS capabilities. Enabling per-application QoS in the context of individual subscriber’s VPN access points maximizes the ability to monetize the application service, because a direct correlation can be made between customers paying for the service and the performance improvements obtained from it. By using an integrated solution there is no additional cost related to router port consumption, interconnect overhead or resilience to implement in-line application-aware policy enforcement.
AA for Residential Subscriber Edge and VPN PE

Multiple deployment models are supported for integrating application assurance in the various subscriber edge and VPN PE network topologies. In all cases, application assurance can be added by in-service upgrade to the installed base of equipment rather than needing deploy and integrate a whole new set of equipment and vendors into the network for Layer 4-7 awareness.

Integrating Layer 4-7 application policy with the 7750 SR or 7450 ESS subscriber edge policy context is the primary solution to address both residential broadband edge or Layer 2/Layer 3 application aware business VPN. Placement of Layer 4-7 analysis at the distributed subscriber edge policy point simplifies AA deployments in the following ways:

- For residential markets, CO-based deployment allows deployment-driven scaling of resources to the amount of bandwidth needed and the amount of subscribers requiring application-aware functionality.
- For AA business VPNs, a network deployment allows large scale application functionality at a VPN provider edge access point, vastly reducing complexity, cost, and time to market required to offer application-aware VPN services.
- Traffic asymmetry is avoided. Any subscriber traffic usually passes through one CO subscriber edge element so there is no need for flow paths to be recombined for stateful analysis.
- PE integration provides a single point of policy enforcement.

![Figure 3: AA Deployment Topologies](image_url)
There are residential topologies where it is not possible or practical to distribute ISAs into the same network elements that run ESM, including for legacy edge BRASs that still need Application Assurance policy (reporting and control) for the same internet services, and which needs to be aligned and consistent with the ESM AA policy. This is supported using transit AA subscribers, typically in the first routed element behind the legacy edge.

Application Assurance enables per AA-subscriber (a residential subscriber, or a Layer 2/Layer 3 SAP or spoke SDP), per application policy for all or a subset of AA subscriber’s applications. This provides the ability to:

- Implement Layer 4-7 identification of applications using a multitude of techniques from a simple port-based/IP address based identification to behavioral techniques used to identify, for example, encrypted or evasive applications.

- Once identified, to apply QoS policy on either an aggregate or a per-AA-subscriber, per-application basis.

- Provide reports on the identification made, the traffic volume and performance of the applications, and policies implemented.

An integrated AA module allows the SR/ESS product families to provide application-aware functions that previously required standalone devices (either in residential or business environment) at a fraction of cost and operational complexity that additional devices in a network required.

A key benefit if integrating AA in the existing IP/MPLS network infrastructure (as opposed to an in-line appliance) is the ability to select traffic for treatment on a granular, reliable basis. Only traffic that requires AA treatment is simply and transparently diverted to the ISA. Other traffic from within the same service or interface will follow the normal forwarding path across the fabric. In the case of ISA failure, ISA redundancy is supported and in the case no backup ISAs are available the AA traffic reverts to the normal fabric matrix forwarding, also known as “fail to fabric”.

**Table 3: Traffic Diversion to the ISA**

<table>
<thead>
<tr>
<th>Deployment Case</th>
<th>System Divert ID</th>
<th>AA-Sub Type</th>
<th>App-Profile on:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Residential Edge</td>
<td>ESM Sub-ID</td>
<td>Subscriber (ESM)</td>
<td>Sub (prefix, not hosts)</td>
</tr>
<tr>
<td>Business Edge</td>
<td>L2/L3 SAP</td>
<td>SAP</td>
<td>SAP (Aggregate)</td>
</tr>
<tr>
<td>Residential Transit</td>
<td>Parent L3 SAP/Spoke-SDP</td>
<td>Transit AA</td>
<td>Transit Sub</td>
</tr>
<tr>
<td>Spoke Attached Edge</td>
<td>Spoke SDP</td>
<td>Spoke SDP</td>
<td>Spoke SDP (Aggregate)</td>
</tr>
</tbody>
</table>
Fixed Residential Broadband Services

Fixed residential HSI services as a single edge Broadband Network Gateway (BNG) or as part of the Triple Play Service Delivery Architecture (TPSDA) are a primary focus of Application Assurance performance, subscriber and traffic scale.

To the service provider, application-based service management offers:

• Application aware usage metering packages (quotas, 0-rating etc...)
• New revenue opportunities to increase ARPU (average revenue per user) (for gaming, peer-to-peer, iVoIP, iVideo, etc.).
• Fairness: Aligns usage of HSI network resources with revenue on a per-subscriber basis.
• Operational visibility into the application usage, trends, and pressure points in the network.

To the C/ASP, service offerings can be differentiated by improving the customer’s on-line access experience. The subscriber can benefit from this by gaining a better application experience, while paying only for the value (applications) that they need and want.
Application-Aware Business VPN Services

AA for business services can be deployed at the Layer 2 or Layer 3 network provider edge (PE) policy enforcement point for the service or at Layer 2 aggregation policy enforcement point complimentary to the existing Layer 3 IP VPN PE. In a business environment, an AA-subscriber represents a VPN access point. A typical business service can have a much larger average bandwidth rate then the residential service and is likely to have a smaller AA-subscriber count than a residential deployment.

Up to seven active ISAs can be deployed per PE, each incrementally processing up to 10Gbps. The in-network scalability is a key capability that allows a carrier to be able to grow the service bandwidth without AA throughput affecting the network architecture (more edge nodes, application-aware devices).

Application-aware Layer 2 and Layer 3 VPNs implemented using AA ISA equipped 7750 SR/7450 ESS together with rich network management (5620 SAM, 5750 RAM, end customer application service portals) give operators a highly scalable, flexible, and cost effective integrated solution for application-based services to end customers. These services may include:

- Rich application reporting with VPN, access site visibility.
- Right-sizing access pipes into a VPN service to improve/ensure application performance.
- Application-level QoS (policing, session admission, remarking, etc.) to ensure application-level performance, end-customer QoE objectives are met.
- Value-added services such as application verification, new application detection, application mirroring.
- Performance reporting for real time (RTP) and non-real time (TCP) based applications.
- Control unauthorized or recreational applications by site, by time of day.
Figure 4: AA BVS Services integrated into the Provider Edge
AA in Dual Stack Residential Deployment

The dual-stack IPoE Routed Gateway (RG) service allows operators of existing TR-101 network to deploy IPv6 over Ethernet services in conjunction with an existing IPv4 over Ethernet service. The dual-stack aspect represents both IPv4 and IPv6 traffic on the single subscriber circuit that share a common subscriber-ident, SLA and subscriber profile.
The architecture allows for some SAPs to be IPv4 while others are IPv6. There is nothing in the architecture however, to limit all the traffic within a SAP to be either IPv4 or IPv6. A mix is allowed.

6 to 4, as discussed in RFC 3056, *Connection of IPv6 Domains via IPv4 Clouds*, allows IPv6 sites to communicate over an IPv4 network without the need to configure explicit tunnels, as well as and for them to communicate with native IPv6 domains through relay routers. Effectively 6to4 treats the wide area IPv4 network as a unicast point-to-point link layer. Both ends of the 6to4 tunnel are dual-stack routers. Because 6to4 does not build explicit tunnels, it scales better and is easier to manage after setup.

6to4 encapsulates an IPv6 packet in the payload portion of an IPv4 packet with protocol type 41. The IPv4 destination address for the encapsulating IPv4 packet header is derived from the IPv6 destination address of the inner packet (which is in the format of 6to4 address), by extracting the 32 bits immediately following the IPv6 destination address's 2002:: prefix. The IPv4 source address in the encapsulating packet header is the IPv4 address of the outgoing interface (not system IP address).

From an AA point of view, 6to4 packets are IPv4 packets, however, the payload contains IPv6 header. Hence, the true packet payload is embedded further down in the packet. The protocol type is set to 41.
Adjunct Off-line Content Processing

Some deployments require specialized off-line processing not provided by AA. An example of such processing is Lawful Intercept (LI) traffic content processing or using an off-line appliance. To enable such capabilities in a highly-scalable fashion that minimizes traffic seen by the off-line device, the AA allows operators to use an AQP action to mirror traffic conditioned by both application and AA subscriber context, so detailed content processing can be performed only for AA subscribers and applications of choice. The content processing equipment generally needs to see the entire traffic stream for a given application, therefore, the entire application’s traffic is mirrored including packets that have not yet been identified. Optionally, only traffic positively identified can be mirrored as well.

Although similar functionality could be achieved by mirroring service or a SAP, the total bandwidth and added complexity that an off-line appliance would need to handle extra bandwidth makes such a solution more costly and harder to scale.

Since the application mirroring is an additional function independent from all other AA functions provided on the ESS/SR, the in-line deployed AA ISA modules not only reduces the amount of traffic the off-line device must see, but also allows in-line policy enforcement actions with application awareness once the off-line devices triggers such a policy change. For example, AA subscriber traffic for an application or applications being mirrored can be quarantined while the remaining traffic remains unaffected.

Figure 7 depicts an example of application mirroring to a specialized off-line appliance for further processing.

1. AA subscriber traffic contains applications requiring specialized off-line appliance processing that requires Layer 2 — Layer 7 application identification.

2. AA ISA with AQP configured:
   Match:
   → Application for off-line processing for selected subscribers (downstream only, upstream only, or both).
   Action:
   → Mirror source for application’s IP packets into a mirror service configured on a router.

3. Specialized appliance sees only the required traffic and performs the desired off-line processing.
Figure 7: AA Mirroring for Off-Line Specialized Appliance Processing
Application Assurance System Architecture

AA ISA Resource Configuration

AA ISAs are flexible embedded, packet processing resource cards that require configuration such that services may be associated with the resources. This includes assigning ISAs to groups, optionally defining group partitions, and setting the redundancy model. Load balancing is affected by how ISAs are grouped.

AA ISA Groups and Partitions

An AA ISA group allows operators to group multiple AA ISAs into a single logical group for consistent management of AA resources and policies across multiple AA ISA cards configured for that group.

Multiple AA ISA Groups

An AA ISA group allows operators to group multiple AA ISAs into one of several logical groups for consistent management of AA resources and policies across multiple AA ISA cards configured for that group. The following operations can be performed at the group level:

- Define one or multiple AA ISA groups to allow AA resource partitioning/reservation for different types of AA service.
- Assign physical AA ISAs to a group.
- Select forwarding classes to be diverted for inspection by the AA subscribers belonging to the group and select the AA policy to be applied to the group.
- Configure redundancy and bypass mode features to protect against equipment failure.
- Configure QoS on IOMs which host AA ISAs for traffic toward AA ISAs and from AA ISAs.
- Configure ISA capacity planning using low and high thresholds.
- Enable partitions of a group.
- Configure the ISA traffic overload behaviour for the group to either backpressure to the host IOM (resulting in possible network QoS-based discards) or to cut-through packets through the ISA without full AA processing. Cut-through is typically enabled for AA VPN groups but not for residential groups.

Residential services is an example where all AA services might be configured as part of a single group encompassing all AA ISAs, for operator-defined AA service. This provides management of
common applications and reporting for all subscribers and services, with common or per customer AQP (using ASOs characteristics to divide AA group’s AQP into per app-profile QoS policies).

Multiple groups can be further used to create separate services based on different sets of common applications, different traffic divert needs (such as for capacity planning) or different redundancy models. Cases where multiple groups might be used can include:

- For mix of residential and business customers.
- Among different business VPN verticals.
- For business services with a common template base but for different levels of redundancy, different FC divert, or scaling over what is supported per single group.
- System level status statistics have AA ISA group/partition scope of visibility.
AA Group Partitions

VPN-specific AA services are enabled using operator defined partitions of an AA Group into AA policy partitions, typically with one partition for each VPN-specific AA Service. The partition allows VPN specific custom protocols/application/application group definition, VPN specific policy definition and VPN specific reporting (e.g. some VPNs with Volume only reports, while others with Volume and Performance reports). Each partition’s policy can be again divided into multiple application QoS policies using ASOs.

Use of ISA Groups and partitions also improves scaling of policies, as needed with VPN-specific AA policies.

If partitions are not defined, all of the AA Group acts as a single partition. When partitions are configured, application identification, policy and statistics configuration applies only to the given partition and not any other partitions configured under the same AA Group.

Definition of Application profiles (and related ASO characteristics/values) are within the context of a given partition (however, App profiles names must have node-wide uniqueness)

Definition of applications, application groups and AQP are also specific to a given partition. This allows:

- Definition of unique applications and app-groups per partition.
- Definition of AQP policy per partition.
- Definition of common applications and app-groups per partition with per partition processing and accounting.

Partitions also enable accounting/reporting customization for every AA subscriber associated with a partition, for example:

- Ability to define different types of reporting/accounting policies for different partitions in a single AA group, such as uniquely define which application, protocols, app groups are being reported on for every AA subscriber that uses a given partition.
- AA group level protocol statistics with partition visibility (for example, protocol counts reported for each partition of the group separately).

The system provides independent editing and committing of each partition config (separate begin/commit/abort).

Policer templates allow group-wide policing, and can be referenced by partition policies.
Bypass Modes

If no active AA ISA is available (for example, due to an operational failure, misconfiguration) the default behavior is to forward traffic as if no AA was configured, the system does not send traffic to the AA ISA (equivalent to fail to closed). Alarms are raised to flag this state externally. There is an optional “fail to open” feature where AA ISA service traffic is dropped if no active AA ISA is present (such as no AA ISA is present and operationally up).
Redundancy

AA ISA group redundancy is supported, to protect against card failure and to minimize service interruption during maintenance or protocol signature upgrades.

No AA ISA Group Redundancy

AA can be configured with no ISA redundancy within the AA group. All AA ISAs are configured as primary with no backup (up to the limit of active AA ISAs per node). There is no fault state indicating that a spare AA ISA is missing. If a primary is configured but not active, there will be a “no aa-isa” fault.

Failure to Fabric

In the event that no ISA redundancy is deployed or insufficient ISAs are available for needed sparing, the system implements “failure to fabric”. When the ISA status shows the is not available and there is no redundant ISA available, the ingress IOMs simply do not divert the packets that would have been sent to that ISA, but instead these proceed to the next hop directly across the fabric. When the ISA becomes available, the divert eligible packets resume divert through the ISA. This behavior is completely internal to the system, without affecting the forwarding or routing configuration and behavior of the node or the network.

N+1 AA ISA Card Warm Redundancy

The system supports N+1 AA ISA equipment warm redundancy (N primary and 1 backup). If a backup is configured and there is no ISA available (a primary and backup failed), there will be a “no aa-isa” fault. The backup AA ISA is pre-configured with isa-aa.tim and the group policies. Datapath traffic is only sent to active AA ISAs, so the backup has no flow state. If a backup ISA is unavailable, there will be a “backup missing” fault.

An AA subscriber is created and assigned to a primary AA ISA when an application profile is assigned to a subscriber, SAP, or spoke SDP. By default, AA subscribers are balanced across all configured primary AA ISAs.

Upon failure of a primary AA ISA, all of its AA subscribers and their traffic are operationally moved to the newly active backup AA ISA but the current flow states are lost (warm redundancy). The new AA ISA will identify any session-based active flows at a time of switchover as an existing protocol, while the other flows will be re-identified. The existing protocol-based application filters can be defined to ensure service hot redundancy for a subset of applications. Once the backup AA ISA has taken control, it will wait for operator control to revert activity to the failed primary AA ISA module.
The user can disable a primary AA ISA for maintenance by triggering a controlled AA ISA activity switch to do the AA ISA software field upgrade (a shutdown of an active AA ISA is recommended to trigger an activity switch).

The activity switch experiences the following AA service impact:

- All flow states for the primary ISA are lost, but existing flows can be handled with special AQP rules for the existing flows by the newly active backup AA ISA until sessions end.
- All statistics gathered on the active AA ISA since the last interval information that was sent to the CPM will be lost.
ISA Load Balancing

Capacity-cost based load balancing allows a cost to be assigned to diverted AA subscribers (by the app-profile). Load Balancing uses the total allocated costs on a per-ISA basis to assign the subscriber to the lowest sum cost ISA resource. Each ISA supports a threshold as the summed cost value that notifies the operator if or when capacity planning has been exceeded.

The load balancing decision is made based on the AA capacity cost of an AA subscriber. The capacity cost is configured against the app-profile. When assigning a new diverted aa-sub to an ISA, the ISA with the lowest summed cost (that also has sufficient resources) is chosen. Examples of different load-balancing approaches that may be implemented using this flexible model include:

- aa-sub count balancing — Configure the capacity cost for each app-profile to the same number (for example, 1).
- aa-sub stats resource balancing — Configure the capacity cost to the number of stats collected for AA subscribers using the app-profile. This might be used if different partitions have significantly different stats requirements.
- Bandwidth balancing — Configure the capacity cost to the total bandwidth in both directions (in kbps) expected for those AA subscribers. This might be used if different AA subscribers have highly varying bandwidth needs.

Load balancing operates across ISAs within an AA group, and will not balance across groups. The system will ensure that app-profiles assigned to AA subscribers (ESM subscribers, SAPs and spoke-sdps) that are within a single VPLS/Epipe/IES/VPRN service are all part of the same AA group (partitions within an AA group are not checked/relevant).

Users can replace the app-profile assigned to an AA subscriber with another app-profile (from the same group/partition) that has a different capacity cost.

Regardless of the preferred choice of ISA, the system takes into account:

- Per previous releases, resource counts have per-ISA limits. If exceeded on the ISA of choice, that ISA cannot be used and the next best is chosen.
- Divert IOM service queuing resources may limit load-balancing. If queuing resources are exhausted, the system attempts to assign the aa-sub to the ISA where the first AA subscriber within that service (VPLS/Epipe) or service type (IES/VPRN) was allocated.

For prefix transit AA subscriber deployments using the remote-site command, traffic for the remote transit subs are processed a second time. The ISA used by the parent AA-sub will be used by all transits within the parent. In remote-site cases there may be a need to increase capacity cost of parent since the transits stay on same ISA as the parent.

Prefix transit AA-subs are all diverted to the same Group and partition as the parent SAP.
Transit Prefix Policy

A transit prefix policy, defined in the **config>app-assure>group** context, is associated with the parent (divert) SAP/SDP to define how transit AA subs are created within that parent. The transit prefix policy must be defined before it can be assigned to a parent. Prefix transit subs can be created by (static) CLI/SNMP configuration of a transit aa-sub within the transit-prefix-policy.

The IP addresses defined in the **transit-prefix-policy** for a transit sub are any length from /0 to /32. Multiple IP addresses (from any prefix/pool and of any length) can be assigned to a single transit AA sub. IP addresses must be unique within a transit IP policy, but can be re-used in separate policies (since they have parent specific context).

The transit prefix policy follows IP filter conventions for first match and ordering of entries. While for residential /32 transits if there is an IP address conflict between any static prefix transit subs, the latter config will be blocked, for business transit subs multiple overlapping address entries are allowed to enable longest match within subnets.

ASO policy override is supported for prefix transit subs.

---

**static-remote-aa-sub Command**

This command enables unique ISA treatment of transit subscribers configured opposite facing to the parent SAP/spoke-SDP using ip prefixes. Provisioning a transit sub as remote-aa-sub (within a transit prefix policy) enables the ISA to treat any network-ip based transit subs in the following ways:

- Treat packets for the parent aa-sub independent of whether transits are also configured (stats and policer for parent work as usual).
- Subsequently treat the same packet as a transit-sub packet when matching to a configured transit sub (stats, policers).
- Allows natural direction of the packet for both the parent aa-sub and the transit-aa-sub, as shown in Figure 8, a packet from a remote client to a local server will be seen as **to-sub** for the parent, and **from-sub** for the transit sub that is logically at the far end site.
- Correct directionality of packet ID for all aa subs allows proper operation of app-filter flow-setup-direction. Otherwise, having a local parent aa-sub and a remote transit suffers from these direction issues.
Figure 8: Transit Subscribers
Transit AA-sub Persistence

Prefix transit subs are not affected by persistence as per IP transit subscribers, since they can only be statically configured.

Policers for Prefix Transit AA-subs

AA-sub per-subscriber policers can provide per SAP policing for the parent SAP, with transit AA-subs each supporting distinct per-sub policers within the parent (packets are only processed once against one aa-sub – the parent or the transit sub). Packets matching transit AA subs and policers will not be included in a parent policer.

There is no policer hierarchy unless system wide policers are referred to by both the parent aa-sub and transit aa-sub. When the remote-site configuration is not used, system policers can be used to police all traffic for a site containing transits, subject to constraints on system policer scale.

When the remote-aa-sub config is used, the parent owns all packets for stats and policing, so any transit sub configuration within the parent does not affect the stats or policers.

AA Policers are supported on a transit subscriber basis, across all (multiple) IP prefixes per sub.
ISA Overload Detection

Capacity cost resource counting does not have a hard per-ISA limit, since the cost values are decoupled from actual ISA resources. However, the value of the total summed cost per-ISA can be reported, and a threshold value can be set which will raise an event when exceeded.

ISA capacity overload detection and events are supported within the system resource monitoring / logging capabilities if the traffic and resource load crosses the following high and low load thresholds on a per-ISA basis:

- ISA capacity cost
- Flow table consumption (number of allocated flows)
- Flow setup rate
- Traffic volume
- Host IOM egress weighted average shared buffer pool use (within the egress QoS configuration for each group). These thresholds are also used for overload cut-through processing

While an app-profile is assigned to AA subscribers, the capacity-cost for that app-profile can be modified. The system makes updates in terms of the load balancing summary, but this does not trigger a re-balance.

In the absence of user configuration, the App-profile default capacity cost is 1. The range for capacity cost is 1 — 65535 (for example, for bandwidth based balancing the value 100 could represent 100kbps). Note that 0 is an invalid value.

If the re-balancing of AA subscribers is required (for instance after the addition of new ISAs), there is a `tools` command to rebalance AA subscribers between ISAs within a group. Rebalance affects which AA subs divert to which ISAs based on capacity cost. Transit subs cannot be rebalanced independent of the parent (they move with the parent divert). The system attempts to move aa-subs from the most full ISA to the least full ISA based on the load balancing mode. If the load becomes balanced or an aa-sub move fails due to ISA resources or divert IOM service queuing resources, the load balancing terminates.

Alternatively, load balancing can be manually accomplished by the AA subscriber being removed and re-added. This will trigger a load balancing decision based on capacity-cost. For all AA subscriber types, this can be accomplished by removing and re-applying the AA subscriber's app-profile. In the case of ESM AA subscribers, shutting down and re-enabling either sub-sla-mgmt or the host(s) will have the same effect. Dynamic ESM AA subscribers will re-balance naturally over time as subscribers come and go from the network.

For transit AA subscriber deployments, the parent divert SAPs are load-balanced based on AA capacity cost from the app-profile configured against the SAP/SDP. The parent capacity cost should be configured to represent the maximum expected cost when all transit subs are present.
All traffic not matching a configured transit subscribers is dealt with as a member of the parent SAP and according to its app-profile.
AA Packet Processing

There are four key elements of Application Assurance packet processing (Figure 9):

1. Divert: Selection of traffic to be diverted to the AA ISA
2. Identification of the traffic on a per flow (session) basis.
3. Reporting of the traffic volume and performance.
4. Policy treatment of the identified traffic.

Figure 9: Application Assurance Functional Components
Divert of Traffic and Subscribers

Any traffic can be diverted for application-aware processing. Application Assurance is enabled through the assignment of an application profile as part of either an enhanced subscriber management or static configuration. This process enables the AA functionality for all traffic of interest to and from a given subscriber/SAP/spoke SDP. Which traffic is deemed of interest, is configured through an AA ISA group-specific configuration of forwarding classes (FCs) to be diverted to AA and enabled on a per subscriber/SAP/spoke SDP using application profiles.

Figure 10 shows the general mechanism for filtering traffic of interest and diverting this traffic to the appropriate AA ISA module residing on an IOM (referred as the host IOM). This traffic management divert method applies to both bridged and routed configurations.

For a SAP, subscribers with application profiles enabling AA, the traffic is diverted to the active AA ISA using ingress QoS policy filters, identifying forwarding and sub-forwarding classes that could be diverted to the Application Assurance. Only single point (SAP, ESM subscriber, spoke SDP) configuration is required to achieve divert for both traffic originated by and destined to a given AA subscriber. Diversion (divert) to the AA ISA is conditional based on the AA ISA status (enabled, failed, bypassed, etc.).

Unless the AA subscriber’s application profile is configured as “divert” using Application Profiles and the FC is selected to be diverted as well, the normal ingress forwarding occurs. Traffic that is...
filtered for divert to AA ISAs is placed in the appropriate location for that system’s AA ISA destination.

Users can leverage the extensive QoS capabilities of the router when deciding what IP traffic is diverted to the Application Assurance system for inspection. Through AA ISA group-wide configuration, at least one or more QoS forwarding classes with the “divert” option can be identified. The forwarding classes can be used for any AA subscriber traffic the service provider wants to inspect with Application Assurance.

Services and AA Subscribers

The AA ISA provides the Layer 3-7 packet processing used by the Application Assurance feature set. Application Assurance is applied to IPv4 traffic on a per ESM subscriber/SAP/spoke SDP (AA subscriber) basis (non-IPv4 traffic is not diverted to AA and forwarded as if AA was not configured) where an AA subscriber may be contained in the following services:

- IES
- VPLS
- VLL — Epipe and Ipipe

Application Assurance is supported with:

- Bridged CO
- Routed CO
- Multi-homed COs
- Layer 2/Layer 3 VPN service access points and spoke SDPs

The AA ISA feature set uses existing QoS capabilities and further enhances them to provide application-aware traffic reporting and management on per individual AA subscriber, AA subscriber-type or group. A few examples of per-application capabilities within the above AA subscriber contexts include:

- Per AA subscriber, application traffic monitoring and reporting.
- Per application bandwidth shaping/policing/prioritization.
- Throttling of flow establishment rate.
- Limiting the number of active flows per application (such as BitTorrent, video or teleconference sessions, etc.).
- Application-level classification to provide higher or lower (including drop) level traffic management in the system (for example, IOM QoS) and network.

The following restrictions are noted:
• Application Assurance is not supported for tunneled transit traffic (using PPP or DHCP) destined for a remote BRAS.

• Residential AA relies on ESM for subscriber context. Therefore any layer 3 edge / aggregation in front of a layer 2 edge (bridged CO) will not be able to use AA, particularly if there is a single MAC across multiple subscribers on a downstream device.
Spoke SDPs

AA on spoke-SDP services allows AA divert of the spoke SDP, logically representing a remote service point, typically used where the remote node does not support AA. A given SAP/spoke can be assigned and app-profile, and when this app-profile is enabled for **divert** all packets to and from that SAP/spoke will be diverted to an AA ISA (for forwarding classes that are configured as divert eligible).

Table 4 shows spoke SDP divert capabilities.

**Table 4: Spoke SDP Divert**

<table>
<thead>
<tr>
<th>Access Node Service (spoke SDP type)</th>
<th>Connected to Service</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Epipe</td>
</tr>
<tr>
<td>Epipe (Ethernet spoke)</td>
<td>Y</td>
</tr>
<tr>
<td>Ipipe (IP spoke)</td>
<td>N/A</td>
</tr>
<tr>
<td>VPLS (ethernet spoke)</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Transit AA Subs

A transit AA-sub incorporates the following attributes:

- Name
- IP address (one or more hosts)
- App-profile (note that the divert/no divert and capacity cost setting of the app-profile does not affect transit AA-subs since divert occurs only against the parent SAP).

AA Subscriber Application Service Definition

- Application Profile on page 50
- Application Profile Map on page 51
- Application Service Options (ASOs) on page 52
- ASO Overrides on page 56
Application Profile

Application profiles enable application assurance service for a given ESM subscriber, Service Access Point or spoke SDP (AA subscriber). Each application profile is unique in the system and defines the AA service that the AA subscriber will receive. An ESM subscriber can be assigned to an application profile which affects every host of the particular subscriber. For SAP or spoke SDP AA subscribers, an application profile can be assigned which affects all traffic originated/destined over that SAP or spoke SDP. By default, ESM subscribers, SAPs or spoke SDPs are not assigned an application profile.

The following are main properties of application profiles:

- One or more application profiles can be configured in the system.
- Application profiles specify whether or not AA subscriber’s traffic is to be diverted to Application Assurance.
- Application profiles are defined by an operator can reference the configured application service options (ASO) characteristics (see Application Service Options (ASOs) on page 52).
- Application profiles must only be assigned once AA resources (AA ISA cards) are configured.
- App-profiles can be assigned a capacity cost used for subscriber load balancing among ISAs within the AA group. (See ISA Load Balancing on page 39.)

ESM includes an application profile string. The string points to an application profile pre-provisioned within the router and is derived by:

- Parsing the DHCP Option 82 sub-option 1 circuit ID payload, vendor specific sub-option 9, or customer-defined option different from option 82, during authentication and the DHCPDISCOVER, as well as re-authentication and the subscriber’s DHCPREQUEST.
- RADIUS using a new VSA. [26-6527-xx] alc-application-profile-string
- Inherited by defaults in the sap>sub-sla-mgmt context, to allow default application profile assignment if no application profile was provided.
- Static configuration.

Mid-session (PPP/DHCP) changes to the application profile string allows:

- Modification of the application profile a subscriber is mapped to and pushes the change into the network as opposed to waiting for the subscriber to re-authenticate to the network.
- Change to the subscribers application profile inline, without a need for the subscriber to re-authenticate to RADIUS or perform any DHCP message exchange (renew or discover) to modify their IP information.
Application Profile Map

Application Assurance adds new map (app-profile-map) application profile command to associate an app-profile-string from dynamic subscriber management to a specific application profile using its app-profile-name that has been pre-provisioned. The application profile map is configured in the config>subscr-mgmt>sub-ident-pol context.

The pre-defined subscriber identification policy has to be assigned to a SAP, which determines the sub-id, sub, sla, and app-profiles.
Application Service Options (ASOs)

ASOs are used to define service provider and/or customer visible network control (policy) that is common between sets of AA subscribers (for example, upstream/downstream bandwidth for a tier of AA service). ASO definition decouples every AA subscriber from needing subscriber-specific entries in the AQP for standard network services.

As an example, an operator can define an ASO called “ServiceTier” to define various HSI services (Super, Lite, etc.) (Figure 12-A). The operator can then reference these defined ASOs when creating the App Profiles that are assigned to AA-subscribers (Figure 12-B).

Figure 12: Configuration Example
Then, the defined ASOs are used in the AQP definition to determine the desired treatment / policy (Figure 13).

```
app-qos-policy
entry 50 create
description "Limit downstream b/w for Super subscribers"
match
    traffic-direction network-to-subscriber
    characteristic "ServiceTier" eq "Super"
exit
action
    bandwidth-policer "SuperDown"
exit
no shutdown
exit
entry 110 create
match
    application-group eq "Tunneling"
    characteristic "SiteType" eq "Remote"
exit
action
    remark fc af
exit
no shutdown
exit
```

**Figure 13: AQP Definition Example**

Alternatively, if ASOs were not used in the previous example, then the operator would have to define a unique AQP entry for every subscriber. Each of these AQPs will have its “match” criteria setup to point to the subscriber ID, while the action for all of these unique AQPs will be the same for the same service (for Tier 1 service, the policer bandwidth will be the same for all Tier 1 AA subscribers) (Figure 14).
The example in Figure 14, shows how the use of just a single ASO can save the user from having to provision an AQP entry every time a subscriber is created.

Other example uses of ASO entries include:

- Entry per application group that is to be managed, such as VoIP, P2P, HTTP.
- Several entries where specific applications within an application group can individually be managed as service parameters, for example, HTTP content from a specific content provider, or streaming video from network television or games.
- HSI tiers (for example, Gold, Silver, and Bronze for specifying bandwidth levels).
- VPN customer ID.
Application characteristics are defined as specific to the services offered within the operator's network. The operator defines ASO characteristics and assigns to each ASO one or more values to define service offering to the customers.

The following are the main elements of an ASO:

- A unique name is applied to each characteristic.
- The name is unique to the group-partition-policy, but the expectation is that characteristics will be consistent network-wide.
- Operator-defined values (variables) are defined for each characteristic and are unique to each characteristic. A default value must be specified from the set of the values configured.

The following lists how ASO characteristics are used:

- Application service options are used as input to application profiles.
- AQP rule sets also use the ASO characteristics to influence how specific traffic is inspected and policies applied.
- Multiple ASO characteristic values are allowed in a single rule.

Syntax checking is performed when defining application profiles and AQPs that include application characteristics. This ensures:

- The characteristic is correctly identified.
- In an app-profile and app-qos-policy when specifying a characteristic, the value must be specified. The "default-value" applies if a characteristic is not specified within an app-profile.
ASO Overrides

This feature enables individual attributes/values to be set against an aa-sub for business AA complementary to using app-profiles. The aa-sub types supported are provisioned business AA SAPs and spoke SDPs, and statically-provisioned transit AA subs.

Application profile assignment is still used to obtain the following information:

- The application-assurance group [and partition] the SAP/spoke SDP is being assigned to
- Whether the traffic should be diverted or not
- Capacity-cost (for load balancing to a multi-isa group)

The information configured in the app-profile is also used, but the following can be overridden:

- ASO characteristics and values (these are from the policy defined in the group and partition)

The overrides are specific to a single divert aa-sub (or parent of transit AA subs). It does not affect any other aa-sub or the app-profile config itself.

Typically the ASO characteristics in the app-profile would not be specified, thus leaving all characteristics at their default values. This is not mandatory though and the app-profile could specify any ASO characteristic and non-default value.

The AA app-qos-policy has entries that can refer to ASO characteristics (attributes) and values in their match criteria. In the absence of any individual attribute/value override, an aa-sub will continue to work as before - using the ASO characteristics/values defined inside the app-profile assigned to them. With overrides, the aa-sub attributes used in app-qos-policy lookups are the combination of the following:

- The characteristics/values from the app-profile,
- Any specific characteristics and values overridden for that aa-sub.

Show command output display the combined set of attributes that apply to the aa-sub.

The `override` commands can only be used if there is already an app-profile assigned to the aa-sub, otherwise, the overrides are rejected.

The app-profile attribute override is assigned to a specific aa-sub (SAP, spoke SDP) within the AA Group:partition with where the subscriber exists. While subscriber names are unique, the Group:partition policy context where apps, app-profiles and ASO characteristics are defined is relevant to the override context.


AA-Sub Scale Mode

An AA VPN policy is generally administered using a per-site (aa-subscriber) policy attribute assignment (ASO override), as opposed to a service profile based model commonly used for residential services. Due to this, the number of attributes and values of ASOs that can be needed in an AA VPN service will be much larger than ASO scale needed for residential uses.

On the other hand, the number of AA subscribers needed per node and per ISA is much smaller for VPN services, and the size of each in bandwidth is generally much larger than residential.

In conjunction with App-profile ASO override, a new capability is added to place an AA-group into a mode optimized for VPN scale requirements:

```
config>sa>aa-group>aa-sub-scale {residential|vpn } (residential is default)
```

In the default residential mode, the limits are unchanged from previous releases.
Parent Services Supporting Transit AA Subs

Transit AA subs are supported on the following Layer 3 SAPs or spoke SDPs that support AA divert:

- IES
- VPRN
- VPLS
- Epipe
- Ipipe

The transit AA-subs within a given parent AA sub can be displayed using the show aa sub using command.

All packets are accounted for once in the ISA records. Therefore, transit AA sub counts do not count against the parent SAP in reporting.

Transit AA-Sub App-Profile

The app-profile assigned to the aa-sub-id affects both stats and control of the policy. App-profiles are assigned to the transit AA-subs either explicitly when the transit-aa-sub is created, or by default (when not specified) according to a default app-profile configured in a transit-ip-policy. This allows transit AA subs to be treated with a different default app-profile than the app-profile (default or specified) set against the parent aa sub. The number of aa-sub stats used per ISA is proportional to the number of AA subscribers including transit subscribers subs are added.
Transit IP Policy

A transit IP policy is associated with the parent (divert) SAP/SDP to define how transit AA subs are created within that parent. The transit IP policy must be defined before it can be assigned to a parent. Transit subs can be created by the following methods:

- Static — CLI/SNMP configuration of a transit aa-sub is done within the transit-ip-policy
- DHCP authentication
- RADIUS accounting to PCRF

The IP addresses defined in the transit-policy for a transit sub are full /32 IP addresses. Multiple IP addresses (from any prefix/ pool) can be assigned to a single transit AA sub. IP addresses must be unique within a transit IP policy, but can be re-used in separate policies (since they have parent specific context).

The transit policy contains the default app-profile for the transit sub if a transit policy is created but app-profile is not specified. An app-profile can be later explicitly assigned to the transit sub after the sub is created (using RADIUS COA, DHCP or static).

For dynamic transit subs, a sub-ident-policy (also used by ESM to associate sub ID policies to a SAP) can now also be associated with the AA-sub parent by defining the sub-ident policy in the transit IP policy. This determines how sub identifying strings are derived from DHCP option 82 fields. The policy also contains app-profile-map which maps the strings to the defined app-profiles. Transit subs do not use the sla-profile or sub-profile aspects of the sub-ident-map.

In the case of multi-homed transit subs, the transit-ip-policy must be the same on both nodes of the multi-homed parent link to ensure consistency of sub context and policy.

There are no configurable limit hosts per sub per sub (this is similar to lease-populate which limits the number of dynamic hosts per SAP), or, limit the number of transit subs per transit ip policy (parent). This is a function for the PE doing subscriber management.

If transit sub resource limits are exceeded (hosts per sub, or subs per ISA) the transit sub creation is blocked (for both static and dynamic models).

There is a per-ISA group/partition show list of AA-subs in a transit-ip-policy which includes a parent field for transit subs (static versus dynamic identified).

Persistent AA statistics is supported dynamic transit AA subs, ensuring that accounting usage information is not lost when the sub disconnects prior to reporting interval end.
Static Transit AA-Subs

Static (through CLI/SNMP) provisioning of transit AA-sub is supported. A profile policy override to set policy characteristics by ASO (as opposed to within an app-profile) is supported only for statically configured transit AA subs.

If there is an IP address conflict between a static and dynamic transit sub, the static takes precedence (per ESM). If the static is configured first, the dynamic transit sub will be rejected. If the dynamic is created first, a warning is provided before removing the dynamic transit sub and notifying the sub-manager by COA failure.

DHCP Transit IP AA-Subs at DHCP Relay Node

DHCP-based transit sub creation provides a sub ID and lease time for IP addresses, correlated to ESM/subscriber context in the PE.

The 7750 DHCP relay agent creates dynamic DHCP AA-subs when the DHCP ACK is received from the DHCP server, including the sub name, IP address and app-profile from DHCP Option 67 (if present) when the DHCP ACK messages passes through AA node to the downstream subscriber-edge node. If there is no app-profile assigned when the transit aa-sub is created, a default transit aa-sub app-profile is used (configured in the transit-ip-policy assigned against the divert parent aa-sub).

This is compatible with the ESM 7x50 edge as well as third-party BRAS and CMTS.

Dynamic AA-sub stats records are persistent across modem reset/session releases. The end of accounting records are created when transit subs are released.

Multiple IPs per transit AA sub are determined by seeing a common the DHCP Option 82 cct ID.
RADIUS Transit AA-Subs

Transit subs can be dynamically provisioned by RADIUS accounting start messages forwarded by the RADIUS AAA server to a RADIUS sub-manager function at the OSS layer (5780 DSC). This RADIUS sub manager manages dynamic transit AA subs on the appropriate ISA and transit-ip-policy based on the RADIUS accounting information. The interface for the sub manager to configure transit AA subs is RADIUS COA messages, which are acknowledged with a COA success message to the sub manager.

If a dynamic transit sub cannot be created as requested by a COA due to resource constraints or conflicts, the node replies to the sub manager with a COA fail message so that retries will not continue. This message should contain information as to the cause of the rejection. Multiple IPs per sub are allowed when common sub-ID names are seen, but with differing IP hosts.

When a RADIUS update/COA message is seen, it could contain a modified IP address or app-profile for an existing transit sub which is accepted without affecting transit aa subscriber statistics. These transit AA-sub are removed by the sub manager when a RADIUS accounting stop message is received.

Figure 15: RADIUS COA Example
The attributes in RADIUS COA that identify the downstream transit AA-subs are:

- Downstream BRAS/ CMTS: NAS-port-ID
- IP address: framed-ip-address
- Subscriber ID: per RADIUS accounting sub-id-string
Transit AA-Sub Persistence

Transit AA subs can be persistent within a single node, since, in some cases, there is not a dual-node BNG subscriber redundancy configuration. This allows a single node that has dynamically created transit subs to retain the subscriber state, context, and stats across a node or ISA reboot.

If dynamic transit AA subs are released, renewed or otherwise changed during an outage or reboot of a transit AA node, the sub manager will notify the transit node of these changes.

Policers for Transit AA-Subs

AA-sub per-subscriber policers can provide per SAP policing for the parent SAP, with transit AA-sub subs each supporting distinct per-sub policers within the parent. Transit AA sub policer counts will not affect the parent policer. There is no hierarchy unless system-wide policers are referred to by both the parent aa-sub and transit aa-sub. AA policers are supported on a transit subscriber basis, across all (multiple) IP hosts per sub.

ISA Host IOM for Transit Subs

The AA divert IOM is not impacted by transit aa subs in the divert parent. The ISA host IOM egress datapath functions to convert the parent SAP into transit AA-subs that are then handled by the ISA consistent with all other AA-sub features. The ISA itself treats all AA-subs equally regardless of whether the AA sub is from ESM, from a SAP, or from a transit subscriber in a parent SAP/spoke.
Application Identification

This section discusses the following topics:

- Application Assurance Identification Components on page 66
- Protocol Signatures on page 68
- Custom Protocols on page 69
- Protocol Shutdown on page 70
- Supported Protocol Signatures on page 71
- Application Groups on page 71
- Applications on page 71
- Application Filters on page 72

Application identification means there is sufficient flow information to provide the network operator with a view to the underlying nature and value of the content. Application ID does not include:

- Anti-virus signatures per IPS/UTM.
- Content inspection (e-mail, text, picture, or video images). The payload data content of flows is typically not examined as part of the application identification.

Application Assurance can identify and measure non-encrypted IP traffic flows using any available information from Layer 2-Layer 7, and encrypted IP traffic flows using heuristic techniques.

Application Assurance attempts to positively identify the protocols and applications for flows based on a pattern signature observation of the setup and initial packets in a flow. The system correlates control and data flows belonging to the same application. In parallel, statistical and behavioral techniques are also used to identify the application. Until identified, the flow will not have a known application and will be treated according to the default policies (AQP policies defined using all or any ASO characteristics, subscriber Id and traffic direction as match criteria) for traffic for that AA subscriber, app-profile and direction (packets will be forwarded unless an action is configured otherwise). If the identification beyond OSI Layer 2 is not successful, the flow will be flagged as an unknown protocol type, (for example unknown_tcp or unknown_udp). The unknown traffic is handled as part of all application statistics and policy, including generation of stats on the volume of unknown traffic.

Application Assurance allows operators to optionally define port-based applications for “trusted” TCP or UDP ports. Operators must explicitly identify a TCP/UDP port(s) in an application filter used for “trusted” port application definition and specify whether a protocol signature-based application identification is to be performed on a flow or not. Two options are available:
• If no protocol signature processing is required (expected to be used only when (A) AQP policy must be performed from the first packet seen, (B) the protocol signature processing requires more than 1 packet to positively identify a protocol/application, and (C) no other application traffic runs over a given TCP/UDP port), the first packet seen by AA ISA for a given flow on that TCP/UDP port will allow application identification. The traffic for a given flow will be identified as “trusted tcp/trusted_udp” protocols.

• If protocol signature verification of an application is required (expected to be used only when (a) AQP policy must be performed from the first packet seen, (b) the protocol signature processing requires more than 1 packet to positively identify a protocol/application, but (c) other application traffic may run over a given TCP/UDP port, for example TCP port 80), the first packet seen will identify the application but protocol signature-based analysis continues. Once the identification completes, the application is re-evaluated against the remaining application filters allowing detection and policy control of unexpected applications on a “trusted” port.

At Application Assurance system startup or after an AA ISA activity switch, all open flows are marked with the “existing” protocol signature and have a policy applied according to an application based on the “existing” protocol until they end or the identification of an in-progress flow is possible. Statistics are generated.

From the first packet of a flow, a default per AA subscriber AQP policy is applied to every packet. Once an application is identified, subsequent packets for a flow will have AA subscriber and application-specific AQP applied. The AA-generated statistics for the flow with AA subscriber and application context are collected based on the final determination of the flow’s application. A subset of the applications may be monitored on an ongoing basis to further refine the identification of applications carried with the traffic flow and to identify applications using an external application wrapper to evade detection.
Application Assurance Identification Components

Figure 16 shows the relationship between the Application Assurance system components used to identify applications and configure Application Assurance related capabilities. Each ID-related component is defined as follows:

- Protocol signatures
- Application filters
- Applications
- Application groups
Table 5 provides an overview of how those various components used in Application Assurance to recognize types of flows/sessions.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol Signature</td>
<td>Alcatel-Lucent’s proprietary component of AA flow identification provided as part of AA S/W load to identify protocols used by clients. Where a protocol is defined as an agreed upon format for transmitting data between two devices.</td>
<td>Tftp, iMap, msn-msgr, RTP, emule, http_video, bittorrent, SIP</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: Alcatel-Lucent’s protocol signatures do not rely on IP port numbers to identify a TCP/UDP port based protocols / applications in order to avoid eliminate false-positives but allow operators to define application filters if a port-based identification is deemed adequate (see an example below).</td>
<td></td>
</tr>
<tr>
<td>Application Filter</td>
<td>Operator configurable, optional component of AA flow identification that uses any combination of protocol signatures, server IP address and port, flow set-up direction, configurable expressions (for example an HTTP string match) to identify user’s traffic.</td>
<td>http_video + IP address of partner’s video server or http_video + an HTTP string to identify partner’s video content TCP or UDP + TCP/UDP port number to identify a TCP or UDP based protocol or application.</td>
</tr>
<tr>
<td>Application</td>
<td>Operator configurable, optional component of AA flow identification that allows defining any specific forms of traffic to and from end user clients by combining application filter entries.</td>
<td>Google Talk, POP3, YouTube, iTunes, Shoutcast</td>
</tr>
<tr>
<td>Application Group</td>
<td>Operator configurable, optional component of AA flow identification that allows grouping of similar end use applications using operator defined names and groups.</td>
<td>IM, Mail, Multimedia, P2P, Tunneling, Web, Other</td>
</tr>
<tr>
<td>Clients</td>
<td>End user programs that generate user traffic for applications and protocols, and that are used in a process of AA flow identification verification.</td>
<td>The list of clients is constantly evolving as new clients or versions are introduced in the marketplace. The following example illustrates clients that may be used to generate Application traffic matching BitTorrent application defined using BitTorrent and DHT protocol signatures: Limewire, BitTorrent, Azureus, Ktorrent, Transmission, Utorrent</td>
</tr>
</tbody>
</table>
Protocol Signatures

The set of signatures used to identify protocols is generated by Alcatel-Lucent and included with the Application Assurance software load. The signature set includes:

- The protocols that can be identified with this load, using a combination of pattern and behavioral techniques. The protocols are used in generating statistics by protocol, and are used as input in combination with other information to identify applications.
- Pattern signatures are the set of pattern-match signatures used in analysis.
- Behavior signatures are the set of diagnostic techniques used in analysis.

Dynamic upgrades of the signatures in the system are implemented by invoking an `admin application-assurance upgrade` command and then performing AA ISA activity switches.

The protocol signatures are included in aa-isa.tim software load which is not tightly coupled with software releases allowing for protocol signature updates without upgrading and impacting of routing/forwarding engines as part of an ISSU upgrade that updates only the AA ISA software. Refer to upgrade procedures described in the 7750 SR and/or 7450 ESS Release Notes for detailed information.

Since protocol signatures are intended to be the most basic block of Application Identification, other AA components like Application Filters are provided to further customize Protocol Signatures allowing operators to customize their applications and to reduce a need for a new Protocol Signature load when a new Application may need to be identified. This architecture gives operators more flexibility in responding to ever changing needs in application identifications.

Signature upgrade without a router upgrade is allowed within a major router release independently of system ISSU limits. An AA ISA signature upgrade is supported before the first ISSU router release (for example, operators can upgrade signatures for pre-ISSU minor releases).

In addition, any router release from ISSU introduction release can run any newer aa-isa.tim image within the same major release by performing an aa-isa.tim single step upgrade. For example, release 8.4 may be upgraded in a single step to run release 8.14 of isa-aa.tim.

Each protocol, except internal protocols used for special-case processing statistic gathering (like “cut-through”, for example), can be referenced in the definition of one or multiple applications (through the App-Filter definition). Assignment of a supported protocol to an app-filter or application is not mandatory. Protocols not assigned to an application are automatically mapped by the system to the default “Unknown” application.
Custom Protocols

Custom protocols are supported using configurable strings (up to 16 hex octets) for pattern-matched application identification in the payload of TCP or UDP based applications (mutually exclusive to other string matches in an app-filter).

The match is specified for the “client-to-server”, “server-to-client”, or “any” direction for TCP based applications, and in the “any” direction for UDP based applications.

There is a configurable description and custom protocol id for a protocol, with configurable shutdown. When disabled, traffic is identified as if the protocol was not configured.

Custom protocols and ALU-provided protocols are functionally equivalent. Custom protocols are used in application definition without limitations (all app-filter entries except strings are supported). Collection of custom protocol statistics on a partition/ISA group/special study sub level is supported.
Protocol Shutdown

The protocol shutdown feature provides the ability for signature upgrades without automatically affecting policy behavior, especially if some or even all new signatures are not required for a service. All new signatures are disabled on upgrade by default to ensure no policy/service impact because of the signature update.

All protocols introduced at the R1 stage of a given release are designated as “Parent” signatures for a given release and cannot be disabled.

Within a major release, all protocols introduced post-R1 of a major release as part of any isa-aa.tim ISSU upgrade are by default shutdown. They must be enabled on a per-protocol basis (system-wide) to take effect.

When shutdown, post R1-introduced protocols do not change AA behavior (app-id, policy, statistics are as before the protocol introduction), for example, traffic maps to the parent protocol on which the new signature is based. In cases where there is more than one parent protocol, all traffic is mapped to a single, most-likely, parent protocol. For example if 80% of a new protocol has traffic mapping to unknown_tcp, and 20% mapping to another protocol(s), unknown_tcp would be used as parent.

Enabling/disabling of a new protocol takes affect for new flows only. The current status (enabled/shutdown) of a signature and the parent protocol is visible to an operator as part of retrieving protocol information through CLI/SNMP.
Supported Protocol Signatures

Protocol signatures are release independent and can be upgraded independently from the router’s software and without impacting router’s operations as part of an ISSU upgrade. A separate document outlines signatures supported for each signature software load (isa-aa.tim). New signature loads are distributed as part of the SR/ESS maintenance cycle. Traffic identified by new signatures will be mapped to an “Unknown” application until the AA policy configuration changes to make use of the newly introduced protocol signatures.

Application Groups

Application groups are defined as a container for multiple applications. The only application group created by default is Unknown. Any applications not assigned to a group are automatically assigned to the default Unknown group. Application groups are expected to be defined when a common policy on a set of applications is expected, yet per each application visibility in accounting is required. The application group name is a key match criteria within application QoS policy rules.

Applications

The application context defines and assigns a description to the application names supported by the application filter entries, and assigns applications to application groups.

- Application name is a key match criteria within application QoS policy rules, which are applied to a subscribers IP traffic.
- Each application can be associated with one of the application groups provided by Application Assurance.

The Application Assurance system provides no pre-defined applications other than Unknown. Applications must be explicitly configured. Any protocols not assigned to an application are automatically assigned to the default Unknown application. Alcatel-Lucent provides sets of known-good application/app-group configurations upon request. Contact the technical support staff for further information.

The applications are used by Application Assurance to identify the type of IP traffic within the subscriber traffic.

The network operator can:

- Define unique applications.
- Associate applications with an application group. The application group must already be configured.
Application Filters

Application filters (app-filter) are provided as an indirection between protocols and applications to allow the addition of variable parameters (port number, IP addresses, etc.) into an application definition. An application filter is a numbered rule entry that defines the use of protocol signatures and other criteria to define an application. Multiple rules can be used to define what constitutes an application but each rule will map to only one application definition.

The system concept of application filters is analogous to IP filters. Match of a flow to multiple rules is possible and is resolved by picking the rule with the lowest entry number that matches. A flow will only ever be assigned to one application.

The following criteria can be assigned to an application filter rule entry:

- Unique entry ID number
- Application name
- Flow setup direction
- Server IP address
- Server port
- Protocol signature
- IP protocol number
- String matches against Layer 5+ protocol header fields (for example, a string expression against HTTP header fields)

The application must be pre-configured prior to using it in an app-filter. Once defined, the new application names can be referenced.
Statistics and Accounting

Application Assurance statistics provide the operator with information to understand application usage within a network node. Application Assurance accounting aggregates the flow information into per application group, per application, per protocol reports on volume usage during the last accounting interval. This information is then sent to a statistics collector element for network wide correlation and aggregation into customized graphical usage reports. Application Assurance uses and benefits from the rich accounting infrastructure and the functionality it provides to control accounting policy details.

The following types of accounting volume records are generated and can be collected:

- Per ISA group and partition record for each configured application group
- Per ISA group and partition record for each configured application
- Per ISA group and partition record for each configured protocol
- Per each AA subscriber record with operator-configurable field content using custom AA records for operator-selected subset of protocols, applications and application groups.
- Per AA subscriber per each configured application record (special study mode)
- Per AA subscriber per each supported protocol record (special study mode)

Per AA flow statistics are provided as described in the cflowd section.

Refer to the OS System Management Guide for information on general accounting functionality.

Per-AA-Subscriber Special Study

The system can be configured to generate statistical records for each application and protocol that the system identifies for specific AA subscribers. These capabilities are disabled by default but can be enabled for a subset of AA subscribers to allow detailed monitoring of those AA subscriber’s traffic.

Per-aa-sub per-application and per-aa-sub per-protocol records are enabled by assigning individual AA subscribers to “special study” service lists. The system and ISA group limit the number of AA subscribers in this mode to constrain the volume of stats generated. When an AA subscriber is in a special study mode, one record for every application and/or one record for every protocol that are configured in the system are generated for that subscriber. For example, if 500 applications are configured and 200 protocols are identified, 700 records per AA subscriber will be generated, if the AA subscriber is listed in both the per-aa-sub-application and per-aa-sub protocol lists.
System Aspects

Application Assurance uses the existing redundant accounting and logging capability of the for sending application and subscriber usage information, in-band or out-of-band. Application Assurance statistics are stored using compressed XML format with other system and subscriber statistics in compact flash modules on the redundant SF/CPMs. A large volume of statistics can be expected under scaled scenarios when per-AA-subscriber statistics/accounting is enabled.

AA accounting and statistics can be deployed as part of other system functionality as long as the system’s function is compatible with AA accounting or as long as the system-level statistics can become application-aware due to, for example, AA ISA-based classification. An example of this feature interaction includes volume and time-based accounting where AA-based classification into IOM queues with volume and time accounting enabled can, for instance, provide different quota/credit management for off-net and on-net traffic or white/grey applications.
**Application Assurance Volume Statistics and Accounting**

Application Assurance is configured to collect and report on the following statistics when at least one AA ISA is active. The default Application Assurance statistics interval is 15 minutes.

Statistics to be exported from the node are aggregated into accounting records, which must be enabled in order to be sent. By default, no records are sent until enabled. Each record template type is enabled individually to control volume of statistics to the desired level of interest. Only non-zero records are written to the accounting files for all AA subscriber based statistics to reduce the volume of data.

The operator can further select a subset of the fields to be included in per-AA-subscriber records and whether to send records if no traffic was present for a given protocol or application, for example, sending only changed records.

Each record generated contains the record fields as described in Table 6. The header row represents the record type.

<table>
<thead>
<tr>
<th>Record Fields</th>
<th>Description</th>
<th>Group/Partition</th>
<th>Group/Partition</th>
<th>Group/Partition</th>
<th>Group/Partition</th>
<th>Group/Partition</th>
<th>Group/Partition</th>
<th>Group/Partition</th>
<th>Group/Partition</th>
<th>Group/Partition</th>
<th>Group/Partition</th>
<th>XML Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Group</td>
<td>Name</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>data name</td>
</tr>
<tr>
<td>Application</td>
<td>Name</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>data name</td>
</tr>
<tr>
<td>Protocol</td>
<td>Name</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>data name</td>
</tr>
<tr>
<td>Aggregation Type ID</td>
<td>ID (can be protocol, application or application group record)</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>agg-type-name</td>
</tr>
<tr>
<td># Active Subscribers</td>
<td># of subscribers who had a flow of this category during this interval</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>ns sub</td>
</tr>
<tr>
<td># allowed flows from-sub</td>
<td># of new flows that were identified and allowed</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>sfa</td>
</tr>
<tr>
<td># allowed flows to-sub</td>
<td>As above in opposite direction</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>nfa</td>
</tr>
<tr>
<td>Record Fields</td>
<td>Description</td>
<td>Group/Partition</td>
<td>Group/Partition</td>
<td>Group/Partition</td>
<td>Group/Partition</td>
<td>AA-Sub Custom</td>
<td>AA-Sub Special Study Protocol</td>
<td>XML Name</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>
<td>-----------------------------</td>
<td>--------</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td># denied flows from-sub</td>
<td>the # of new flows that were identified and denied</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>sfd</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td># denied flows to-sub</td>
<td>As above in opposite direction</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>nfd</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td># Active flows from-sub</td>
<td># of flows that were either: closed, opened &amp; closed, opened, or continued during this interval</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>saf</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td># active flows to-sub</td>
<td>As above, in opposite direction</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>naf</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total packets from-sub</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>spa</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total packets to-sub</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>npa</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total bytes from-sub</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>sba</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total bytes to-sub</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>nba</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total discard packets from-sub</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>spd</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total short flows</td>
<td>Number of flows with duration &lt;= 30 seconds that completed up to the end of this interval</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>sdf</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total medium flows</td>
<td>Number of flows with duration &lt;= 180 seconds that completed up to the end of this interval</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>mdf</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total long flows</td>
<td>Number of flows with duration &gt; 180 seconds that completed up to the end of this interval</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>ldf</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total discard packets to-sub</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>npd</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total discard bytes from-sub</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>sbd</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total discard bytes to-sub</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>nbd</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total flows completed</td>
<td># of to- and from-subscriber flows that have been completed up to the reported interval.</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>tfc</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Record Fields</td>
<td>Description</td>
<td>Group/Partition</td>
<td>Group/Partition</td>
<td>Group/Partition</td>
<td>Group/Partition</td>
<td>AA-Sub Custom</td>
<td>AA-Sub Special Study</td>
<td>XML Name</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>
<td>----------------------</td>
<td>----------</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total flow duration</td>
<td>Duration, in seconds, of all flows that have been completed up to the reported interval.</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>tfd</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>From AA Sub: Maximum throughput byte count</td>
<td>Maximum of all total byte counts recorded for throughput intervals within this accounting interval for traffic originated by AA subscriber for a given application/app-group. AA-ISA discarded traffic is not included.</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>sbm</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>From AA Sub: Packet count corresponding to the max. throughput byte count interval.</td>
<td>Packet count for the throughput interval with the maximum byte count value for traffic originated by AA subscriber for the application/app-group. AA-ISA discarded traffic is not included.</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>spm</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>To AA Sub: Max throughput time slot index</td>
<td>UTC time that corresponds to the end of the 5-minute throughput interval where the max throughput byte count was detected.</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>smt</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>To AA Sub: Maximum throughput byte count</td>
<td>Maximum of all total byte counts recorded for throughput intervals within this accounting interval for traffic originated from Network towards AA subscriber for a given application/app-group. AA-ISA discarded traffic is not included.</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>nbm</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>To AA Sub: Packet count corresponding to the max. Throughput byte count interval.</td>
<td>Packet count for the throughput interval with the maximum byte count value for traffic originated from network towards AA subscriber for a given application/app-group. AA-ISA discarded traffic is not included.</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>npm</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Table 6: Application Assurance Statistics Fields Generated per Record (Accounting File)

<table>
<thead>
<tr>
<th>Record Fields</th>
<th>Description</th>
<th>AA-Sub Custom</th>
<th>AA-Sub Special Study Protocol</th>
<th>XML Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>From AA Sub: Max throughput time slot index</td>
<td>UTC time that corresponds to the end of the 5-minute throughput interval where the max throughput byte count was detected.</td>
<td>X</td>
<td></td>
<td>nmt</td>
</tr>
<tr>
<td>From AA Sub: Maximum throughput byte count</td>
<td>Maximum of all total byte counts recorded for throughput intervals within this accounting interval for all traffic originated by AA subscriber. AA-ISA discarded traffic is not included.</td>
<td>X</td>
<td></td>
<td>sbm</td>
</tr>
<tr>
<td>From AA Sub: Packet count corresponding to the max. Throughput Byte Count interval.</td>
<td>Packet count for the throughput interval with the maximum byte count value for traffic originated by AA subscriber. AA-ISA discarded traffic is not included.</td>
<td>X</td>
<td></td>
<td>spm</td>
</tr>
<tr>
<td>From AA Sub: Max throughput time slot index</td>
<td>UTC time that corresponds to the end of the 5-minute throughput interval where the max throughput byte count was detected.</td>
<td>X</td>
<td></td>
<td>smt</td>
</tr>
<tr>
<td>To AA Sub: Maximum throughput byte count</td>
<td>Maximum of all total byte counts recorded for throughput intervals within this accounting interval for traffic originated from network towards AA subscriber. AA-ISA discarded traffic is not included.</td>
<td>X</td>
<td></td>
<td>nbm</td>
</tr>
<tr>
<td>To AA Sub: Packet count corresponding to the max. Throughput Byte Count interval.</td>
<td>Packet count for the throughput interval with the maximum byte count value for traffic originated from network towards AA subscriber. AA-ISA discarded traffic is not included.</td>
<td>X</td>
<td></td>
<td>npm</td>
</tr>
<tr>
<td>To AA Sub: Max throughput time slot index</td>
<td>UTC time that corresponds to the end of the 5-minute throughput interval where the max throughput byte count was detected.</td>
<td>X</td>
<td></td>
<td>nmt</td>
</tr>
</tbody>
</table>
The records are generated per ISA group and partition, with an ISA group identified by the group ID (XML field name “aaGroup”), partition identified by the partition ID (XML field name “aaPart name”) and per AA subscriber (if applicable) with the AA subscriber identified by the ESM subscriber name, SAP ID (XML field name “subscriber name”, “sap name” or “spoke SDP ID” respectively).

The date, time, and system ID for the records will be visible as part of the existing accounting log capability, thus does not need to be contained inside the Application Assurance records themselves.
Configurable AA-Subscriber Statistics Collection

Existing average volume statistics collected over an accounting interval are extended to provide the maximum volume (bytes/packets) recorded for a throughput measurement period (5 minutes) within an accounting interval. These additional statistics improve accuracy for the access-pipe right-sizing service.

Maximum throughput statistics can be enabled for the selected applications and/or application groups enabled for custom per AA statistics. In addition, the operator can enable (disabled by default) per AA-subscriber “Max-throughput” statistics for total (/aggregate) subscriber traffic, independent of defined applications/application-groups.

Maximum throughput statistics records are allocated from the 2048K records available for use for per subscriber records.

Maximum throughput statistics are not provided for the protocols enabled for custom per AA statistics.
AA-Performance Record for ISA Load

The AA-performance statistics record provides visibility of ISA loading related statistics to allow operational monitoring and planning of ISA overload:

1. Provides end of reporting interval snapshot of current values of the parameters listed in below into a per AA-ISA Planning record. “Current” is the value of a counter at the end of the reporting interval, for rate based values this is the ~10sec short term current rate used in CLI statistics.
2. Provides time-based averages during record interval of the above values: Average(I)
3. Provides peak values of the above values in the reporting interval: Peak(I)

The 5670 RAM provides further analysis and thresholding triggers based on these ISA statistics, suitable for long-range planning trends such as average number of subs or peak numbers of flows.

The node per-ISA planning record values are cleared on accounting read (per all accounting records). Not reading the records means that the average and peak values are the values for the last reporting interval. The time last read is indicated in the record.

The AA performance planning record contains the following fields:

Table 7: AA Performance Planning Record Fields

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Current</th>
<th>Average(I)</th>
<th>Peak(I)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISA ID</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>active flows</td>
<td># flows</td>
<td># flows</td>
<td># flows</td>
</tr>
<tr>
<td>flow setup rate</td>
<td>flows/sec</td>
<td>flows/sec</td>
<td>flows/sec</td>
</tr>
<tr>
<td>traffic rate</td>
<td>bits/sec</td>
<td>bits/sec</td>
<td>bits/sec</td>
</tr>
<tr>
<td>Packet rate</td>
<td>packets/sec</td>
<td>packets/sec</td>
<td>packets/sec</td>
</tr>
<tr>
<td>active subs</td>
<td># subs</td>
<td># subs</td>
<td># subs</td>
</tr>
<tr>
<td>downloaded subs</td>
<td># subs</td>
<td># subs</td>
<td># subs</td>
</tr>
<tr>
<td>flow resources in use (active flows + wildcard flows)</td>
<td># flows</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ISA AA sub stats resource allocation</td>
<td># stats records</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ISA capacity cost</td>
<td>sum of cost of active AA subs</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ISA Transit Subs</td>
<td># subs</td>
<td></td>
<td></td>
</tr>
<tr>
<td>diverted traffic</td>
<td>(packets, octets)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>entered ISA</td>
<td>(packets, octets)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 7: AA Performance Planning Record Fields (Continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Current</th>
<th>Average(l)</th>
<th>Peak(l)</th>
</tr>
</thead>
<tbody>
<tr>
<td>policy discards in ISA</td>
<td>(packets, octets)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>congestion discards in ISA</td>
<td>(packets, octets)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>error discards in ISA</td>
<td>(packets, octets)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>policy bypass errors</td>
<td>(packets, octets)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>returned traffic</td>
<td>(packets, octets)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Cflowd AA Records

AA ISA allows cflowd records to be exported to an external cflowd collector. The cflowd collector parameters (such as IP address and port number) are configured per application assurance group. All cflowd records collected for both volume and per-flow TCP performance are exported to the configured collector(s). AA ISA supports cflowd Version 10/ IPFIX.

A cflowd record is only exported to the collector once the flow is closed/terminated.

TCP Application Performance

AA ISA allows an operator to collect per flow TCP performance statistics to be exported through cflowd v10/IPFIX.

The operator can decide to collect TCP performance for sampled flows within a TCP enabled group-partition-application/application-group. The flow sampling rate is configurable on per ISA-group level. For example a flow sample rate of 10 means that every 10th TCP flow is selected for TCP performance statistics collection. Anytime a flow is sampled (selected for TCP performance statistics collection) its mate flow in reverse direction is also selected. This allows collectors to correlate the results from the two flows and provide additional statistics (such as round-trip delay). Per-flow cflowd TCP performance records are exported to the configured collector(s) upon flow closure. The system can gather per flow TCP performance statistics for up to 307,200 concurrent flows.

Per-flow TCP performance can be enabled (or disabled) per application/app-group per partition per AA ISA-group.

Volume Statistics

AA ISA allows an operator to collect per flow volume statistics to be exported for any group partition. The packet sampling rate is configurable per AA- ISA-group level. For example, a packet sample rate of 10 means that one of every 10 packets is selected for volume statistics collection. If a flow has at least a single packet sampled for cflowd volume statistics, its per-flow cflowd volume record is exported to the configured collector upon flow closure.
Audio/Video (A/V) Application Performance

AA-ISA integrates a third party audio/video performance measurement software stack to perform VoIP and video MOS-related measurements for RTP based A/V applications.

A passive monitoring technology estimates transmission quality of voice and video over packet technologies by considering the effects of packet loss, jitter and delay in addition to the impairments caused by encoding/decoding technology. A rich set of diagnostic data is provided that can be used to help network managers identify a variety of problems that could impact the quality of voice and video streams and/or service level agreements (SLAs).

This feature provides:

- Call quality analysis using optimized ITU-T G.107, such as listening and conversational quality MOS and R-factor scores – MOS-LQ, MOS-CQ R-LQ and R-CQ.
- Measurements of perceptual effects of burst packet loss and recency using ETSI TS 101 29-5 Annex E Extensions
- Measurements and analysis of RTCP XR (RFC 3611, RTP Control Protocol Extended Reports (RTCP XR)) VoIP metrics payloads.

Once a flow terminates, AA-ISA format the flow MOS parameters into a cflowd record and forwards the record to a configured IPFIX /10 Cflowd collector (such as 5670 RAM). The collector then summarizes these records using route of interest information (source/destinations). In addition, RAM provides the user with statistics (min/max/avg values) for the different performance parameters that are summarized.

Like TCP performance, per flow audio/video performance can be enabled (or disabled) per application/app-group per partition per AA-ISA-group.

The operator can decide to collect RTP A/V performance for sampled RTP flows within an RTP A/V enabled group-partition-application/application-group. The flow sampling rate is configurable on per ISA group level. For example a flow sample rate of 10 means that every 10th RTP flow is selected for RTP performance statistics collection. Anytime a flow is sampled (selected for RTP A/V performance statistics collection) its mate flow reverse direction is also selected. The system can gather per flow RTP A/V performance statistics for up to 6000 voice calls.
Policy Actions

Application profiles typically contain one or more characteristics defined as Application Service Options (ASOs). The ASO’s characteristics can comprise a menu of customer or/and operator visible network functionality available for AA subscribers, for example, service tier: Bronze, Silver, or Gold, partner’s premium content such as real-time live video streaming, or VPN customer or application QoS policy identifier for example: AA QoS template 1, Customer X QoS template 1, etc. This optional inclusion of ASO characteristics, which are then later referenced by the application QoS policy (AQP) rules, allows flexible function-based application service offerings.

AQP defines the application policy rules when actions requiring application-awareness are to be performed against the traffic. Application QoS policy would typically use ASO characteristics assigned to the AA subscriber together with other methods to match flows to actions to be performed. Those methods include, among others, application groups, DSCP values, or server IP address.

AQP rules consist of match and action criteria:

- **Match**: Refers to application identification determined by application and application group configuration using protocol signatures and user-configurable application filters that allow customers to create a wide range of identifiable applications. To further enhance system-wide per subscriber/service management user configurable application groups are provided.

- **Actions**: Defines AA actions to be applied to traffic, a set of actions to apply to the flows like bandwidth policing, packet discards, QoS remarking and flow count or/and rate limiting.
Application Assurance Policers

The rate limit (policer) policy actions provide the flow control mechanisms that enable rate limiting by application and/or AA subscriber(s).

There are four types of policers:

- Flow rate policer monitors a flow setup rate.
- Flow count limits control the number of concurrent active flows
- Single-rate bandwidth policers monitor bandwidth using a single rate and burst size parameters.
- Dual-rate bandwidth rate policers monitor bandwidth using CIR/PIR and CBS/MBS. These can only be used at the per-subscriber granularity.

Once a policer is referred to by an AQP action for one traffic direction, the same policer cannot be referred to in the other direction. This also implies that AQP rules with policer actions must specify a traffic direction other than the “both” direction.

Table 8 illustrates a policer's hardware rate steps for AA ISA:

<table>
<thead>
<tr>
<th>Hardware Rate Steps</th>
<th>Rate Range (Rate Step x 0 to Rate Step x 127 and max)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.5Gb/sec</td>
<td>0 to 64Gb/sec</td>
</tr>
<tr>
<td>100Mb/sec</td>
<td>0 to 12.7Gb/sec</td>
</tr>
<tr>
<td>50Mb/sec</td>
<td>0 to 6.4Gb/sec</td>
</tr>
<tr>
<td>10Mb/sec</td>
<td>0 to 1.3Gb/sec</td>
</tr>
<tr>
<td>5Mb/sec</td>
<td>0 to 635Mb/sec</td>
</tr>
<tr>
<td>1Mb/sec</td>
<td>0 to 127Mb/sec</td>
</tr>
<tr>
<td>500Kb/sec</td>
<td>0 to 64Mb/sec</td>
</tr>
<tr>
<td>100Kb/sec</td>
<td>0 to 12.7Mb/sec</td>
</tr>
<tr>
<td>50Kb/sec</td>
<td>0 to 6.4Mb/sec</td>
</tr>
<tr>
<td>10Kb/sec</td>
<td>0 to 1.2Mb/sec</td>
</tr>
<tr>
<td>8Kb/sec</td>
<td>0 to 1Mb/sec</td>
</tr>
<tr>
<td>1Kb/sec</td>
<td>0 to 127Kb/sec</td>
</tr>
</tbody>
</table>
Policers are unidirectional and are named with these attributes:

- Policer name
- Policer type: single or dual bucket bandwidth, flow rate limit, flow count limit.
- Granularity: select per-subscriber or system-wide
- Parameters for flow setup rate (flows per second rate)
- Parameters for flow count (maximum number of flows)
- Rate parameters for single-rate bandwidth policer (PIR)
- Parameters for two-rate bandwidth policer (CIR, PIR)
- PIR and CIR adaptation rules (min, max, closest)
- Burst size (CBS and MBS)
- Conformant action: allow (mark as in-profile)
- Non-conformant action: discard, or mark with options being in profile and out of profile

Policers allow temporary oversubscription of rates to enable new sessions to be added to traffic that may already be running at peak rate. Existing flows are impacted with discards to allow TCP backoff of existing flows, while preventing full capacity from blocking new flows.

Policers can be based on an AQP rule configuration to allow per-app-group, per-AA-sub total, per AA profile policy per application, and per system per app-group enforcement.

Policers are applied with two levels of hierarchy (granularity):

- Per individual AA subscriber
  - Per-AA-sub per app group/application or protocol rate
  - Per-AA-sub per application rate limit for a small selection of applications
  - Per-AA-sub PIR/CIR. This allows the AA ISAAA ISA to emulate IOM ingress policers in from-sub direction.
- Per system (AA ISA or a group of AA subscribers)
  - Total protocol/application rate
  - Total app group rate

Flows may be subject to multiple policers in each direction (from-subscriber-to-network or from-network-to-subscriber).

In Figure 17, Application Assurance policers are applied after ingress SAP policers. Configuration of the SAP ingress policers can be set to disable ingress policing or to set PIR/CIR values such that AA ISA ingress PIR/CIR will be invoked first. This enables application aware discard decisions, ingress policing at SAP ingress is application blind. However, this is a design/implementation guideline that is not enforced by the node.
In the to-aa-sub direction (Figure 18), traffic hits the AA ISA policers before the SAP egress queuing and scheduling. This allows application aware flow, AA subscriber and node traffic policies to be implemented before the internet traffic is mixed with the other services at node egress. Note that AA ISA policers may remark out-of-profile traffic which allows preferential discard at an IOM egress congestion point only upon congestion.
http://www.alcatel-lucent.com

Application Assurance HTTP Redirect

AA HTTP 404 Redirect

HTTP status code-based redirect feature provides error resolution and search technology that enhances the internet experience for end customers while generating new revenue stream for the ISP.

Alcatel-Lucent’s AA-ISA HTTP status code-based redirect feature, along with its partners Barefruit and Xercole, replaces unhelpful DNS and HTTP error messages with relevant alternatives, giving the user a search solution rather than a no direction. Customers benefit from an improved surfing experience as they are served relevant results that can help them find what they were looking for. The ISP, on the other hand, receives a share of the search revenue.

Every time an end-user clicks on a broken link (Page Not Found), an error page displays. Frequently, a search provider produces results, through a browser plug-in, for that user. This generates revenue for the search provider if the user clicks on a paid link.

With AA-ISA HTTP status code-based redirect feature, the user sees high-quality, relevant search results. In addition, instead of the search provider receiving all of the revenue, the ISP is paid every time a user clicks on a sponsored link. A win-win solution.

AA-ISA provides full customer control to configure an AQP action that redirects traffic that matches the AQP match criteria (Figure 19). Hence, the HTTP redirect service can applied at any level (application, application group, specific subscribers, specific source IP addresses) or any other AQP match criteria.
HTTP headers are intercepted by AA-ISA on the return path from the requested web site. If the HTTP status code is a non custom 404, then the response is replaced with JavaScript that redirects the client to the Contextual Analysis Servers (Barefruit server). This redirect contains details of the original URI that gave rise to the 404 error.

The operator can configure AA-ISA HTTP 404 redirect to use either Barefruit or Xerocole partner contextual analysis servers. A redirect policy can be defined once at the AA group level (similar to policers), and then referenced as many times as needed in AQP actions. The system allows a maximum of one HTTP 404 redirect policy per AA group.
Application QoS Policy (AQP)

An AQP is an ordered set of entries defining application-aware policy (actions) for IP flows diverted to a given AA ISA group. The IP flow match criteria are based on application identification (application or application group name) but are expected to use additional match criteria such as ASO characteristic value, IP header information or AA subscriber ID, for example.

When application service option characteristic values are used in application profiles, the characteristics values can be further used to subdivide an AQP into policy subsets applicable only to a subset of AA subscribers with a given value of an ASO characteristic in their profile. This allows to, for example, subdivide AQP into policies applicable to a specific service option (MOS iVideo Service), specific subscriber class (Broadband service tier, VPN, Customer X), or a combination of both.

A system without AQP defined will have statistics generated but will not impact the traffic that is flowing through the system. However, it is recommended that an AQP policy is configured with at least default bandwidth and flow policing entries to ensure a fair access to AA ISA bandwidth/flow resources for all AA subscribers serviced by a given AA ISA.

An AQP consists of a numbered and ordered set of entries each defining match criteria including AND, NOT and wildcard conditions followed by a set of actions.

AQP Entry <#> = <Match Criteria> AND <Match Criteria> <action> <action>

OR match conditions are supported in AQP through defining multiple entries. Multiple match criteria of a single AQP entry form an implicit AND function. An AQP can be defined for both recognized and unrecognized traffic. IP traffic flows that are in the process of being identified have a default policy applied (AQP entries that do not include application identification or IP header information). Flows that do not match any signatures are identified as unknown-tcp or unknown-udp and can have specific policies applied (as with any other protocol).
**AQP Match Criteria**

Match criteria consists of any combination of the following parameters:

- The source/destination IP address and port
- Application name
- Application group name
- One or more application service option characteristic and value pairs
- Direction of traffic (subscriber to network, network to subscriber, or both, or spoke SDP)
- DSCP name
- AA subscriber (ESM subscriber, SAP or spoke SDP)

AQP entries with match criteria that exclusively use any combination of ASO characteristic and values, direction of traffic, and AA subscriber define default policies. All other AQP entries define application aware policies. Both default and application aware policies. Until a flow's application is identified only default policies can be applied.

**AQP Actions**

An AQP action consists of the following action types. Multiple actions are supported for each rule entry (unlike ip-filters):

- Dual or single-bucket bandwidth rate limit policer
- Flow setup rate limit policer
- Total active flow count limit policer
- Remark QoS (one or a combination of discard priority, forwarding class name, DSCP). When applied, ingress marked FC and discard priority is overwritten by AA ISA and the new values are used during egress processing (for example, egress queueing or egress policy DSCP remarking). For MPLS class-based forwarding, ingress-marked FC is still used to select an egress tunnel.
- Drop (discard)
- None (monitor and report only)
- Source mirror for an existing mirror service
- 404 HTTP Redirect

Any flow diverted to an ISA group is evaluated against all entries of an AQP defined for that group at flow creation (default policy entries), application identification completion (all entries), and an AA policy change (all flows against all entries as a background task). Any given flow can match multiple entries, in which case multiple actions will be selected based on the AQP entry’s order (lowest number entry, highest priority) up to a limit of:
• 1 drop action
• Any combination of (applied only if no drop action is selected):
  → Up to 1 mirror action;
  → up to 1 FC, 1 priority and 1 DSCP remark action;
  → up to 4 BW policers;
  → up to 12 flow policers.

AQP entries the IP flow matched, that would cause the above per-IP-flow limits to be exceeded are ignored (no actions from that rule are selected).

Examples of some policy entries may be:

• Limit the subscriber to 20 concurrent Peer To Peer (P2P) flows max.
• Rate limit upstream total P2P application group to 400kbps.

Remark the voice application group to EF.

Time of Day Policing Adjustments

Time-of-day changes to Application Assurance policing rates can be implemented through the system's existing cron command. Typically, an operator may write scripts that can be executed at specific times of day that adjust policing rates. The adjusted policing limits are applied immediately to any pre-existing or new flows.
CLI Batch: Begin, Commit and Abort Commands

The Application Assurance uses CLI batches capability in policy definition. To start editing a policy, a begin command must be executed. To finish editing either abort (discard all changes) or commit (accept all changes) needs to be executed. CLI batch commands/state are preserved on HA activity switch.

To enter the mode to create or edit policies, the **begin** keyword must be entered at the prompt. Other editing commands include:

- The **commit** command saves changes made to policies during a session. The newly committed policy takes affect immediately for all new flows. Existing flows will transition onto the new policy shortly after the commit.
- The **abort** command discards changes that have been made to policies during a session.

To allow flexible order for policy editing, the **policy>commit** function cross references policy components to verify, among others:

- Whether all ASO characteristics have a default value and are defined in the app-profile.
- Limits checking.
Per AA Subscriber Service Monitoring and Debugging

Operators can use AA-specific tools in addition to system tools that allow them to monitor, adjust, debug AA services.

The following are examples of some of the available functions:

1. Display and monitor AA ISA group status and statistics (AA ISA status and capacity planning/monitoring).
2. Clear AA ISA group statistics (clears all system and per-AA-subscriber statistics).
3. Special study mode for real-time monitoring of AA-subscriber traffic (ESM subscriber, SAP or spoke SDP).
4. Per AQP entry statistics for number of hits (flow matching the entry) and conflicts (actions ignored due to per flow action limit exceeded).
5. Mirror (all or any subset of traffic seen by an AA ISA group).
6. All the per-ISA statistics from the aa-performance record, for examining resource loading of each ISA.
7. The top active AA-subscribers per ISA by bytes, packets or flows, for traffic in each direction.

CPU Utilization

The ISA show status command displays per ISA CPU utilization by main tasks, to provide insight into what aspects of load may be loading the ISA. These are split into 2 main areas:

- Management CPU, which includes all tasks related to communication between the CPM and the ISA, with the following usage percentage reported:
  → System — Various infrastructure and overhead work
  → Management — Managing AA policy, AA subscriber and trap configurations and handling tools requests
  → Statistics — Collecting and reporting statistics and Cflowd reporting
  → Idle
- Datapath CPUs, which includes all tasks related to datapath packet and flow processing on the ISA, with the following usage percentage reported:
  → System — Various infrastructure and overhead work
  → Packet processing — Receiving, associating with flows, applying application QoS policy and transmitting
→ Application ID — Using protocol signatures and other techniques to identify application/app-group and determine the application QoS policy.
Configuring Application Assurance with CLI

This section provides information to configure Application Assurance entities using the command line interface. It is assumed that the user is familiar with basic configuration of policies.

Provisioning AA ISA

The following illustrates syntax to provision AA ISA and configure ingress IOM QoS parameters. (The egress IOM QoS is configured in the config>isa>application-assurance-grp>qos context.)

config isa
tunnel-group 1 create
  primary 1/1
  backup 2/1
  no shutdown
exit all

CLI Syntax:  config service ies 199 customer 1 create
  interface "public-1" create
    address 64.251.12.1/32
  sap tunnel-1.public:200 create
exit all

CLI Syntax:  config service vprn 1 customer 1 create
  interface "gre tunnel to ce1" tunnel create
    address 10.0.0.1/30
    ip-mtu 1476
  sap tunnel-1.private:210 create
  gre-tunnel "to ce1" to 10.0.0.2 create
    source 64.251.12.1
    remote-ip 12.47.10.33
    backup-remote-ip 12.47.51.7
    delivery-service 199
    dscp af11
    no shutdown
exit
  ingress
  egress
exit all

CLI Syntax:  configure>card>mda mda-slot
  mda-type isa-aa
  network
    ingress
      pool
        slope-policy slope-policy-name
        resv-cbs percent-or-default
        queue-policy network-queue-policy-name

  egress
      pool
        slope-policy slope-policy-name
        resv-cbs percent-or-default
        queue-policy network-queue-policy-name
The following output displays AA ISA configuration example.

*A:cpm-a>config>app-assure# show mda 1/1
===============================================================================
<table>
<thead>
<tr>
<th>Slot</th>
<th>Mda</th>
<th>Provisioned</th>
<th>Equipped</th>
<th>Admin</th>
<th>Operational</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Mda-type</td>
<td>Mda-type</td>
<td>State</td>
<td>State</td>
</tr>
<tr>
<td>------</td>
<td>-----</td>
<td>-------------</td>
<td>----------</td>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>isa-aa</td>
<td>isa-ms</td>
<td>up</td>
<td>up</td>
</tr>
</tbody>
</table>
===============================================================================
*A:cpm-a>config>app-assure#

*A:cpm-a>config>card# info
----------------------------------------------
| card-type | iom-20g-b |
| mda 1     |
| mda-type  | isa-aa    |
| exit      |
----------------------------------------------
*A:cpm-a>config>card#
Configuring AA ISA

To enable AA on the router:

- Create an AA ISA group.
- Assign AA ISA(s) to an AA ISA group.
- Select one or more FC to be diverted to AA.
- Enable the group.

The following example illustrates AA ISA group configuration with:

- Primary AA ISA and warm redundancy provided by the backup AA ISA.
- “fail-to-wire” behavior configured on group failure.
- BE forwarding class selected for divert.
- Default IOM QoS for logical ISA egress ports. The ISA ingress QoS is configured as part of ISA provisioning (config>card>mda>network>ingress>qos).

The following commands illustrate AA ISA group configuration context.

**CLI Syntax:**
```
config>>isa>application-assurance-group isa-aa-group-id
    backup mda-id
    description description
    divert-fc fc-name
    fail-to-open
    isa-capacity-cost-high-threshold threshold
    isa-capacity-cost-low-threshold threshold
    partitions
    primary mda-id
    qos
    egress
        from-subscriber
            pool pool-name
            resv-cbs percent-or-default
            slope-policy slope-policy-name
            port-scheduler-policy port-scheduler-policy-name
            queue-policy network-queue-policy-name
        to-subscriber
            pool pool-name
            resv-cbs percent-or-default
            slope-policy slope-policy-name
            port-scheduler-policy port-scheduler-policy-name
            queue-policy network-queue-policy-name

[no] shutdown
```
The following output displays an AA ISA group configuration example.

A:ALU-A>config>isa>aa-grp# info detail
----------------------------------------------
no description
primary 1/2
backup 2/2
no fail-to-open
isa-capacity-cost-high-threshold 4294967295
isa-capacity-cost-low-threshold 0
no partitions
divert-fc be
qos
egress
  from-subscriber
    pool
      slope-policy "default"
      resv-cbs default
      exit
      queue-policy "default"
      no port-scheduler-policy
    exit
to-subscriber
    pool
      slope-policy "default"
      resv-cbs default
      exit
      queue-policy "default"
      no port-scheduler-policy
    exit
  exit
  exit
no shutdown
----------------------------------------------
A:ALU-A>config>isa>aa-grp#
Configuring Watermark Parameters

Use the following CLI syntax to configure thresholds for logs and traps when under high consumption of the flow table. The flow table has a limited size and these thresholds can be established to alert the user that the table is approaching capacity. These flow table watermarks represent number of flow contexts allocated on the ISA, which will be slightly higher than the actual number of existing flows at the point when the watermark is reached.

The low threshold is used while the high threshold is used as an alarm.

CLI Syntax:  
```
config>application-assurance
flow-table-high-wmark high-watermark
flow-table-low-wmark low-watermark
```
Configuring Application Assurance with CLI

Configuring a Group Policy

Beginning and Committing a Policy Configuration

To enter the mode to create or edit Application Assurance policies, you must enter the `begin` keyword at the `config>app-assure>group>policy` prompt. The `commit` command saves changes made to policies during a session. Changes do not take affect in the system until they have performed the commit function. The `abort` command discards changes that have been made to policies during a session.

The following error message displays when creating or modifying a policy without entering `begin` first.

A:ALA-B>config>app-assure>group>policy#
MINOR: AA #1005 Invalid Set - Cannot proceed with changes when in non-edit mode

There are no default policy options. All parameters must be explicitly configured.

Use the following CLI syntax to begin a policy configuration.

**CLI Syntax:**
```
config>app-assure# group group-id
   policy
   begin
```

Use the following CLI syntax to commit a policy configuration.

**CLI Syntax:**
```
config>app-assure# group group-id
   policy
   commit
```

Aborting a Policy Configuration

Use the following CLI syntax to abort a policy configuration.

**CLI Syntax:**
```
config>app-assure# group group-id
   policy
   abort
```
Configuring an Application Filter

An operator can use an application filter to define applications based on ALU protocol signatures and a set of configurable parameters like IP flow setup direction, IP protocol number, server IP address and server TCP/UDP port. An application filter references an application configured as previously shown.

Use the following CLI syntax to configure an application filter entry.

**CLI Syntax:**
```
config>app-assure>group>policy# app-filter
    entry entry-id [create]
        application application-name
        description description-string
        expression expr-index expr-type {eq | neq} expr-string
        flow-setup-direction {subscriber-to-network | network-to-subscriber | both}
        ip-protocol-num {eq | neq} protocol-id
        protocol {eq | neq} protocol-signature-name
        server-address {eq | neq} ip-address[/mask]
        server-port {eq | neq | gt | lt} server-port-number
        server-port {eq | neq} range start-port-num end-port-num
        server-port {eq | range start-port-num end-port-num} {port-num | range start-port-num end-port-num} first-packet-trusted|first-packet-validate
        no shutdown
```

The following example displays an application filter configuration.

```
*A:ALA-48>config>app-assure>group>policy>app-filter# entry 30 create
*A:ALA-48>config>app-assure>group>policy>app-filter>entry# info
----------------------------------------------
description "DNS traffic to local server on expected port #53"
protocol eq "dns"
flow-setup-direction subscriber-to-network
ip-protocol-num eq *
server-address eq 192.0.2.0/32
server-port eq 53
application "DNS_Local"
no shutdown
----------------------------------------------
*A:ALA-48>config>app-assure>group>policy>app-filter>entry#
```
Configuring an Application Group

An operator can configure an application group to group multiple application into a single application assurance entity by referencing those applications to the group created.

Use the following CLI syntax to configure an application group.

**CLI Syntax:**
```
config>app-assure>group>policy# app-group application-group-name [create]
            description description
```

The following example displays an application group configuration.

```
*A:ALA-48>config>app-assure>group>policy# app-group "Peer to Peer" create
*A:ALA-48>config>app-assure>group>policy>app-grp# info
----------------------------------------------
description "Peer to Peer file sharing applications"
----------------------------------------------
*A:ALA-48>config>app-assure>group>policy>app-grp#`
```
Configuring AA Volume, TCP and RTP Performance Reporting

**CLI Syntax:**
```
cfg>application-assurance>group isa-aa-group-id
cflowd
  collector <ip-address[:port]> [create]
  no collector <ip-address[:port]>
    description <description-string>
    no description
    [no] shutdown
volume
  rate <sample-rate>
  no rate
  [no] shutdown
performance
  flow-rate {tcp|rtp} <sample-rate>
  no flow-rate {tcp|rtp}
  template-retransmit <seconds>
  no template-retransmit
  [no] shutdown
```

**CLI Syntax:**
```
cfg>application-assurance
  group isa-aa-group-id[:<partition>] [create]
  no group isa-aa-group-id[:<partition>]
cflowd
  volume
    [no] shutdown
    application <application-name> {tcp|rtp}
    no application <application-name> {tcp|rtp}
    app-group <app-group-name> {tcp|rtp}
    no app-group <app-group-name> {tcp|rtp}
    [no] shutdown
```
The following example shows a configuration that:

- Enables per-flow volume stats for group 1, partition 1 and configures sampling rate to 1/1000.
- Enables per-flow TCP performance stats for web_traffic application within group 1, partition 1 and configures TCP sampling rate to 1/500.
- Enables per-flow RTP A/V performance stats for voip_traffic application within group 1, partition 1 and configures rtp sampling rate to 1/10.

```
*A:ALA-48# configure application-assurance group 1 cflowd
*A:ALA-48>config>app-assure>group>cflowd# volume rate 1000
*A:ALA-48>config>app-assure>group>cflowd# performance flow-rate tcp 500
*A:ALA-48>config>app-assure>group>cflowd# performance flow-rate rtp 10
*A:ALA-48>config>app-assure>group>cflowd# no shutdown
*A:ALA-48>config>app-assure>group>cflowd# info
----------------------------------------------
collector 138.120.131.149:55000 create
description "cflowd_collector_NewYork"
exit
volume
rate 1000
exit
performance
flow-rate tcp 500
flow-rate rtp 10
exit
no shutdown
----------------------------------------------
*A:ALA-48>config>app-assure>group>cflowd#

*A:ALA-48# configure application-assurance group 1:1 cflowd
*A:ALA-48>config>app-assure>group>cflowd#
*A:ALA-48>config>app-assure>group>cflowd# volume no shutdown
*A:ALA-48>config>app-assure>group>cflowd# performance application "web_traffic" tcp
*A:ALA-48>config>app-assure>group>cflowd# performance application "voip_traffic" rtp
*A:ALA-48>config>app-assure>group>cflowd# performance no shutdown
*A:ALA-48>config>app-assure>group>cflowd# info
----------------------------------------------
volume
no shutdown
exit
performance
no shutdown
application "web_traffic" tcp
application "voip_traffic" rtp
exit
----------------------------------------------
*A:ALA-48>config>app-assure>group>cflowd#
```
Configuring an Application

An operator can configure an application to group multiple protocols, clients or network applications into a single Application Assurance application by referencing it later in the created application filters as display in other sections of this guide.

Use the following CLI syntax to configure an application.

**CLI Syntax:**
```
config>app-assure>group>policy# application application-name [create]
    app-group app-group-name
    description description
```

The following example displays an application configuration.

```
*A:ALA-48>config>app-assure>group>policy# application "SQL" create
*A:ALA-48>config>app-assure>group>policy>app# info
-------------------------------------------------------
    description "SQL protocols"
    app-group "Business Critical Applications"
-------------------------------------------------------
*A:ALA-48>config>app-assure>group>policy>app#
```
Configuring an Application Profile

Use the following CLI syntax to configure an application profile.

**CLI Syntax:**
```
config>app-assure>group>policy# app-profile app-profile-name
[create]
  characteristic characteristic-name value value-name
  description description-string
  divert
```

The following example displays an application profile configuration.

```
*A:ALA-48>config>app-assure>group>policy# app-profile "Super" create
*A:ALA-48>config>app-assure>group>policy>app-prof# info
----------------------------------------------
description "Super User Application Profile"
dividt
characteristic "Server" value "Prioritize"
characteristic "ServiceBw" value "SuperUser"
characteristic "Teleworker" value "Yes"
characteristic "VideoBoost" value "Priority"
----------------------------------------------
*A:ALA-48>config>app-assure>group>policy>app-prof#
```
Configuring a Policer

Use the following CLI syntax to configure a policer.

**CLI Syntax:**
```
config>app-assure>group>policy# policer policer-name type type
granularity granularity create
action {priority-mark | permit-deny}
adaptation-rule pir {max | min | closest} [cir {max | min | closest}]
cbs committed burst size
description description-string
flow-count flow-count
mbs maximum burst size
rate pir-rate [cir cir-rate]
```

The following example displays an Application Assurance policer configuration.

```
*A:ALA-48>config>app-assure>group# policer "RegDown_Policer" type dual-bucket-bandwidth
granularity subscriber create
*A:ALA-48>config>app-assure>group>policer# info
----------------------------------------------
description "Control the downstream aggregate bandwidth for Regular 1Mbps
subscribers"
rate 1000 cir 500
mbs 100
cbs 50
----------------------------------------------
*A:ALA-48>config>app-assure>group>policer#
```
Configure an HTTP Redirect

Use the following CLI syntax to configure an HTTP redirect policy:

**CLI Syntax:**
```
cfg>app-assure>group> http-error-redirect redirect-name
create
description <description string>
no description
template <template_id>  // {1, 2} one for Barefruit, 2= Xerocole
no template
http-host <http-host name>  // eg. www.demo.barefruit.com
no http-host
participant-id <string>  // 32-char string used by template 1
no participant-id
error-code <http-error-code> [custom-msg-size <0-1500>]
no error-code <http-error-code>
[no] shutdown
no http-error-redirect <redirect_name>
```

The following example displays an Application Assurance http redirect configuration.

```
*A:ALA-48>config>app-assure>group# http-error-redirect "redirect-404"
create
create
description "redirect policy of 404 to Barefruit servers"
template 1
http-host att.barefruit.com
participant-id att-ISP
error-code 404

*A:ALA-48>config>app-assure>group> http-error-redirect# redirect-404
info
----------------------------------------------
description "redirect policy of 404 to Barefruit servers"
template 1
http-host "att.barefruit.com"
participant-id "att-ISP"
error-code 404

*A:ALA-48>config>app-assure>group>http-error-redirect#
```
Configuring an Application QoS Policy

Use the following CLI syntax to configure an application QoS policy.

**CLI Syntax:**
```plaintext
config>app-assure>group>policy# app-qos-policy
    entry entry-id [create]
        action
            bandwidth-policer policer-name
            drop
            flow-count-limit policer-name
            flow-rate-limit policer-name
            http-error-redirect redirect-name
            mirror-source [all-inclusive] mirror-service-id
            remark
                dscp in-profile dscp-name out-profile dscp-name
                fc fc-name
                priority priority-level
            description description-string
        match
            aa-sub sap {eq | neq} sap-id
            aa-sub esm {eq | neq} sub-ident-string
            aa-sub spoke-sdp {eq | neq} sdp-id:vc-id
            app-group {eq | neq} application-group-name
            application {eq | neq} application-name
            characteristic characteristic-name {eq} value-name
            dscp {eq | neq} dscp-name
            dst-ip {eq | neq} ip-address[/mask]
            dst-port {eq | neq} port-num
            dst-port {eq | neq} range start-port-num end-port-num
            src-ip {eq | neq} ip-address[/mask]
            src-port {eq | neq} port-num
            src-port {eq | neq} range start-port-num end-port-num
            traffic-direction {subscriber-to-network | network-to-subscriber | both}
        no shutdown
```
The following example displays an application QoS policy configuration.

A:ALA-48>config>app-assure>group>policy>aqp# entry 20 create
---
description "Limit downstream bandwidth to Reg_1M subscribers"
match
  traffic-direction network-to-subscriber
  characteristic "ServiceBw" eq "Reg_1M"
exit
action
  bandwidth-policer "RegDown_Policer"
exit
no shutdown
---
A:ALA-48>config>app-assure>group>policy>aqp#

The following example display an AQP entry configuration to mirror all positively identified only P2P traffic (AppGroup P2P) for a subset of subscribers with ASO characteristic **aa-sub-mirror** enabled.

A:ALA-48>config>app-assure>group>policy>aqp# entry 100 create
---
match
  app-group eq P2P
  characteristic aa-sub-mirror eq enabled
exit
action
  mirror-source 100
  # mirror to an existing mirror service id
exit
no shutdown
---
A:ALA-48>config>app-assure>group>policy>aqp#

The following example display AQP entries to mirror all P2P traffic (all positively identified P2P traffic and any unidentified traffic that may or may not be P2P - AppGroup P2P) for a subset of subscribers with ASO characteristic **aa-sub-mirror** enabled (the order is significant):

A:ALA-48>config>app-assure>group>policy>aqp# entry 100 create
---
match
  app-group eq P2P
  characteristic aa-sub-mirror value enabled
exit
action
  mirror-source all-inclusive 100
exit
no shutdown
---
A:ALA-48>config>app-assure>group>policy>aqp#
Configuring Application Service Options

Use the following CLI syntax to configure application service options.

**CLI Syntax:**
```
config>app-assure>group>policy# app-service-options
characteristic characteristic-name [create]
default-value value-name
value value-name
```

The following example displays an application service options configuration.

```
*A:ALA-48>config>app-assure>group>policy>aso# info
----------------------------------------------
characteristic "Server" create
  value "Block"
  value "Permit"
  value "Prioritize"
  default-value "Block"
exit
characteristic "ServiceBw" create
  value "Lite_128k"
  value "Power_5M"
  value "Reg_1M"
  value "SuperUser"
  default-value "Reg_1M"
exit
characteristic "Teleworker" create
  value "No"
  value "Yes"
  default-value "No"
exit
characteristic "VideoBoost" create
  value "No"
  value "Priority"
  default-value "No"
exit
----------------------------------------------
*A:ALA-48>config>app-assure>group>policy>aso#
```
Configuring AA Volume Accounting and Statistics

A network operator can configure AA volume statistic collection and accounting on both AA ISA system and subscriber levels.

The following commands illustrate the configuration of statistics collection and accounting policy on an AA group/partition aggregate level (without subscriber context).

**CLI Syntax:**
```
config>app-assure>group>statistics>app-group
    accounting-policy act-policy-id
    collect-stats
```

**CLI Syntax:**
```
config>app-assure>group>statistics>application
    accounting-policy act-policy-id
    collect-stats
```

**CLI Syntax:**
```
config>app-assure>group>statistics>protocol
    accounting-policy act-policy-id
    collect-stats
```

These commands illustrate the configuration of statistics collection and accounting policy for each AA subscriber in the system.

**CLI Syntax:**
```
config>app-assure>group>statistics>aa-sub
    accounting-policy act-policy-id
    app-group app-group-name
    application application-name
    collect-stats
    protocol protocol-signature-name
    aggregate-stats
    max-throughput-stats
```

These commands illustrate configuration of special study mode for a subset of AA subscribers (configured) to collect all protocol and/or application statistics with an AA subscriber context.

**CLI Syntax:**
```
config>app-assure>group>statistics# aa-sub-study {application|protocol}
    accounting-policy acct-policy-id
    collect-stats
```

For details on accounting policy configuration (including among others AA record type selection and customized AA subscriber record configuration) refer to the OS System Management Guide.
The following output illustrates per AA-subscriber statistics configuration that elects statistic collection for a small subset of all application groups, applications, protocols:

*A:ALU-40>config>app-assure>group>statistics>aa-sub# info
----------------------------------------------
accounting-policy 4
collect-stats
app-group "File Transfer"
app-group "Infrastructure"
app-group "Instant Messaging"
app-group "Local Content"
app-group "Mail"
app-group "MultiMedia"
app-group "Business_Critical"
app-group "Peer to Peer"
app-group "Premium Partner"
app-group "Remote Connectivity"
app-group "Tunneling"
app-group "Unknown"
app-group "VoIP"
app-group "Web"
app-group "Intranet"
application "BitTorrent"
application "eLearning"
application "GRE"
application "H323"
application "TLS"
application "HTTP"
application "HTTPS"
application "HTTPS_Server"
application "HTTP_Audio"
application "HTTP_Video"
application "eMail_Business"
application "eMail_Other"
application "Oracle"
application "Skype"
application "SAP"
application "SIP"
application "SMTP"
application "SQL_Alltypes"
application "TFTP"
protocol "bittorrent"
protocol "dns"
protocol "sap"
protocol "skype"
----------------------------------------------
*A:ALU-40>config>app-assure>group>statistics>aa-sub#
Configuring Cflowd Collector

The following output displays an Application Assurance cflowd collector configuration example:

**Example:** *A:ALA-48# configure application-assurance group 1 cflowd collector 138.120.131.149:55000 create
*A:ALA-48>config>app-assure>group>cflowd>collector$ description "cflowd_collector_NewYork"
*A:ALA-48>config>app-assure>group>cflowd>collector# no shutdown
*A:ALA-48>config>app-assure>group>cflowd>collector# exit

*A:ALA-48>config>app-assure>group>cflowd# info
----------------------------------------------
collector 138.120.131.149:55000 create
description "cflowd_collector_NewYork"
no shutdown
----------------------------------------------
*A:ALA-48>config>app-assure>group>cflowd#
The following example shows a configuration that:

- Enables per-flow volume stats for group 1, partition 1 and configures sampling rate to 1/1000.
- Enables per-flow TCP performance stats for web_traffic application within group 1, partition 1 and configures TCP sampling rate to 1/500.
- Enables per-flow RTP A/V performance stats for voip_traffic application within group 1, partition 1 and configures rtp sampling rate to 1/10.

*A:ALA-48# configure application-assurance group 1 cflowd
*A:ALA-48>config>app-assure>group>cflowd# volume rate 1000
*A:ALA-48>config>app-assure>group>cflowd# tcp-performance flow-rate 500
*A:ALA-48>config>app-assure>group>cflowd# rtp-performance flow-rate 10
*A:ALA-48>config>app-assure>group>cflowd# no shutdown
*A:ALA-48>config>app-assure>group>cflowd# info
  ----------------------------------------------
  collector 138.120.131.149:55000 create
  description "cflowd_collector_NewYork"
  exit
  volume
  rate 1000
  exit
  tcp-performance
  flow-rate 500
  rtp-performance
  flow-rate 10
  exit
  no shutdown
  ----------------------------------------------
*A:ALA-48>config>app-assure>group>cflowd#

*A:ALA-48# configure application-assurance group 1:1 cflowd
*A:ALA-48>config>app-assure>group>cflowd# volume no shutdown
*A:ALA-48>config>app-assure>group>cflowd# tcp-performance application "web_traffic"
*A:ALA-48>config>app-assure>group>cflowd# tcp-performance no shutdown
*A:ALA-48>config>app-assure>group>cflowd# rtp-performance application "voip_traffic"
*A:ALA-48>config>app-assure>group>cflowd# rtp-performance no shutdown
*A:ALA-48>config>app-assure>group>cflowd# info
  ----------------------------------------------
  volume
  no shutdown
  exit
  tcp-performance
  no shutdown
  application "web_traffic"
  rtp-performance
  no shutdown
  application "voip_traffic" rtp
  exit
  ----------------------------------------------
*A:ALA-48>config>app-assure>group>cflowd#
Configuring AA Volume, TCP and RTP Performance Reporting

**CLI Syntax:**

```
config>application-assurance>group isa-aa-group-id
cflowd
    collector ip-address[:port] [create]
    no collector ip-address[:port]
    description description-string
    no description
    [no] shutdown
rtp-performance
    flow-rate sample-rate
    no flow-rate
tcp-performance
    flow-rate sample-rate
    no flow-rate
template-retransmit seconds
    no template-retransmit
    [no] shutdown
volume
    rate sample-rate
    no rate
    [no] shutdown
```

```
config>application-assurance
    group isa-aa-group-id[:partition [create]]
    no group isa-aa-group-id[:partition
    cflowd
        volume
        [no] shutdown
    rtp-performance
        [no] app-group app-group-name
        [no] application application-name
        [no] shutdown
    tcp-performance
        [no] app-group app-group-name
        [no] application application-name
        [no] shutdown
```
The following example shows a configuration that:

- Enables per-flow volume stats for group 1, partition 1 and configures sampling rate to 1/1000.
- Enables per-flow TCP performance stats for web_traffic application within group 1, partition 1 and configures TCP sampling rate to 1/500.
- Enables per-flow RTP A/V performance stats for voip_traffic application within group 1, partition 1 and configures RTP sampling rate to 1/10.

```
*A:ALA-48# configure application-assurance group 1 cflowd
*A:ALA-48>config>app-assure>group>cflowd# volume rate 1000
*A:ALA-48>config>app-assure>group>cflowd# tcp-performance flow-rate 500
*A:ALA-48>config>app-assure>group>cflowd# rtp-performance flow-rate 10
*A:ALA-48>config>app-assure>group>cflowd# no shutdown
*A:ALA-48>config>app-assure>group>cflowd# info

----------------------------------------------
collector 138.120.131.149:55000 create
description "cflowd Collector NewYork"
exit
volume
  rate 1000
exit
tcp-performance
  flow-rate 500
rtp-performance
  flow-rate 10
exit
no shutdown

----------------------------------------------
*A:ALA-48>config>app-assure>group>cflowd#*
*A:ALA-48# configure application-assurance group 1:1 cflowd
*A:ALA-48>config>app-assure>group>cflowd#
*A:ALA-48>config>app-assure>group>cflowd# volume no shutdown
*A:ALA-48>config>app-assure>group>cflowd# tcp-performance application "web_traffic"
*A:ALA-48>config>app-assure>group>cflowd# tcp-performance no shutdown
*A:ALA-48>config>app-assure>group>cflowd# rtp-performance application "voip_traffic"
*A:ALA-48>config>app-assure>group>cflowd# rtp-performance no shutdown
*A:ALA-48>config>app-assure>group>cflowd# info

--------------------------------------------------------
volume
  no shutdown
exit
tcp-performance
  no shutdown
    application "web_traffic"
  rtp-performance
    no shutdown
    application "voip_traffic" rtp
  exit

--------------------------------------------------------
*A:ALA-48>config>app-assure>group>cflowd#
```
Application Assurance Command Reference

- Hardware Commands on page 121
- Admin Commands on page 122
- ISA Commands on page 122
- ISA Application Assurance Group on page 122
- Application Assurance Commands on page 124
- AA Group Commands on page 124
- Group Policy Commands on page 125
- Application Filter Commands on page 125
- Application Group Commands on page 125
- Application Profile Commands on page 125
- AQP Commands on page 126
- Application Service Options Commands on page 127
- Statistics Commands on page 127
- Show Commands on page 130
- Tools Commands on page 131
- Clear Commands on page 131
- Debug Commands on page 131
- Admin Commands on page 122

Hardware Commands

```bash
cfg
   — card slot-number
      — mda mda-slot
         — mda-type mda-type
            — network
               — ingress
                  — pool [pool-name]
                  — no pool
                  — resv-cbs percent-or-default
                  — no resv-cbs
                  — slope-policy slope-policy-name
                  — no slope-policy
                  — queue-policy network-queue-policy-name
                  — no queue-policy
```
Admin Commands

```
admin
   — application-assurance
      — upgrade
```

ISA Commands

```
config
   — isa
      — tunnel-group tunnel-group-id [create]
      — no tunnel-group tunnel-group-id
         — backup mda-id
         — no backup
         — description description-string
         — no description
         — no primary
         — primary mda-id
         — [no] shutdown

config
   — isa
      — application-assurance-group application-assurance-group-index [create] [aa-sub-scale sub-scale]
      — no application-assurance-group application-assurance-group-index
         — [no] backup mda-id
         — description description-string
         — no description
         — [no] divert-fc fc-name
         — [no] fail-to-open
         — isa-capacity-cost-high-threshold threshold
         — no isa-capacity-cost-high-threshold
         — isa-capacity-cost-low-threshold threshold
         — no isa-capacity-cost-low-threshold
         — [no] isa-overload-cut-through
         — [no] partitions
         — [no] primary mda-id
         — qos
            — egress
               — from-subscriber
                  — pool [pool-name]
                  — no pool
                     — resv-cbs percent-or-default
                     — no resv-cbs
                     — slope-policy slope-policy-name
                     — no slope-policy
                  — port-scheduler-policy port-scheduler-policy-name
                  — no port-scheduler-policy
               — queue-policy network-queue-policy-name
                  — no queue-policy
                  — wa-shared-high-wmark percent
                  — no wa-shared-high-wmark
                  — wa-shared-low-wmark percent
                  — no wa-shared-low-wmark
               — to-subscriber
```
— pool [pool-name]
— pool [pool-name]
— no pool
  — resv-cbs percent-or-default
  — no resv-cbs
  — slope-policy slope-policy-name
  — no slope-policy
— port-scheduler-policy port-scheduler-policy-name
— no port-scheduler-policy
— queue-policy network-queue-policy-name
— no queue-policy
— wa-shared-high-wmark percent
— no wa-shared-high-wmark
— wa-shared-low-wmark percent
— no wa-shared-low-wmark

— [no] shutdown
— statistics
  — performance
    — accounting-policy acct-policy-id
    — no accounting-policy
    — [no] collect-stats
— transit-prefix-ipv4-entries entries
— no transit-prefix-ipv4-entries
— transit-prefix-ipv6-entries entries
— no transit-prefix-ipv6-entries
— transit-prefix-ipv6-remote-entries entries
— no transit-prefix-ipv6-remote-entries
Application Assurance Commands

```
config
  application-assurance
    bit-rate-high-wmark high-watermark
    bit-rate-low-wmark low-watermark
    no bit-rate-low-wmark
    flow-setup-high-wmark high-watermark
    flow-setup-low-wmark low-watermark
    no flow-setup-low-wmark
    flow-table-high-wmark high-watermark
    no flow-table-high-wmark
    flow-table-low-wmark low-watermark
    no flow-table-low-wmark
    group aa-group-id:partition-id [create]
    no group aa-group-id:partition-id
  cflowd
    collector ip-address[:port] [create]
    no collector ip-address[:port]
      description description-string
    no description
    [no] shutdown
  rtp-performance
    [no] app-group app-group-name perf-meas-type
    [no] application application-name perf-meas-type
    flow-rate perf-meas-type sample-rate
    no flow-rate perf-meas-type
    [no] shutdown
  [no] shutdown
  tcp-performance
    [no] app-group app-group-name perf-meas-type
    [no] application application-name perf-meas-type
    flow-rate perf-meas-type sample-rate
    no flow-rate perf-meas-type
    [no] shutdown
  template-retransmit seconds
  no template-retransmit
  volume
    rate sample-rate
    no rate
    [no] shutdown
  http-error-redirect redirect-name [create]
  no http-error-redirect redirect-name
    description description-string
    no description
    error-code error-code [custom-msg-size custom-msg-size]
    no error-code error-code
    http-host http-host
    no http-host
    participant-id participant-id
    no participant-id
    [no] shutdown
    template template-id
    no template
  [no] http-match-all-requests
  [no] http-x-online-host
```
— policer policer-name type type granularity granularity [create]
— policer policer-name
— no policer policer-name
  — action {priority-mark | permit-deny}
  — adaptation-rule pir {max | min | closest} [cir {max | min | closest}]
  — no adaptation-rule
  — cbs committed burst size
  — no cbs
  — description description-string
  — no description
  — flow-count flow-count
  — no flow-count
  — mbs maximum burst size
  — no mbs
  — rate pir-rate [cir cir-rate]
  — no rate
— policy
  — abort
  — begin
  — commit
  — app-filter
    — entry entry-id [create]
    — no entry entry-id
    — application application-name
    — description description-string
    — no description
    — expression expr-index expr-type {eq | neq | eq | neq} expr-string
    — no expression expr-index
    — flow-setup-direction {subscriber-to-network | network-to-subscriber | both}
    — ip-protocol-num {eq | neq} protocol-id
    — no ip-protocol-num
    — protocol {eq | neq} protocol-signature-name
    — no protocol
    — server-address {eq | neq} ip-address
    — no server-address
    — server-port {eq | neq | gt | lt} server-port-number
    — no server-port
    — [no] shutdown
— app-group application-group-name [create]
— no app-group application-group-name
  — description description-string
  — no description
— app-profile app-profile-name [create]
— no app-profile app-profile-name
  — capacity-cost cost
  — no capacity-cost
  — characteristic characteristic-name value-value-name
  — no characteristic characteristic-name
  — description description-string
— no description
— [no] divert
— app-service-options characteristic-name value value-name
— no app-service-options characteristic-name
— app-qos-policy
  — entry entry-id [create]
  — no entry entry-id
    — action
      — bandwidth-policer policer-name
      — no bandwidth-policer
      — [no] drop
      — flow-count-limit policer-name
      — no flow-count-limit
      — flow-rate-limit policer-name
      — no flow-rate-limit
      — http-error-redirect redirect-name
      — no http-error-redirect
      — mirror-source [all-inclusive] mirror-service-id
      — no mirror-source
      — remark
      — dscp in-profile dscp-name out-profile dscp-name
        — no dscp
        — fc fc-name
        — no fc
        — priority priority-level
        — no priority
    — description description-string
    — no description
    — match
      — aa-sub esm {eq | neq} sub-ident-string
      — aa-sub sap {eq | neq} sap-id
      — aa-sub spoke-sdp {eq | neq} sdp-id:vc-id
      — aa-sub transit {eq | neq} transit-aasub-name
      — no aa-sub
      — app-group {eq | neq} application-group-name
      — no app-group
      — application {eq | neq} application-group-name
      — no application
      — characteristic characteristic-name eq value-name
      — no characteristic
      — dscp {eq | neq} dscp-name
      — no dscp
      — dst-ip {eq | neq} ip-address
      — no dst-ip
      — dst-port {eq | neq} port-num
      — dst-port {eq | neq} range start-port-num end-port-num
      — no dst-port
      — src-ip {eq | neq} ip-address
      — no src-ip
      — src-port {eq | neq} port-num
      — src-port {eq | neq} range start-port-num end-port-num
no src-port
traffic-direction {subscriber-to-network | network-to-subscriber | both}
[no] shutdown
app-service-options
characteristic characteristic-name [create]
no characteristic characteristic-name
default-value value-name
no default-value
[no] value value-name
application application-name [create]
no application application-name
app-group app-group-name
description description-string
no description
custom-protocol custom-protocol-id ip-protocol-num protocol-id [create]
custom-protocol custom-protocol-id
no custom-protocol custom-protocol-id
description description-string
no description
expression expr-index eq expr-string offset payload-octet-offset
direction direction
no expression expr-index
[no] shutdown
diff
policy-override
policy aa-sub {sap sap-id | spoke-sdp sdp-id:vc-id} [create]
no policy aa-sub {sap sap-id | spoke-sdp sdp-id:vc-id}
characteristic characteristic-name value value-name
no characteristic characteristic-name
statistics
aa-sub
accounting-policy acct-policy-id
no accounting-policy
[no] aggregate-stats
[no] app-group app-group-name
[no] application application-name
[no] collect-stats
[no] max-throughput-stats
[no] protocol protocol-name
aa-sub-study study-type
aa-sub {esm sub-ident-string | sap sap-id | spoke-sdp sdp-id:vc-id | transit transit-aasub-name}
[no] aa-sub {esm sub-ident-string | sap sap-id | spoke-sdp sdp-id:vc-id | transit transit-aasub-name}
accounting-policy acct-policy-id
no accounting-policy
[no] collect-stats
app-group
accounting-policy acct-policy-id
no accounting-policy
[no] collect-stats
— application
  — accounting-policy acct-policy-id
  — no accounting-policy
  — [no] collect-stats
— protocol
  — accounting-policy acct-policy-id
  — no accounting-policy
  — [no] collect-stats
— transit-ip-policy ip-policy-id [create]
— no transit-ip-policy ip-policy-id
  — def-app-profile app-profile-name
  — no def-app-profile
  — description description-string
  — no description
  — dhcp
    — [no] shutdown
— radius
  — authentication-policy name
  — no authentication-policy
  — [no] shutdown
— static-aa-sub transit-aasub-name
— static-aa-sub transit-aasub-name app-profile app-profile-name [create]
— no static-aa-sub transit-aasub-name
  — [no] ip ip-address
— sub-ident-policy sub-ident-policy-name
  — no sub-ident-policy
— transit-prefix-policy prefix-policy-id [create]
— no transit-prefix-policy prefix-policy-id
  — description description-string
  — no description
  — entry entry-id [create]
  — entry entry-id
    — no entry entry-id
    — aa-sub transit-aasub-name
    — no aa-sub
    — match
      — aa-sub-ip ip-address[/mask]
      — no aa-sub-ip
      — network-ip ip-address[/mask]
      — no network-ip
— static-aa-sub transit-aasub-name
— static-aa-sub transit-aasub-name app-profile app-profile-name [create]
— no static-aa-sub transit-aasub-name
— static-remote-aa-sub transit-aasub-name
— static-remote-aa-sub transit-aasub-name app-profile app-profile-name [create]
— no static-remote-aa-sub transit-aasub-name
— packet-rate-high-wmark high-watermark
— packet-rate-low-wmark low-watermark
— no packet-rate-low-wmark
— protocol protocol-name
  — [no] shutdown
Persistence Commands

```
config
  system
    persistence
      application-assurance
        description description-string
        no description
        location cflash-id
        no location
```
Show Commands

show
  — isa
    — application-assurance-group [aa-group-id [load-balance [unassigned]]]
    — application-assurance-group [aa-group-id]
      — aa-sub esm sub-ident-string [snapshot]
      — aa-sub sap sap-id
      — aa-sub spoke-sdp sd-id:vc-id [snapshot]
      — aa-sub transit transit-aasub-name [snapshot]
        — app-group [app-group-name] count [detail]
        — application [application-name] count [detail]
        — count [detail]
        — policers
          — protocol [protocol-name] count [detail]
          — summary
      — aa-sub-list [isa mda-id]
      — aa-sub-list policers-exceeded
      — aa-sub-list summary
      — aa-sub-study esm sub-ident-string [snapshot]
      — aa-sub-study sap sap-id [snapshot]
      — aa-sub-study spoke-sdp sd-id:vc-id [snapshot]
      — aa-sub-study transit transit-aasub-name [snapshot]
        — application [application-name] count [detail]
        — protocol [protocol-name] count [detail]
      — app-group [app-group-name] count [detail]
      — application [application-name] count [detail]
  — cflowd
    — collector [detail]
    — status
  — partition summary
  — policer [policer-name]
  — policer summary
  — policy
    — admin
    — app-filter [entry-id]
    — app-group [app-group-name]
    — app-profile [app-prof-name]
    — app-profile app-prof-name associations
    — app-qos-policy [entry-id]
    — app-service-option [characteristic-name]
    — application [app-name]
    — custom-protocol
      — summary
      — protocol [protocol-name] count [detail]
  — status [isa mda-id] cflowd
  — status [isa mda-id]
  — status [isa mda-id] detail
  — status [isa mda-id] cpu [sample-period seconds]
  — status [isa mda-id] qos count
  — status [isa mda-id] qos pools
  — http-error-redirect
    — error-codes
    — template
    — protocol [protocol-name]
Tools Commands

tools
dump

application-assurance
group aa-group-id [partition-id]

aa-sub-search search-type granularity [direction direction] [max-count max-count]

congestion-search search-type [isa mda-id]

flow-record-search aa-sub {esm sub-ident-string | sap sap-id | spoke-sdp sdp-id:vc-id | transit transit-aasub-name} [protocol protocol-name] [application app-name] [app-group app-group-name] [flow-status flow-status] [start-flowid start-flowid] [max-count max-count] [search-type search-type] [url file-url]

flow-record-search isa mda-id [protocol protocol-name] [application app-name] [app-group app-group-name] [flow-status flow-status] [start-flowid start-flowid] [max-count max-count] [search-type search-type] [url file-url]

load-balance [service service-id]

Clear Commands

clear

application-assurance
group aa-group-id eflow
group aa-group-id statistics
group aa-group-id status

Debug Commands

debug

[no] mirror-source service-id

isa-aa-group aa-group-id {all | unknown}

no isa-aa-group aa-group-id
Application Assurance Commands

- Application Assurance Commands on page 133
  → Generic Commands on page 133
  → Hardware Commands on page 135
  → Application Assurance Commands on page 137
  → Group Commands on page 146
    - Policer Commands on page 146
    - Policy Commands on page 150
      - Application Filter Commands on page 154
      - Application Profile Commands on page 159
      - Application QoS Policy Commands on page 161
      - Application Service Options Commands on page 171
    - Statistics Commands on page 175
  • ISA Commands on page 188

Application Assurance uses system components for some of its functionality. Refer to the following for details on:

- Configuration of Application Assurance Accounting policy including per accounting type record selection and customization of AA subscriber records.
- Configuration of AA ISA IOM QoS.

Generic Commands

description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>description</th>
<th>description-string</th>
</tr>
</thead>
<tbody>
<tr>
<td>no description</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Context</th>
<th>config&gt;isa&gt;tunnel-group</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>config&gt;app-assure&gt;protocol</td>
</tr>
<tr>
<td></td>
<td>config&gt;app-assure&gt;group&gt;policer</td>
</tr>
<tr>
<td></td>
<td>config&gt;app-assure&gt;group&gt;policy&gt;app-filter&gt;entry</td>
</tr>
<tr>
<td></td>
<td>config&gt;app-assure&gt;group&gt;policy&gt;app-group</td>
</tr>
<tr>
<td></td>
<td>config&gt;app-assure&gt;group&gt;policy&gt;app-profile</td>
</tr>
<tr>
<td></td>
<td>config&gt;app-assure&gt;group&gt;policy&gt;aqp&gt;entry</td>
</tr>
<tr>
<td></td>
<td>config&gt;app-assure&gt;group&gt;policy&gt;application</td>
</tr>
<tr>
<td></td>
<td>config&gt;app-assure&gt;group&gt;cflowd&gt;collector</td>
</tr>
<tr>
<td></td>
<td>config&gt;app-assure&gt;group&gt;cflowd&gt;group&gt;cflowd</td>
</tr>
</tbody>
</table>
**Generic Commands**

```
config>app-assure>group>cflowd>group>cflowd>collector
config>app-assure>group>cflowd>group>cflowd>volume
config>app-assure>group>policy>custom-protocol
config>app-assure>group>policy>transit-ip-policy
config>app-assure>group>http-err-redir
```

**Description**
This command creates a text description which is stored in the configuration file to help identify the content of the entity.

The `no` form of the command removes the string from the configuration.

**Default**
none

**Parameters**

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

**shutdown**

**Syntax**
```
[no] shutdown
```

**Context**
```
config>isa>tunnel-group
config>app-assure>group
config>app-assure>group>policy>app-filter>entry
config>app-assure>group>policy>aqp>entry
config>app-assure>group>cflowd>collector
config>app-assure>group>cflowd>group>cflowd>performance
config>isa>lns-group
config>app-assure>group>policy>transit-ip-policy>dhcp
config>app-assure>group>policy>transit-ip-policy>radius
config>app-assure>group>cflowd>tcp-performance
```

**Description**
This command administratively disables the entity. When disabled, an entity does not change, reset, or remove any configuration settings or statistics. Many entities must be explicitly enabled using the `no shutdown` command.

The `shutdown` command administratively disables an entity. 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.
**Hardware Commands**

**isa-aa (mda-type)**

**Syntax**

```
mda-type isa-aa
no mda-type
```

**Context**

```
config>card>mda
```

**Description**

This command provisions an adaptor into an MDA position on an IOM slot. The AA ISA is provisioned into the system in the same manner as all other MDA type. Once an AA ISA is provisioned, independent of it actually existing in the system or the specified slot and MDA position, the AA ISA can be defined as a member of an application assurance group.

The `no` form of this command removes the module from the configuration. The module must be administratively shut down before it can be deleted from the configuration.

Refer to the for further information on command usage and syntax for the AA ISA and other MDA and ISA types.

**Default**

No ISA types are configured for any slots by default.

**Parameters**

`isa-aa` — Specifies the Application Assurance Integrated Services Adapter for the slot position.
Admin Commands

application-assurance

Syntax application-assurance
Context admin
Description This command enables the context to perform Application Assurance (AA) configuration operations.

upgrade

Syntax upgrade
Context admin>app-assure
Description Use this command to load a new isa-aa.tim file as part of a router-independent signature upgrade. An AA ISA reboot is required.
Application Assurance Commands

bit-rate-high-wmark

Syntax: `bit-rate-high-wmark high-watermark`

Context: `config>application-assurance`

Description: This command configures the high watermark for bit rate alarms.

Parameters:

- `high-watermark` — specifies the high watermark for bit rate alarms. The value must be larger than or equal to the low-watermark value.

Values: 1 — 10000, max megabits/sec

bit-rate-low-wmark

Syntax: `bit-rate-low-wmark low-watermark`

Context: `config>application-assurance`

Description: This command configures the utilization of the flow records on the ISA-AA Group when the full alarm will be cleared by the agent.

Default: 0

Parameters:

- `low-watermark` — Specifies the low watermark for bit rate alarms. The value must be lower than or equal to the high-watermark value.

Values: 0 — 10000 megabits/sec

packet-rate-high-wmark

Syntax: `packet-rate-high-wmark high-watermark`

Context: `config>app-assure`

Description: This command configures the packet rate on the ISA-AA when a packet rate alarm will be raised by the agent.

Default: max = disabled

Parameters:

- `high-watermark` — Specifies the high watermark for packet rate alarms. The value must be larger than or equal to the packet-rate-low-wmark value.

Values: 1 — 14880952, max packets/sec
Application Assurance Commands

**packet-rate-low-wmark**

**Syntax**

```
packet-rate-low-wmark low-watermark
no packet-rate-low-wmark
```

**Context**

`config>app-assure`

**Description**

This command configures the system wide low watermark threshold for per-ISA throughput in packets/second when an high packet rate alarm will be cleared by the agent. The value must be less than or equal to the packet-rate-high-wmark parameter.

The `no` form of the command sets the parameter to minimum (watermark disabled).

**Default**

0

**Parameters**

`low-watermark` — Specifies the low watermark for packet rate alarms. The value must be lower than or equal to the packet-rate-low-wmark value.

**Values**

0 — 14880952 packets/sec

**flow-setup-high-wmark**

**Syntax**

```
flow-setup-high-wmark high-watermark
```

**Context**

`config>application-assurance`

**Description**

This command configures the system wide high watermark threshold for per-ISA throughput in packets/second when an alarm will be raised by the agent. The value must be larger than or equal to the packet-rate-low-wmark parameter.

The `no` form of the command sets the parameter to maximum (watermark disabled).

**Default**

0

**Parameters**

`high-watermark` — Specifies the high watermark for flow setup rate alarms. The value must be larger than or equal to the flow-setup-low-wmark value.

**Values**

1 — 200000, max flows/sec

**flow-setup-low-wmark**

**Syntax**

```
flow-setup-low-wmark low-watermark
no flow-setup-low-wmark
```

**Context**

`config>application-assurance`

**Description**

This command configures the flow setup rate on the ISA-AA when a flow setup alarm will be raised by the agent.

**Default**

0

**Parameters**

`low-watermark` — Specifies the low watermark for flow setup rate alarms. The value must be larger than or equal to the flow-setup-high-wmark value.
Application Assurance Commands

Values 1 — 200000, max flows/sec

application-assurance

Syntax application-assurance
Context config
Description This command enables the context to perform Application Assurance (AA) configuration operations.

flow-table-high-wmark

Syntax flow-table-high-wmark high-watermark
no flow-table-high-wmark
Context config>app-assure
Description The command configures the system-wide high watermark threshold as a percentage of the flow table size for the per-ISA utilization of the flow records when a full alarm will be raised by the agent.
Parameters high-watermark — Specifies the high watermark for flow table full alarms.
Values 0 — 100
Default 95%

flow-table-low-wmark

Syntax flow-table-low-wmark low-watermark
no flow-table-low-wmark
Context config>app-assure
Description This command configures the system-wide low watermark threshold as a percentage of the flow table size for per-ISA. The value must be lower than or equal to the flow-table-high-wmark high-watermark parameter.
Parameters low-watermark — Specifies the low watermark for flow table full alarms.
Values 0 — 100
Default 90%

protocol

Syntax protocol protocol-name
Context config>app-assure
Application Assurance Commands

**Description**  
This command configures the shutdown of protocols system-wide.

**Parameters**  
*protocol-name* — A string of up to 32 characters identifying a predefined protocol.

### group

**Syntax**  
group aa-group-id[;partition-id [create]]  
no group aa-group-id:partition-id

**Context**  
config>app-assure

**Description**  
This command configures and enables the context to configure an application assurance group and partition parameters.

**Parameters**  
aa-group-id — Represents a group of ISA MDAs.

<table>
<thead>
<tr>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 — 255</td>
</tr>
</tbody>
</table>

partition-id — Specifies a partition within a group,

<table>
<thead>
<tr>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 — 65535</td>
</tr>
</tbody>
</table>

create — Keyword used to create the partition in the group.

### cflowd

**Syntax**  
cflowd

**Context**  
config>app-assure>group

**Description**  
This command enables the context to configure cflowd parameters for the application assurance group.

### collector

**Syntax**  
collector ip-address[:port] [create]  
no collector ip-address[:port]

**Context**  
config>app-assure>group>cflowd

**Description**  
This command defines a flow data collector for cflowd data. The IP address of the flow collector must be specified. The UDP port number is an optional parameter. If it is not set, the default of 2055 is used.

**Parameters**  
*ip-address* — The IP address of the flow data collector in dotted decimal notation.

*port* — The UDP port of flow data collector.

<table>
<thead>
<tr>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>2055</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 — 65535</td>
</tr>
</tbody>
</table>
rtp-performance

**Syntax**  
formance

**Context**  
config>app-assure>group>cflowd

**Description**  
This command configures the cflowd RTP performance export.

app-group

**Syntax**  
[no] app-group app-group-name

**Context**  
config>app-assure>group>cflowd>rtp-performance
config>app-assure>group>cflowd>tcp-performance

**Description**  
This command configures application groups to export performance records with cflowd. The no form of the command removes the parameters from the configuration.

**Parameters**  
app-group-name — Specifies the application group name.

application

**Syntax**  
[no] application application-name

**Context**  
config>app-assure>group>cflowd>rtp-performance
config>app-assure>group>cflowd>tcp-performance

**Description**  
This command configures applications to export performance records with cflowd. The no form of the command removes the parameters from the configuration.

**Parameters**  
application-name — Specifies the name defined for the application.

flow-rate

**Syntax**  
flow-rate sample-rate

no flow-rate perf-meas-type

**Context**  
config>app-assure>group>cflowd>rtp-performance
config>app-assure>group>cflowd>tcp-performance

**Description**  
This command configures specifies the per-flow sampling rate for the cflowd export of Application Assurance performance statistics. The no form of the command reverts to the default.

**Default**  
no flow-rate

**Parameters**  
sample-rate — This is the rate at which to sample flows that are eligible for TCP performance measurement.
Values

1 — 1000

template-retransmit

Syntax template-retransmit seconds

no template-retransmit

Context config>app-assure>group>cflowd

Description This command configures the period of time, in seconds, for the template to be retransmitted.

Parameters seconds — Specifies the time period for the template to be retransmitted.

Values 10 — 600

Default 600

tcp-performance

Syntax tcp-performance

Context config>app-assure>group>cflowd

Description This command enables the context to configure Cflowd TCP performance export parameters.

volume

Syntax volume

Context config>app-assure>group>cflowd

Description This command configures the cflowd volume export.

rate

Syntax rate sample-rate

no rate

Context config>app-assure>group>cflowd>volume

Description This command configures the sampling rate of packets for the cflowd export of application assurance volume statistics.

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

Parameters sample-rate — This is the rate at which to sample packets for the cflowd export of application assurance volume statistics.

Values 1 — 10000
http-error-redirect

Syntax  
http-error-redirect redirect-name [create]  
no http-error-redirect redirect-name  

Context  
config>app-assure>group  

Description  
This command configures an HTTP error redirect policy. The policy contains important information relevant to the redirect server.  

The no form of the command removes the redirect name from the group configuration.  

Default  
none  

Parameters  
redirect-name — A string of up to 32 characters that identifies the HTTP error redirect policy.  

error-code

Syntax  
error-code error-code [custom-msg-size custom-msg-size]  
no error-code error-code  

Context  
config>app-assure>group>http-error-redirect  

Description  
This command refers to which HTTP status codes a redirect action is applied. Currently, only 404 http error code is supported. Only messages with sizes less than that configured here (custom-msg-size) are eligible for redirect action.  

The no form of the command removes the parameters from the configuration.  

Default  
Error code: none  

Parameters  
error-code — Specifies the error code for a HTTP Error Redirect.  

Values  
0 — 4294967295  

custom-msg-size — Specifies the maximum message size above which redirect will not be done.  

Values  
0 — 4294967295  

http-host

Syntax  
http-host http-host  
no http-host  

Context  
config>app-assure>group>http-error-redirect  

Description  
This is a string that refers to the http host name of the landing server (barefurit or xerocole). It is used in the HTTP GET operation from the client (which is being redirected) to the redirect search landing server. It must contain a valid IP address or HTTP host name / URI for the HTTP GET from the client to the landing server to work.  

The no form of the command removes the HTTP host string from the configuration.  

Default  
none
Application Assurance Commands

**Parameters**

`http-host` — Specifies a string of 255 chars max length, that refers to the HTTP host name of the landing server (barefurit or xerocole).

**participant-id**

**Syntax**

```
participant-id
no participant-id
```

**Context**

`config>app-assure>group> http-error-redirect`

**Description**

This command specifies a 32-character string assigned to the operator by Barefruit. It is used by barefruit landing servers (applies to template # 1 only).

**Default**

None

**Parameters**

`participant-id` — 32-char string supplied by the Barefruit

**template**

**Syntax**

```
template template-id
no template
```

**Context**

`config>app-assure>group`

**Description**

The redirect template refers to the template of parameters passed from the AA-ISA to the redirect server via JavaScript in the redirect packet. The template is specific to the redirect server being used in the network.

Currently, two partners are used and tested with AA-ISA redirect solution, Barefruit and Xerocole. The `no` form of the command reverts to the default.

**Default**

1 = referring to redirect format for barefruit landing server.

**Parameters**

`template-id` — Specifies an HTTP error redirect template.

- 1 = Barefruit specific template
- 2 = xerocole specific template.

**Values**

0 — 4294967295

**http-match-all-requests**

**Syntax**

```
[no] http-match-all-requests
```

**Context**

`config>app-assure>group`

**Description**

This command enables constant monitoring performed for HTTP request strings for application changes in regular HTTP flows.

The `no` form of the command disables the monitoring.
http-x-online-host

Syntax [no] http-x-online-host

Context config>app-assure>group

Description This command specifies whether X-Online-Host header field is used as a replacement for the HTTP Host header field.

The no form of the command disables the use of X-Online-Host header field used as a replacement.
**Policer Commands**

**Syntax**

```
policer policer-name type type granularity granularity [create]
policer policer-name
no policer policer-name
```

**Context**

```
config>app-assure>group
```

**Description**

This command creates application assurance policer profile of a specified type. Policers can be bandwidth or flow limiting and can have a system scope (limits traffic entering AA ISA for all or a subset of AA subscribers), subscriber scope or granularity (limits apply to each AA subscriber traffic).

The policer type and granularity can only be configured during creation. They cannot be modified. The policer profile must be removed from all AQP's in order to be removed. Changes to policer profile parameters take effect immediately for policers instantiated as result of AQP actions using this profile.

The `no` form of the command deletes the specified policer from the configuration.

**Parameters**

- `type` — Specifies the policer type.

  **Values**
  
  - `single-bucket-bandwidth` — Creates a profile for a single bucket (PIR) bandwidth limiting policer.
  - `dual-bucket-bandwidth` — Creates profile for a dual packet (PIR, CIR) bandwidth limiting policer.
  - `flow-rate-limit` — Creates profile for a policer limiting rate of flow set-ups.
  - `flow-count-limit` — Creates profile for a policer limiting total flow count.

- `granularity` — Specifies the granularity type.

  **Values**
  
  - `system` — Creates system policer profile for a policer that limits the traffic in the scope of all or a subset of AA subscribers on a given AA ISA.
  - `subscriber` — Creates a policer profile for a policer for each AA subscriber that limits the traffic in the scope of that subscriber.

- `create` — Keyword used to create the policer name and parameters.

- `Default` none

- `Parameters` `policer-name` — A string of up to 32 characters that identifies policer.
action

**Syntax**  
`action {priority-mark | permit-deny}

**Context**  
`config>app-assure>group>policer`

**Description**  
This command configures the action to be performed by single-bucket bandwidth policers for non-conformant traffic.

Dual bucket bandwidth policers cannot have their action configured and always mark traffic below CIR in profile, between CIR and PIR out of profile, and drop traffic above PIR. Flow policers always discard non-conformant traffic.

When multiple application assurance policers are configured against a single flow (including policers at both subscriber and system), the final action done to the flow/packet will be a logical OR of all policers’ actions. For example, if only of the policers requires the packet to be discarded, the packet will be dropped regardless of the action of the other policers.

**Default**  
permit-deny

**Parameters**

- **priority-mark** — Non-conformant traffic will be marked out of profile and the conformant traffic will be marked in profile. The new marking will overwrite any previous IOM QoS marking done to a packet.

- **permit-deny** — Non-conformant traffic will be dropped.

adaptation-rule

**Syntax**  
`adaptation-rule pir {max | min | closest} [cir {max | min | closest}]

**Context**  
`config>app-assure>group>policer`

**Description**  
This command defines 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 option. To change the CIR adaptation rule only, the current PIR rule must be part of the command executed.

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**  
closest

**Parameters**

- **max** — The operational PIR or CIR for the queue will be equal to or less than the administrative rate specified using the `rate` command.

- **min** — The operational PIR or CIR for the queue will be equal to or greater than the administrative rate specified using the `rate` command.

- **closest** — The operational PIR or CIR for the queue will be the rate closest to the rate specified using the `rate` command.
Group Commands

flow-count

Syntax

```
flow-count flow-count
no flow-count
```

Context

```
config>app-assure>group>policer
```

Description

This command configures the flow count for the flow-count-limit policer. It is recommended to configure flow count subscriber-level policer for AA subscribers to ensure fair usage of flow resources between AA subscribers.

Parameters

- `flow-count` — Specifies the flow count for the flow-count-limit policer.

---

cbs

Syntax

```
cbs committed-burst-size
no cbs
```

Context

```
config>app-assure>group>policer
```

Description

This command provides a mechanism to configure the committed burst size for the policer. It is recommended that CBS is configured larger than twice the maximum MTU for the traffic handled by the policer to allow for some burstiness of the traffic. CBS is configurable for dual-bucket bandwidth policers only.

The `no` form of the command resets the CBS value to its default.

Default

0

Parameters

- `committed-burst-size` — An integer value defining size, in kbytes, for the CBS of the policer.

  Values

  0 — 131071

---

mbs

Syntax

```
mbs maximum-burst-size
no mbs
```

Context

```
config>app-assure>group>policer
```

Description

This command provides a mechanism to configure the maximum burst size for the policer. It is recommended that MBS is configured larger than twice the MTU for the traffic handled by the policer to allow for some burstiness of the traffic. MBS is configurable for single-bucket, dual-bucket bandwidth and flow setup rate policers only.

The `no` form of the command resets the MBS value to its default.

Default

0

Parameters

- `maximum-burst-size` — An integer value defining either size, in kbytes, for the MBS of the bandwidth policer, or flow count for the MBS of the flow setup rate policers.

  Values

  0 — 131071
rate

Syntax rate pir-rate [cir cir-rate]
no rate

Context config>app-assure>group>policer

Description This command configures the administrative PIR and CIR for bandwidth policers and flow setup rate limits for flow policers. The actual rate sustained by the flow can be limited by other policers that may be applied to that flow’s traffic. This command does not apply to flow-count-limit policers. The cir option is applicable only to dual-bucket bandwidth policers. It is recommended to configure flow setup rate subscriber-level policer for AA subscribers to ensure fair usage of flow resources between AA subscribers.

The no form of the command resets the values to defaults.

Default 0

Parameters pir-rate — An integer specifying either the PIR rate in Kbps for bandwidth policers.

Values 1 — 100000000, max or flows

cir-rate — An integer specifying the CIR rate in Kbps.

Values 0 — 100000000, max
Policy Commands

policy

Syntax: policy
Context: config>app-assure>group>policy
Description: This command enables the context to configure parameters for application assurance policy. To edit any policy content begin command must be executed first to enter editing mode. The editing mode is left when the abort or commit commands are issued.

abort

Syntax: abort
Context: config>app-assure>group>policy
Description: This command ends the current editing session and aborts any changes entered during this policy editing session.

begin

Syntax: begin
Context: config>app-assure>group>policy
Description: This command begins a policy editing session. The editing session continues until one of the following conditions takes place:
- Abort or commit is issued.
- Control complex resets.
The editing session is not interrupted by:
- HA activity switch.
- CLI session termination (for example, as result of closing a Telnet session).

commit

Syntax: commit
Context: config>app-assure>group>policy
Description: This command commits changes made during the current editing session. None of the policy changes done will take effect until commit command is issued. If the changes can be successfully committed,
no errors detected during the commit during cross-reference verification against exiting application assurance configuration, the editing session will also be closed.

The newly committed policy takes affect immediately for all new flows, existing flows will transition onto the new policy shortly after the commit.

### app-group

**Syntax**

```
app-group application-group-name [create]
no app-group application-group-name
```

**Context**

```
config>app-assure>group>policy
```

**Description**

This command creates an application group for an application assurance policy.

The no form of the command deletes the application group from the configuration. All associations must be removed in order to delete a group.

**Default**

`no app-group`

**Parameters**

- `application-group-name` — A string of up to 32 characters uniquely identifying this application group in the system.

- `create` — Mandatory keyword used when creating an application group. The `create` keyword requirement can be enabled/disabled in the `environment>create` context.

### app-filter

**Syntax**

```
app-filter
```

**Context**

```
config>app-assure>group>policy
```

**Description**

This command enables the context to configure an application filter for application assurance.

### app-profile

**Syntax**

```
app-profile app-profile-name [create]
no app-profile app-profile-name
```

**Context**

```
config>app-assure>group>policy
```

**Description**

This command creates an application profile and enables the context to configure the profile parameters.

The no form of the command removes the application profile from the configuration.

**Default**

`none`

**Parameters**

- `app-profile-name` — Specifies the name of the application profile up to 32 characters in length.

- `create` — Mandatory keyword used when creating an application profile. The `create` keyword requirement can be enabled/disabled in the `environment>create` context.
Group Commands

app-qos-policy

Syntax  app-qos-policy
Context  config>app-assure>group>policy
Description  This command enables the context to configure an application QoS policy.

app-service-options

Syntax  app-service-options
Context  config>app-assure>group>policy
Description  This command enables the context to configure application service option characteristics.

diff

Syntax  diff
Context  config>app-assure>group>policy
Description  This command compares the newly configured policy against the operational policy.

application

Syntax  application application-name [create]
no application application-name
Context  config>app-assure>group>policy
Description  This command creates an application of an application assurance policy.
The no form of the command deletes the application. To delete an application, all associations to the application must be removed.
Default  none
Parameters  application-name — Specifies a string of up to 32 characters uniquely identifying this application in the system.
create — Mandatory keyword used when creating an application. The create keyword requirement can be enabled/disabled in the environment>create context.

policy-override

Syntax  policy-override
Application Assurance Commands

Context config>app-assure>group>policy

Description This command enables the context to configure policy override parameters.

policy aa-sub

Syntax policy aa-sub {sap sap-id | spoke-sdp sdp-id:vc-id} [create]
no policy aa-sub {sap sap-id | spoke-sdp sdp-id:vc-id}

Context config>app-assure>group>policy>policy-override

Description This command specifies the SAP or SDP

Parameters sap sap-id — Specifies the physical port identifier portion of the SAP definition.
sdp-id:vc-id — Specifies the spoke SDP ID and VC ID.

Values 1 — 17407
       1 — 4294967295

characteristic

Syntax characteristic characteristic-name value value-name
no characteristic characteristic-name

Context config>app-assure>group>policy>policy-override

Description This command configure an override characteristic and value.

Parameters characteristic-name — Specifies the characteristic name up to 32 characters in length.
value value-name — Specifies the override characteristic value for the application profile
characteristic used by the Application assurance subscriber.

app-group

Syntax app-group application-group-name

Context config>app-assure>group>policy>application

Description This command associates an application with an application group of an application assurance policy.

Default none

Parameters application-name — A string of up to 32 characters uniquely identifying an existing application in
the system.
APPLICATION FILTER COMMANDS

entry

Syntax

entry entry-id [create]
no entry entry-id

Context
config>app-assure>group>policy>app-filter

Description
This command creates an application filter entry.

App filter entries are an ordered list, the lowest numerical entry that matches the flow defines the application for that flow.

An application filter entry or entries configures match attributes of an application.

The no form of this command deletes the specified application filter entry.

Default
none

Parameters
entry-id — An integer that identifies an app-filter entry.

Values
1 — 65535

create — Keyword used to create the entry.

application

Syntax
application application-name

Context
config>app-assure>group>policy>app-filter>entry

Description
This command assigns this application filter entry to an existing application. Assigning the entry to Unknown application restores the default configuration.

Default
unknown application

Parameters
application-name — Specifies an existing application name.

expression

Syntax
expression expr-index expr-type {eq | neq} expr-string
no expression expr-index

Context
config>app-assure>group>policy>app-filter>entry

Description
This command configures string values to use in the application definition.

Parameters
expr-index — Specifies an index value which represents expression substrings.

Values
1 — 4
expr-type — Represents a type (and thereby the expression substring).

- http-host, http-uri, http-referer, sip-ua, sip-uri
- http-host — Matches the string against the HTTP Host field.
- http-uri — Matches the string against the HTTP URI field.
- http-referer — Matches the string against the HTTP Referer field.
- http-user-agent —
- sip-ua — Matches the string against the SIP UA field.
- sip-uri — Matches the string against the SIP URI field.
- sip-mt — Matches the string against the SIP MT field.
- citrix-app — Matches the string against the Citrix app field.
- h323-product-id — Matches the string against the h323-product-id field.
- tls-cert-subj-org-name — Matches the TLS Certificate Subject Organization Name substring.
- tls-cert-subj-common-name — Matches the TLS Certificate Subject Common Name substring.
- * - udp/tcp wildcard

eq — Specifies the equal to comparison operator to match the specified HTTP string.
neq — Specifies the not equal to comparison operator to match the specified HTTP string.

expr-string — Specifies an expression string, up to 64 characters, used to define a pattern match. Denotes a printable ASCII substring used as input to an application assurance filter match criteria object.

- The following syntax is permitted within the substring to define the pattern match criteria:
  - ^<substring>* - matches when <substring> is at the beginning of the object.
  - *<substring>* - matches when <substring> is at any place within the object.
  - *<substring>$ - matches when <substring> is at the end of the object.
  - ^<substring>$ - matches when <substring> is the entire object.

- Rules for <substring> characters:
  - <substring> must contain printable ASCII characters.
  - <substring> must not contain the “double quote” character or the “ ” (space) character on its own.
  - <substring> match is case sensitive.
  - <substring> must not include any regular expression meta-characters.

- The “\” (slash) character is used as an ESCAPE sequence. The following ESCAPE sequences are permitted within the <substring>:

<table>
<thead>
<tr>
<th>Character to match</th>
<th>&lt;substring&gt; input</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hexidecimal Octet YY</td>
<td>\xYY</td>
</tr>
</tbody>
</table>

  Note: A <substring> that uses the \\ (backslash) ESCAPE character which is not followed by a “\” or “\x” and a 2-digit hex octet is not valid.

Operational notes:

1. When matching a TCP flow against HTTP-string based applications, the HTTP header fields are collected from the first HTTP request (for example a GET or a POST) for a given TCP flow. The collected strings are then evaluated against each HTTP flow created within the given TCP flow to determine whether a given HTTP flow matches the application. By not specifying a protocol, the HTTP expressions are matched against all protocols in the
HTTP family. By specifying a specific HTTP protocol (for example, http_video) the expression match can be constrained to a subset of the HTTP protocols.

2. To uniquely identify a SIP-based application a protocol match is not required in the app-filter entry with the SIP expression. The SIP expression match is performed against any protocol in the SIP family (such as sip and rtp_sip). By specifying a specific SIP protocol (like rtp_sip) the expression match can be constrained to a subset of the SIP protocols.

### flow-setup-direction

**Syntax**

```plaintext
flow-setup-direction {subscriber-to-network | network-to-subscriber | both}
```

**Context**

`config>app-assure>group>policy>app-filter>entry`

**Description**

This command configures the direction of flow setup to which the application filter entry is to be applied.

**Parameters**

- **subscriber-to-network** — Specifies that the app-filter entry will be applied to flows initiated by a local subscriber.
- **network-to-subscriber** — Specifies that the app-filter entry will be applied to flows initiated from a remote destination towards a local subscriber.
- **both** — Specifies that the app filter entry will be applied for subscriber-to-network and network-to-subscriber traffic.

**Default**

both

### ip-protocol-num

**Syntax**

```plaintext
ip-protocol-num {eq | neq} protocol-id
no ip-protocol-num
```

**Context**

`config>app-assure>group>policy>app-filter>entry`

**Description**

This command configures the IP protocol to use in the application definition. The `no` form of the command restores the default (removes IP protocol number from application criteria defined by this app-filter entry).

**Default**

none

**Parameters**

- **eq** — Specifies that the value configured and the value in the flow must be equal.
- **neq** — Specifies that the value configured differs from the value in the flow.
- **protocol-id** — Specifies the decimal value representing the IP protocol to be used as an IP filter match criterion. Well known protocol numbers include ICMP (1), TCP (6), UDP (17).

The `no` form the command removes the protocol from the match criteria.

**Values**

- `0` — 255 (values can be expressed in decimal, hexadecimal, or binary - DHB)
- Keywords: none, crtp, crudp, egp, eigrp, encaps, ether-ip, gre, icmp, idrp, igmp, igp, ip, ipv6, ipv6-frag, ipv6-icmp, ipv6-no-nxt, ipv6-opts, ipv6-route, isis, iso-ip,
server-address

**Syntax**

```
server-address {eq | neq} ip-address
no server-address
```

**Context**

`config>app-assure>group>policy>app-filter>entry`

**Description**

This command configures the server address to use in application definition. The server IP address may be the source or destination, network or subscriber IP address.

The `no` form of the command restores the default (removes the server address from application criteria defined by this entry).

**Default**

no net-address

**Parameters**

- **eq** — Specifies a comparison operator that the value configured and the value in the flow are equal.
- **neq** — Specifies a comparison operator that the value configured differs from the value in the flow.
- **ip-address** — Specifies a valid unicast address.

**Values**

- **ipv4-address** — a.b.c.d[/mask]
  - mask - [1..32]
- **ipv6-address** — x:x:x:x:x/x:prefix-length
  - x:x:x:x:x:d:d:d
  - x - [0..FFFF]H
  - d - [0..255]D
  - prefix-length — [1..128]

server-port

**Syntax**

```
server-port {eq | neq | gt | lt} server-port-number
server-port {eq | neq} range start-port-number end-port-number
server-port {eq} {port-num | range start-port-number end-port-number} {first-packet-trusted | first-packet-validate}
no server-port
```

**Context**

`config>app-assure>group>policy>app-filter>entry`

**Description**

This command specifies the server TCP or UDP port number to use in the application definition.

The `no` form of the command restores the default (removes server port number from application criteria defined by this app-filter entry).

**Default**

no server-port (the server port is not used in the application definition)

**Parameters**

- **eq** — Specifies that the value configured and the value in the flow are equal.
- **neq** — Specifies that the value configured differs from the value in the flow.
- **gt** — Specifies all port numbers greater than server-port-number match.
Group Commands

It — Specifies all port numbers less than server-port-number match.

server-port-num — Specifies a valid server port number.

Values

0 — 65535

start-port-num, end-port-num — Specifies the starting or ending port number.

Values

0 — 65535

Server Port Options:

• **No option specified**: TCP/UDP port applications with full signature verification:
  - AA ensures that other applications that can be identified do not run over a well-known port.
  - Application-aware policy applied once signature-based identification completes (likely requiring several packets).

• **first-packet-validate**: TCP/UDP trusted port applications with signature verification:
  - Application identified using well known TCP/UDP port based filters and re-identified once signature identification completes.
  - AA policy applied from the first packet of a flow while continuing signature-based application identification. Policy re-evaluated once the signature identification completes, allowing to detect improper/unexpected applications on a well-known port.

• **first-packet-trusted**: TCP/UDP trusted port applications - no signature verification:
  - Application identified using well known TCP/UDP port based filters only.
  - Application Aware policy applied from the first packet of a flow.
  - No signature processing assumes operator/customer trusts that no other applications can run on the well-known TCP/UDP port (statistics collected against trusted_tcp or trusted_udp protocol).

protocol

**Syntax**

protocol (eq | neq) protocol-name

no protocol

**Context**

config>app-assure>group>policy>app-filter>entry

**Description**

This command configures protocol signature in the application definition.

The no form of the command restores the default (removes protocol from match application defined by this app-filter entry).

**Default**

no protocol

**Parameters**

eq — Specifies that the value configured and the value in the flow are equal.

neq — Specifies that the value configured differs from the value in the flow.

protocol-name — A string of up to 32 characters identifying a predefined protocol.
APPLICATION PROFILE COMMANDS

capacity-cost

Syntax  
capacity-cost cost
nocapacity-cost

Context  
config>app-assure>group>policy>app-profile

Description  
This command configures an application profile capacity cost. Capacity-Cost based load balancing allows a cost to be assigned to diverted SAPs (with the app-profile) and this is then used for load-balancing SAPs between ISAs as well as for a threshold that notifies the operator if/when capacity planning has been exceeded.

Parameters  

cost — Specifies the profile capacity cost.

Values  
1 — 65535

characteristic

Syntax  
characteristic characteristic-name value value-name

no characteristic characteristic-name

Context  
config>app-assure>group>policy>app-profile

Description  
This command assigns one of the existing values of an existing application service option characteristic to the application profile. The no form of the command removes the characteristic from the application profile.

Default  
none

Parameters  
characteristic-name — Specifies the name of an existing ASO characteristic.

value value-name — Specifies the name for the application profile characteristic up to 32 characters in length.

divert

Syntax  
[no] divert

Context  
config>app-assure>group>policy>app-profile

Description  
This command enables the redirection of traffic to AA ISA for the system-wide forwarding classes diverted to application assurance (divert-fc) for AA subscribers using this application profile. The no form of the command stops redirect of traffic to AA ISAs for the AA subscribers using this application profile.
Default  no divert
APPLICATION QoS POLICY COMMANDS

**entry**

**Syntax**

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

**Context**

```
config>app-assure>group>policy>aqp
```

**Description**

This command creates an application QoS policy entry. A flow that matches multiple Application QoS policies (AQP) entries will have multiple AQP entries actions applied. When a conflict occurs for two or more actions, the action from the AQP entry with the lowest numerical value takes precedence.

The `no` form of this command deletes the specified application QoS policy entry.

**Default**

none

**Parameters**

- `entry-id` — An integer identifying the AQP entry.
  - **Values**
    - 1 — 65535
  - `create` — Mandatory keyword creates the entry. The `create` keyword requirement can be enabled/disabled in the `environment>create` context.

**action**

**Syntax**

```
action
```

**Context**

```
config>app-assure>group>policy>aqp>entry
```

**Description**

This command enables the context to configure AQP actions to be performed on flows that match the AQP entry’s match criteria.

**bandwidth-policer**

**Syntax**

```
bandwidth-policer policer-name
no bandwidth-policer
```

**Context**

```
config>app-assure>group>policy>aqp>entry>action
```

**Description**

This command assigns an existing bandwidth policer as an action on flows matching this AQP entry. The match criteria for the AQP entry must specify a uni-directional traffic direction before a policer action can be configured. If a policer is used in one direction in an AQP match entry the same policer name cannot be used by another AQP entry which uses a different traffic direction match criteria.

When multiple policers apply to a single flow, the final action on a packet is the worse case of all policer outcome (for example, if one of the policers marks packet out of profile, the final marking will reflect that).
Group Commands

The **no** form of the command removes bandwidth policer from actions on flows matching this AQP entry.

**Default**  
no bandwidth-policer

**Parameters**  
policer-name — The name of the existing flow setup rate policer for this application assurance profile. The **policer-name** is configured in the config>app-assure>group>policer context.

drop

**Syntax**  
[no] drop

**Context**  
config>app-assure>group>policy>aqp>entry>action

**Description**  
This command configures the drop action on flows matching this AQP entry. When enabled, all flow traffic matching this AQP entry will be dropped. When drop action is part of a set of multiple actions to be applied to a single flow as result of one or more AQP entry match, drop action will be performed first and no other action will be invoked on that flow.

The **no** form of the command disables the drop action on flows matching this AQP entry.

**Default**  
no drop

flow-count-limit

**Syntax**  
flow-count-limit **policer-name**

**Context**  
config>app-assure>group>policy>aqp>entry>action

**Description**  
This command assigns an existing flow count limit policer as an action on flows matching this AQP entry.

The match criteria for the AQP entry must specify a uni-directional traffic direction before a policer action can be configured. If a policer is used in one direction in an AQP match entry the same policer name cannot be used by another AQP entry which uses a different traffic direction match criteria.

When multiple policers apply to a single flow, the final action on a packet is the worse case of all policer outcome (for example, if one of the policers marks packet out of profile, the final marking will reflect that).

The **no** form of the command removes this flow policer from actions on flows matching this AQP entry.

**Default**  
no flow-count-limit

**Parameters**  
policer-name — The name of the existing flow setup rate policer for this application assurance profile. The **policer-name** is configured in the config>app-assure>group>policer context.
flow-rate-limit

Syntax  
\texttt{flow-rate-limit \textit{policer-name}}

no flow-rate-limit

Context  
\texttt{config>app-assure>group>policy>aqp>entry>action}

Description  
This command assigns an existing flow setup rate limit policer as an action on flows matching this AQP entry.

The match criteria for the AQP entry must specify a uni-directional traffic direction before a policer action can be configured. If a policer is used in one direction in an AQP match entry the same policer name cannot be used by another AQP entry which uses a different traffic direction match criteria.

When multiple policers apply to a single flow, the final action on a packet is the worse case of all policer outcome (for example, if one of the policers marks packet out of profile, the final marking will reflect that).

The \texttt{no} form of the command removes this flow policer from actions on flows matching this AQP entry.

Default  
no flow-rate-limit

Parameters  
\textit{policer-name} — The name of the existing flow setup rate policer for this application assurance profile. The \textit{policer-name} is configured in the \texttt{config>app-assure>group>\textcolor{red}{policer}} context.

http-error-redirect

Syntax  
\texttt{http-error-redirect \textit{redirect-name}}

no http-error-redirect

Context  
\texttt{config>app-assure>group>policy>aqp>entry>action}

Description  
This command specifies the HTTP error redirect that will be applied as defined in the redirect table. An empty value specifies no HTTP error redirect.

Parameters  
\textit{redirect-name} — Specifies an http-error redirect action, up to 32 characters in length, for flows matching this entry.

mirror-source

Syntax  
\texttt{mirror-source [all-inclusive] \textit{mirror-service-id}}

no mirror-source

Context  
\texttt{config>app-assure>group>policy>aqp>entry>action}

Description  
This command configures an application-based policy mirroring service that uses this AA ISA group’s AQP entry as a mirror source. When configured, AQP entry becomes a mirror source for IP packets seen by the AA (note that the mirrored packet is an IP packet analyzed by AA and does not include encapsulations present on the incoming interfaces).

Default  
no mirror-source
Parameters

all-inclusive — Specifies that all packets during identification phase that could match a given AQP rule are mirrored in addition to packets after an application identification completes that match the AQP rule. This ensures all packets of a given flow are mirrored at a cost of sending unidentified packets that once the application is identified will no longer match this AQP entry.

mirror-service-id — Specifies the mirror source service ID to use for flows that match this policy.

Values

1 — 214748364
svc-name: 64 char max

remark

Syntax remark

Context config>app-assure>group>policy>aqp>entry>action

Description

This command configures remark action on flows matching this AQP entry.

dscp

Syntax dscp in-profile dscp-name out-profile dscp-name

Context config>app-assure>group>policy>aqp>entry>action>remark

Description

This command enables the context to configure DSCP remark action or actions on flows matching this AQP entry. When enabled, all packets for all flows matching this AQP entry will be remarked to the configured DSCP name.

DSCP remark can only be applied when the entry remarks forwarding class or forwarding class and priority. In-profile and out-of-profile of a given packet for DSCP remark is assessed after all AQP policing and priority remarking actions took place.

The no form of the command stops DSCP remarking action on flows matching this AQP entry.

Parameters

in-profile dscp-name — Specifies the DSCP name to use to remark in-profile flows that match this policy.

out-profile dscp-name — Specifies the DSCP name to use to remark out-of-profile flows that match this policy.

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, cs5, cp41, cp42, cp43, cp44, cp45, ef, cp47, nc1, cp49, cp50, cp51, cp52, cp53, cp54, cp55, nc2, cp57, cp58, cp59, cp60, cp61, cp62, cp63

fc

Syntax fc fc-name

no fc
Application Assurance Commands

Context config>app-assure>group>policy>aqp>entry>action>remark

Description This command configures remark FC action on flows matching this AQP entry. When enabled, all packets for all flows matching this AQP entry will be remarked to the configured forwarding class. The no form of the command stops FC remarking action on packets belonging to flows matching this AQP entry.

Parameters fc-name — Configure the FC remark action for flows matching this entry.

   Values be, l2, af, l1, h2, ef, h1, nc

priority

Syntax priority priority-level
   no priority

Context config>app-assure>group>policy>aqp>entry>action>remark

Description This command configures remark discard priority action on flows matching this AQP entry. When enabled, all packets for all flows matching this AQP entry will be remarked to the configured discard priority.

Default no priority

Parameters priority-level — Specifies the priority to apply to a packet.

   Values high, low

match

Syntax match

Context config>app-assure>group>policy>aqp>entry

Description This command enables the context to configure flow match rules for this AQP entry. A flow matches this AQP entry only if it matches all the match rules defined (logical and of all rules). If no match rule is specified, the entry will match all flows.

aa-sub

Syntax aa-sub esm {eq | neq} sub-ident-string
   aa-sub sap {eq | neq} sap-id
   aa-sub spoke-sdp {eq | neq} sdp-id:vc-id
   aa-sub transit {eq | neq} transit-aasub-name
   no aa-sub

Context config>app-assure>group>policy>aqp>entry>match

Description This command specifies a Service Access Point (SAP) or an ESM subscriber as matching criteria.
Group Commands

The \textbf{no} form of the command removes the SAP or ESM matching criteria.

**Parameters**

- \textbf{eq} — Specifies that the value configured and the value in the flow are equal.
- \textbf{neq} — Specifies that the value configured differs from the value in the flow.

- \textit{sub-ident-string} — Specifies the name of an existing application assurance subscriber.
- \textit{sap-id} — Specifies the SAP ID.

- \textit{sap sap-id} — Specifies the physical port identifier portion of the SAP definition. Refer to Appendix A: Common CLI Command Descriptions on page 533 for syntax.

- \textit{sdp-id:vc-id} — Specifies the spoke SDP ID and VC ID.

  **Values**

  - $1 - 17407$
  - $1 - 4294967295$

- \textit{transit-aa-sub-name} — Specifies the name of a transit AA subscriber.

**app-group**

**Syntax**

\begin{verbatim}
app-group {eq | neq} application-group-name
no app-group
\end{verbatim}

**Context**

\texttt{config>app-assure>group>policy>aqp>entry>match}

**Description**

This command adds app-group to match criteria used by this AQP entry. The \textbf{no} form of the command removes the app-group from match criteria for this AQP entry.

**Default**

no app-group

**Parameters**

- \textbf{eq} — Specifies that the value configured and the value in the flow are equal.
- \textbf{neq} — Specifies that the value configured differs from the value in the flow.

- \textit{application-group-name} — The name of the existing application group entry. The \textit{application-group-name} is configured in the \texttt{config>app-assure>group>policy>aqp>entry>match} context.

**application**

**Syntax**

\begin{verbatim}
application {eq | neq} application-name
no application
\end{verbatim}

**Context**

\texttt{config>app-assure>group>policy>aqp>entry>match}

**Description**

This command adds an application to match criteria used by this AQP entry. The \textbf{no} form of the command removes the application from match criteria for this AQP entry.

**Default**

no application

**Parameters**

- \textbf{eq} — Specifies that the value configured and the value in the flow are equal.
- \textbf{neq} — Specifies that the value configured differs from the value in the flow.
**characteristic**

**Syntax**
```
characteristic characteristic-name eq value-name
no characteristic
```

**Context**
```
config>app-assure>group>policy>aqp>entry>match
```

**Description**
This command adds an existing characteristic and its value to the match criteria used by this AQP entry. The no form of the command removes the characteristic from match criteria for this AQP entry.

**Default**
no characteristic

**Parameters**
- `eq` — Specifies that the value configured and the value in the flow are equal.
- `characteristic-name` — The name of the existing ASO characteristic up to 32 characters in length.
- `value-name` — The name of an existing value for the characteristic up to 32 characters in length.

**dscp**

**Syntax**
```
dscp {eq | neq} dscp-name
no dscp
```

**Context**
```
config>app-assure>group>policy>aqp>entry>match
```

**Description**
This command adds a DSCP name to the match criteria used by this AQP entry. The no form of the command removes dscp from match criteria for this AQP entry.

**Default**
no dscp

**Parameters**
- `eq` — Specifies that the value configured and the value in the flow are equal.
- `neq` — Specifies that the value configured differs from the value in the flow.
- `dscp-name` — The DSCP name to be used in match.

**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

**dst-ip**

**Syntax**
```
dst-ip {eq | neq} ip-address
no dst-ip
```

**OS Multi-Service ISA Guide**
Group Commands

Context config>app-assure>group>policy>aqp>entry>match

Description This command specifies a destination IP address to use as match criteria.

Parameters

- `eq` — Specifies that a successful match occurs when the flow matches the specified address or prefix.
- `neq` — Specifies that a successful match occurs when the flow does not match the specified address or prefix.

`ip-address` — Specifies a valid unicast address.

Values

- ipv4-address a.b.c.d[/mask]
  - mask - [1..32]
- ipv6-address x:x:x:x:x:x:x:[/prefix-length]
  - x - [0..FFFF]
  - d - [0..255]
  - prefix-length [1..128]

```
Context config>app-assure>group>policy>aqp>entry>match

Description This command specifies a destination TCP/UDP port or destination range to use as match criteria. The no form of the command removes the parameters from the configuration.

Parameters

- `eq` — Specifies that a successful match occurs when the flow matches the specified port.
- `neq` — Specifies that a successful match occurs when the flow does not match the specified port.

`port-num` — Specifies the destination port number.

Values

- 0 — 65535

`start-port-num end-port-num` — Specifies the start or end destination port number.

Values

- 0 — 65535

```

Context config>app-assure>group>policy>aqp>entry>match

Description This command specifies a source TCP/UDP address to use as match criteria.

Parameters `eq` — Specifies that a successful match occurs when the flow matches the specified address or prefix.
neq — Specifies that a successful match occurs when the flow does not match the specified address or prefix.

ip-address — Specifies a valid IPv4 unicast address.

Values

- ipv4-address: a.b.c.d[/mask]
  - mask: [1..32]
- ipv6-address: x:x:x:x:x:x:x:/prefix-length
  - x: [0..FFFF]H
  - d: [0..255]D
  - prefix-length: [1..128]

src-port

Syntax

src-port {eq | neq} port-num
src-port {eq | neq} range start-port-num end-port-num
no src-port

Context

config>app-assure>group>policy>aqp>entry>match

Description

This command specifies a source IP port or source range to use as match criteria.

The no form of the command removes the parameters from the configuration.

Parameters

- eq — Specifies that a successful match occurs when the flow matches the specified port.
- neq — Specifies that a successful match occurs when the flow does not match the specified port.
- port-num — Specifies the source port number.

Values

- 0 — 65535

start-port-num end-port-num — Specifies the start or end source port number.

Values

- 0 — 65535

traffic-direction

Syntax

traffic-direction {subscriber-to-network | network-to-subscriber | both}

Context

config>app-assure>group>policy>aqp>entry>match

Description

This command specifies the direction of traffic where the AQP match entry will be applied.

To use a policer action with the AQP entry the match criteria must specify a traffic-direction of either subscriber-to-network or network-to-subscriber.

Default

both

Parameters

- subscriber-to-network — Traffic from a local subscriber will match this AQP entry.
- network-to-subscriber — Traffic to a local subscriber will match this AQP entry.
both — Combines subscriber-to-network and network-to-subscriber.
APPLICATION SERVICE OPTIONS COMMANDS

characteristic

Syntax  
characteristic characteristic-name [create]  
no characteristic characteristic-name

Context  config>app-assure>group>policy>aso

Description  This command creates the characteristic of the application service options. The no form of the command deletes characteristic option. To delete a characteristic, it must not be referenced by other components of application assurance.

Default  none

Parameters  
characteristic-name — Specifies a string of up to 32 characters uniquely identifying this characteristic.

create — Mandatory keyword used to create when creating a characteristic. The create keyword requirement can be enabled/disabled in the environment>create context.

default-value

Syntax  
default-value value-name  
no default-value

Context  config>app-assure>group>policy>aso>char

Description  This command assigns one of the characteristic values as default. When a default value is specified, app-profile entries that do not explicitly include this characteristic inherit the default value and use it as part of the AQP match criteria based on that app-profile.

A default-value is required for each characteristic. This is evaluated at commit time.

The no form of the command removes the default value for the characteristic.

Default  none

Parameters  value-name — Specifies the name of an existing characteristic value.

value

Syntax  
[no] value value-name

Context  config>app-assure>group>policy>aso>char

Description  This command configures a characteristic value. The no form of the command removes the value for the characteristic.
### Group Commands

**Default**  none

**Parameters**  
- `value-name` — Specifies a string of up to 32 characters uniquely identifying this characteristic value.
**CUSTOM PROTOCOL COMMANDS**

**custom-protocol**

**Syntax**

```
custom-protocol custom-protocol-id ip-protocol-num protocol-id [create]
custom-protocol custom-protocol-id
no custom-protocol custom-protocol-id
```

**Context**

```
config>app-assure>group>policy
```

**Description**

This command creates and enters configuration context for custom protocols. Custom protocols allow the creation of TCP and UDP-based custom protocols (based on the *ip-protocol-num* option) that employ pattern-match at offset in protocol signature definition.

Operator-configurable custom-protocols are evaluated ahead of any Alcatel-Lucent provided protocol signature in order of *custom-protocol-id* (the lower ID is matched first in case of flow matching multiple custom-protocols) within the context the protocol is defined.

Custom protocols must be created before they can be used in application definition but do not have to be enabled. To reference a custom protocol in application definition, or any other CLI configuration one must use protocol name that is a concatenation of “custom_” and `<custom-protocol-id>`, (for example `custom_01`, `custom_02` ... `custom_10`, etc.). This concatenation is also used when reporting custom protocol statistics.

**Parameters**

- `custom-protocol-id` — Specifies the index into the protocol list that defines a custom protocol for application assurance.
  - **Values**
    - `1 — 10`

- `protocol-id` — Specifies the IP protocol number to match against for the custom protocol.
  - **Values**
    - `0 — 255`, Protocol numbers accepted in DHB,
      - keywords: `none, crtp, crudp, egp, eigrp, encap, ether-ip, gre, icmp, idrp, igmp, igrp, ip, ipv6, ipv6-frag, ipv6-icmp, ipv6-no-nxt, ipv6-opts, ipv6-route, isis, iso-ip, l2tp, ospf-igrp, pim, pnni, ptp, rdp, rsvp, stp, tcp, udp, vrrp`
    - `* - udp/tcp wildcard`

- `create` — Mandatory keyword used when creating custom protocol. The `create` keyword requirement can be enabled/disabled in the `environment>create` context.

**expression**

**Syntax**

```
expression expr-index eq expr-string offset payload-octet-offset direction direction
no expression expr-index
```

**Context**

```
config>app-assure>group>policy>custom-protocol
```

**Description**

This command configures an expression string value for pattern-based custom protocols match. A flow matches a custom protocol if the specified string is found at an offset of a TCP/UDP of the first payload packet.
Options:

- **client-to-server** — A pattern will be matched against a flow from a TCP client.
- **server-to-client** — A pattern will be matched against a flow from a TCP server.
- **any** — A pattern will be matched against a TCP/UDP flow in any direction (towards or from AA subscriber)

The **no** form of this command deletes a specified string expression from the definition.

### Parameters

- **expr-index** — Specifies the expression substring index.
  - **Values**
    - **1**

- **expr-string** — Denotes a printable ASCII string, up to 16 characters, used to define a custom protocol match. Rules for expr-string characters:
  - Must contain printable ASCII characters.
  - Must not contain the “double quote” character or the “ ” (space) character on its own.
  - Match is case sensitive.
  - Must not include any regular expression meta-characters.

The “\” (slash) character is used as an ESCAPE sequence. The following ESCAPE sequences are permitted within the expr-string:

<table>
<thead>
<tr>
<th>Character to match</th>
<th>expr-string input</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hexadecimal Octet YY</td>
<td>\xYY</td>
</tr>
</tbody>
</table>

- **offset payload-octet-offset** — specifies the offset (in octets) into the protocol payload, where the expr-string match criteria will start.
  - **Values**
    - **0 — 127**

- **direction** — Specifies the protocol direction to match against to resolve to a custom protocol.
  - **Values**
    - **client-to-server, server-to-client, any**
Statistics Commands

statistics

Syntax

statistics

Context

config>app-assure>group

Description

This command enables the context to configure accounting and billing statistics for this AA ISA group.

app-group

Syntax

[no] app-group app-group-name

Context

config>app-assure>group>statistics

Description

This command enables the context to configure accounting and statistics collection parameters per system for application groups of application assurance for a given AA ISA group/partition.

The no form of the command removes the application group name.

Default

none

Parameters

app-group-name — Specifies an existing application group name up to 32 characters in length.

aa-sub

Syntax

aa-sub

Context

config>app-assure>group>statistics

Description

This command enables the context to configure accounting and statistics collection parameters per application assurance subscribers.

aa-sub-study

Syntax

aa-sub-study study-type

Context

config>app-assure>group>statistics

Description

This command enables the context to configure accounting and statistics collection parameters per application assurance special study subscribers.

Parameters

study-type — Specifies special study protocol subscriber stats.

  Values application, protocol
Group Commands

application

Syntax  
application application-name

Context  
config>app-assure>group>statistics

Description  
This command enables the context to configure accounting and statistics collection parameters per system for application groups of application assurance for a given AA ISA group/partition.

The no form of the command removes the application name.

Default  
none

Parameters  
application-name — Specifies an existing application name up to 32 characters in length.

accounting-policy

Syntax  
accounting-policy acct-policy-id

Context  
config>app-assure>group>statistics>app-grp
config>app-assure>group>statistics>app
config>app-assure>group>statistics>protocol
config>app-assure>group>statistics>aa-sub
config>app-assure>group>statistics>aa-sub-study
config>isa>aa-grp>statistics

Description  
This command specifies the existing accounting policy to use for AA. Accounting policies are configured in the config>log>accounting-policy context.

Parameters  
acct-policy-id — Specifies the existing accounting policy to use for applications.

Values  
1 — 99

aggregate-stats

Syntax  
[no] aggregate-stats

Context  
config>app-assure>group>statistics>app-grp

Description  
This command enables aggregate statistics collection.

The no form of the command disables the collection.

protocol

Syntax  
protocol

Context  
config>app-assure>group>statistics

Description  
This command enables the context to configure accounting and statistics collection parameters per system for protocols of application assurance for a given AA ISA group/partition.
aa-sub

**Syntax**

```plaintext
[no] aa-sub {esm sub-ident-string | sap sap-id} | spoke-sdp sdp-id:vc-id | transit transit-aasub-name}
```

**Context**

`config>app-assure>group>statistics>aa-sub-study`

**Description**

This command adds an existing subscriber identification to a group of special study subscribers (for example, subscribers for which per subscriber statistics and accounting records can be collected for protocols and applications of application assurance).

The **no** form of the command removes the subscriber from the special study subscribers.

Up to 100 subscribers can be configured into the special study group for protocols and up to a 100 potentially different subscribers can be configured into the special study group for applications.

When adding a subscriber to the special study group, accounting records and statistics generation will commence immediately. When removing a subscriber from the group, special study statistics and accounting records for that subscriber in the current interval will be lost.

**Default**

none

**Parameters**

- `sub-ident-string` — The name of a subscriber ID. Note that the subscriber does not need to be currently active. Any sub-ident-string will be accepted. When the subscriber becomes active, statistics generation will start automatically at that time.
- `esm sub-ident-string` — Specifies an existing subscriber identification policy name.
- `sap sap-id` — Specifies the physical port identifier portion of the SAP definition. Refer to Appendix A: Common CLI Command Descriptions on page 533 for syntax.
- `spoke-id sdp-id:vc-id` — Specifies the spoke SDP ID and VC ID.
  - **Values**
    - 1 — 17407
    - 1 — 4294967295
- `transit transit-aasub-name` — Specifies an existing transit subscriber name string up to 32 characters in length.

**collect-stats**

**Syntax**

```plaintext
[no] collect-stats
```

**Context**

`config>app-assure>group>statistics>app-grp`  
`config>app-assure>group>statistics>application`  
`config>app-assure>group>statistics>protocol`  
`config>app-assure>group>statistics>aa-sub`  
`config>app-assure>group>statistics>aa-sub-study`  
`config>isa>aa-grp>statistics`

**Description**

This command enables statistic collection within the applicable context.

**Default**

disabled
max-throughput-stats

Syntax  
[no] max-throughput-stats

Context  
config>app-assure>group>statistics>app-sub

Description  
This command enables the collection of max-throughput statistics. The no form of the command disables the collection.

protocol

Syntax  
protocol protocol-name
no protocol

Context  
config>app-assure>group>statistics>app-sub

Description  
This command configures protocol signature in the application definition. The no form of the command restores the default (removes protocol from match application defined by this app-filter entry).

Default  
no protocol

Parameters  
protocol-name  —  A string of up to 32 characters identifying a predefined protocol signature.

Values  
Use the show>application-assurance>protocols command to display a full list of protocols available based on isa-aa.tim image used with the given release software.

transit-ip-policy

Syntax  
transit-ip-policy ip-policy-id [create]
no transit-ip-policy ip-policy-id

Context  
config>application-assurance>group>policy

Description  
This command defines a transit AA subscriber IP policy. 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 deletes the policy from the configuration. All associations must be removed in order to delete a policy.

Default  
no transit-ip-policy

Parameters  
ip-policy-id  —  An integer that identifies a transit IP profile entry.

Values  
1 — 65535

create  —  Keyword used to create the entry.
def-app-profile

Syntax  def-app-profile  app-profile-name
       no  def-app-profile

Context  config>app-assure>group>policy>transit-ip-policy

Description  This command defines a default app-profile to be associated to dynamically created transit aa-subs
created using this profile, when no app-profile is explicitly assigned.
The no form of the command removes the default app-profile from the policy.

Parameters  app-profile-name — Specifies the name of the application profile up to 32 characters in length.

dhcp

Syntax  dhcp

Context  config>app-assure>group>policy>transit-ip-policy

Description  This command enables dynamic DHCP-based management of transit aa-subs for the transit-ip-policy.
This is mutually exclusive to other types management of transit subs for a given transit-ip-policy.

radius

Syntax  radius

Context  config>app-assure>group>policy>transit-ip-policy

Description  This command enables dynamic radius based management of transit aa-subs for the transit-ip-policy.
This is mutually exclusive to other types management of transit subs for a given transit-ip-policy.

authentication-policy

Syntax  authentication-policy  name
       no  authentication-policy

Context  config>app-assure>group>policy>transit-ip-policy>radius

Description  This command configures the RADIUS authentication-policy for the IP transit policy.

static-aa-sub

Syntax  static-aa-sub  transit-aasub-name
       static-aa-sub  transit-aasub-name app-profile  app-profile-name [create]
       no  static-aa-sub transit-aasub-name

Context  config>app-assure>group>policy>transit-ip-policy
This command configures static transit aa-sub with a name and an app-profile. A new transit sub with both a name and an app-profile is configured with the create command. Static transit aa-sub must have an explicitly assigned app-profile. An existing transit sub can optionally be assigned a different app-profile, or this command can be used to enter the static-aa-sub context.

The no form of the command deletes the named static transit aa-sub from the configuration.

**Default**

**Parameters**

- **transit-aasub-name** — Specifies the name of a transit subscriber up to 32 characters in length.
- **app-profile-name** — Specifies the name of an existing application profile up to 32 characters in length.
- **create** — Keyword used to create a new app-profile entry.

This command configures the /32 ip address for a static transit aa-sub. The no form of the command deletes the ip address assigned to the static transit aa-sub from the configuration.

**Default**

**Parameters**

- **ip-address** — Specifies the IP address in a.b.c.d form

This command associates a subscriber identification policy to this SAP. The subscriber identification policy must be defined prior to associating the profile with a SAP in the config>subscribermgmt>sub-ident-policy context.

Subscribers are managed by the system through the use of subscriber identification strings. A subscriber identification string uniquely identifies a subscriber. For static hosts, the subscriber identification string is explicitly defined with each static subscriber host.

For dynamic hosts, the subscriber identification string must be derived from the DHCP ACK message sent to the subscriber host. The default value for the string is the content of Option 82 CIRCUIT-ID and REMOTE-ID fields interpreted as an octet string. As an option, the DHCP ACK message may be processed by a subscriber identification policy which has the capability to parse the message into an alternative ASCII or octet string value.

When multiple hosts on the same port are associated with the same subscriber identification string they are considered to be host members of the same subscriber.

A sub-ident-policy can also be used for identifying dynamic transit subscriber names.
The `no` form of the command removes the default subscriber identification policy from the SAP configuration.

**Default**

```
no sub-ident-policy
```

### transit-prefix-ipv4-entries

**Syntax**

```
transit-prefix-ipv4-entries entries
no transit-prefix-ipv4-entries
```

**Context**

```
config>isa>aa-grp
```

**Description**

This command defines the number of transit-prefix IPv4 entries for an ISA.

The `no` form of the command removes the assignment of entries space from the configuration. All entries must be removed in order to delete the configuration.

**Parameters**

```
entries — Specifies an integer that determines the number of transit-prefix-ipv4 entries.
```

**Values**

```
0 — 16383
```

### transit-prefix-ipv6-entries

**Syntax**

```
transit-prefix-ipv6-entries entries
no transit-prefix-ipv6-entries
```

**Context**

```
config>isa>aa-grp
```

**Description**

This command configures the ISA-AA-group transit prefix IPv6 entry limit.

**Parameters**

```
entries — Specifies the ISA-AA-Group transit prefix IPv6 entry limit.
```

**Values**

```
0 — 16383
```

### transit-prefix-ipv6-remote-entries

**Syntax**

```
transit-prefix-ipv6-remote-entries entries
no transit-prefix-ipv6-remote-entries
```

**Context**

```
config>isa>aa-grp
```

**Description**

This command configures the ISA-AA-group transit prefix IPv6 remote entry limit.

**Parameters**

```
entries — Specifies the ISA-AA-Group transit prefix IPv6 remote entry limit.
```

**Values**

```
0 — 16383
```
transit-prefix-policy

Syntax  transit-prefix-policy prefix-policy-id [create]
       no transit-prefix-policy prefix-policy-id

Context  config>app-assure>group

Description  This command configures the number of transit prefix IPv4 entries to be supported on the ISA.
             The no form of the command removes the prefix policy ID from the configuration.

Parameters  prefix-policy-id — Indicates the transit prefix policy to which this subscriber belongs.
            Values  

create   — Mandatory keyword used when creating transit prefix policy. The create keyword
            requirement can be enabled/disabled in the environment>create context.

entry

Syntax  entry entry-id [create]
        entry entry-id
        no entry entry-id

Context  config>app-assure>group>transit-prefix-policy

Description  This command configures the index to a specific entry of a transit prefix policy.
             The no form of the command removes the entry ID from the transit prefix policy configuration.

Default  none

Parameters  entry-id — Specifies a transit prefix policy entry.
            Values  1 — 4294967295

aa-sub

Syntax  aa-sub transit-aasub-name
        no aa-sub

Context  config>app-assure>group>transit-prefix-policy>entry

Description  This command configures a transit prefix policy entry subscriber.
             The no form of the command removes the transit subscriber name from the transit prefix policy configuration.

Default  none

Parameters  transit-aasub-name — specifies the name of the transit prefix AA subscriber up to 32 characters in length.
match

Syntax
match

Context
config>app-assure>group>transit-prefix-policy>entry

Description
This command enables the context to configure transit prefix policy entry match criteria.

aa-sub-ip

Syntax
aa-sub-ip ip-address[mask]  
no aa-sub-ip

Context
config>app-assure>group>transit-prefix-policy>entry>match

Description
This command configures a transit prefix subscriber ip address prefix.

Parameters

Values

network-ip

Syntax
network-ip ip-address[mask]  
no network-ip

Context
config>app-assure>group>transit-prefix-policy>entry>match

Description
This command configures a transit prefix network ip address prefix.

The no form of the command removes the network IP address/mask from the match criteria.

Parameters

Values

ipv4-address - a.b.c.d[/mask]
mask - [1..32]
ipv6-address - x:x:x:x:x:x/x/prefix-length
x:x:x:x:x:x:d.d.d
x - [0..FFFF]H
d - [0..255]D
prefix-length [1..128]
Group Commands

**static-aa-sub**

**Syntax**
```
static-aa-sub transit-aasub-name
static-aa-sub transit-aasub-name app-profile app-profile-name [create]
no static-aa-sub transit-aasub-name
```

**Context**
```
config>app-assure>group>transit-prefix-policy
```

**Description**
This command configures a static transit prefix subscriber. The `no` form of the command removes the name from the transit prefix policy.

**Parameters**
```
transit-aasub-name — Specifies a transit aasub-name up to 32 characters in length.
```

**static-remote-aa-sub**

**Syntax**
```
static-remote-aa-sub transit-aasub-name
static-remote-aa-sub transit-aasub-name app-profile app-profile-name [create]
no static-remote-aa-sub transit-aasub-name
```

**Context**
```
config>app-assure>group>transit-prefix-policy
```

**Description**
This command configures a static remote transit prefix subscriber. The `no` form of the command removes the name from the transit prefix policy.

**Parameters**
```
transit-aasub-name — Specifies a transit aasub-name up to 32 characters in length.
```

**packet-rate-high-wmark**

**Syntax**
```
packet-rate-high-wmark high-watermark
```

**Context**
```
config>app-assure
```

**Description**
This command configures the packet rate on the ISA-AA when a packet rate alarm will be raised by the agent.

**Default**
```
max = disabled
```

**Parameters**
```
high-watermark — Specifies the high watermark for packet rate alarms. The value must be larger than or equal to the packet-rate-low-wmark value.
```

**Values**
```
1 — 14880952 , max packets/sec
```

**packet-rate-low-wmark**

**Syntax**
```
packet-rate-low-wmark low-watermark
no packet-rate-low-wmark
```

**Context**
```
config>app-assure
```

Page 184 OS Multi-Service ISA Guide
Description
This command configures the packet rate on the ISA-AA when a packet rate alarm will be cleared by the agent.

The no form of the command reverts to the default.

Default
0

Parameters

- **low-watermark** — Specifies the low watermark for packet rate alarms. The value must be lower than or equal to the packet-rate-low-wmark value.
  
  **Values**
  0 — 14880952 packets/sec

wa-shared-high-wmark

**Syntax**
wa-shared-high-wmark percent
no wa-shared-high-wmark

**Context**
config>isa>aa-grp>qos>egress>from-sub
config>isa>aa-grp>qos>egress>to-sub

**Description**
This command configures the high watermark for the weighted average utilization of the shared buffer space in the from-subscriber buffer pool for each ISA. When a buffer pool is not in the overload state and the wa-shared buffer utilization for an ISA crosses above the high watermark value in the ISA from-subscriber buffer pool enters an overload state and an overload notification is raised.

**Default**
100

**Parameters**

- **percent** — Specifies the weighted average shared buffer utilization high watermark
  
  **Values**
  0 — 100

wa-shared-low-wmark

**Syntax**
wa-shared-low-wmark percent
no wa-shared-low-wmark

**Context**
config>isa>aa-grp>qos>egress>from-sub
config>isa>aa-grp>qos>egress>to-sub

**Description**
This command configures the low watermark for the weighted average utilization of the shared buffer space in the from-subscriber buffer pool. When a buffer pool is in an overloaded state and the wa-shared buffer utilization for an ISA drops below low watermark value ISA from-subscriber buffer pool leaves the overload state and a is sent to indicate the overload state has cleared.

**Default**
0

**Parameters**

- **percent** — Specifies the weighted average shared buffer utilization low watermark
  
  **Values**
  0 — 100
Group Commands

**protocol**

**Syntax**  
protocol protocol-name

**Context**  
config>app-assure

**Description**  
This command configures the shutdown of protocols system-wide

**Parameters**  
protocol-name — Specifies a shutable (disable) protocol name.

**shutdown**

**Syntax**  
[no] shutdown

**Context**  
config>app-assure>protocol

**Description**  
This command administratively disables the protocol specified in protocol protocol-name.  
The **no** form of the command enables the protocol.
System Persistence Commands

persistence

Syntax  persistence

Context  config>system

Description  This command enables the context to configure persistence parameters on the system. The persistence feature enables state on information learned through DHCP snooping across reboots to be retained. This information includes data such as the IP address and MAC binding information, lease-length information, and ingress SAP information (required for VPLS snooping to identify the ingress interface).

If persistence is enabled when there are no DHCP relay or snooping commands enabled, it will simply create an empty file.

Default  no persistence

application-assurance

Syntax  application-assurance

Context  config>system>persistence

Description  This command enables the context to configure application assurance persistence parameters.

location

Syntax  location cflash-id

Context  config>system>persistence

Description  This command instructs the system where to write the file. The name of the file is: dhcp-persistence.db. On boot the system scans the file systems looking for dhcp-persistence.db, if it finds it it starts to load it.

In the subscriber management context, the location specifies the flash device on a CPM card where the data for handling subscriber management persistency is stored.

The no form of this command returns the system to the default. If there is a change in file location while persistence is running, a new file will be written on the new flash, and then the old file will be removed.

Default  no location
ISA Commands

**tunnel-group**

**Syntax**
```
tunnel-group tunnel-group-id [create]
no tunnel-group tunnel-group-id
```

**Context**
```
config>isa
```

**Description**
This command enables the context to configure ISA tunnel group parameters.

**backup**

**Syntax**
```
backup mda-id
no backup
```

**Context**
```
config>isa>tunnel-group
```

**Description**
This command specifies the configured role of the ISA-AA MDA as backup.

**primary**

**Syntax**
```
primary mda-id
no primary
```

**Context**
```
config>isa>tunnel-group
```

**Description**
This command specifies the configured role of the ISA-AA MDA as primary.
Application Assurance Group Commands

application-assurance-group

**Syntax**
```
application-assurance-group application-assurance-group-index [create] [aa-sub-scale sub-scale]
no application-assurance-group application-assurance-group-index
```

**Context**
```
config>isa
```

**Description**
This command enables the context to create an application assurance group with the specified system-unique index and enables the context to configure that group's parameters.

The `no` form of the command deletes the specified application assurance group from the system. The group must be shutdown first.

**Default**
one

**Parameters**
- `application-assurance-group-index` — Specifies an integer to identify the AA group
  - **Values** 1
  - `create` — Mandatory keyword used when creating an application assurance group in the ISA context.
    - The `create` keyword requirement can be enabled/disabled in the `environment>create` context.
  - `aa-sub-scale sub-scale` — Specifies the set of scaling limits that are supported with regards to the maximum number of AA subscribers per ISA and the corresponding policies that can be specified.
    - **Values**
      - residential: Scaling limits for residential operation.
      - vpn: Scaling limits for VPNs.
      - mobile-gateway: Scaling limits for operation as a mobile gateway.
    - **Default** residential

backup

**Syntax**
```
[no] backup mda-id
```

**Context**
```
config>isa>aa-grp
```

**Description**
This command assigns an AA ISA configured in the specified slot to this application assurance group. The backup module provides the application assurance group with warm redundancy when the primary module in the group is configured. Primary and backup modules have equal operational status and when both module are coming up, the ones that becomes operational first becomes the active module. A module can serve as a backup for multiple AA ISA cards but only one can fail to it at one time.

On an activity switch from the primary module, configurations are already on the backup MDA but flow state information must be re-learned. Any statistics not yet spooled will be lost. Auto-switching from the backup to primary, once the primary becomes available again, is not supported.
Operator is notified through SNMP events when:
• When the AA service goes down (all modules in the group are down) or comes back up (a module in the group becomes active).
• When AA redundancy fails (one of the modules in the group is down) or recovers (the failed module comes back up).
• When an AA activity switch occurred.

The no form of the command removes the specified module from the application assurance group.

Default no backup

Parameters

**mda-id** — Specifies the card/slot identifying a provisioned module to be used as a backup module.

**Values**

<table>
<thead>
<tr>
<th>slot/mda</th>
<th>mda-id:</th>
</tr>
</thead>
<tbody>
<tr>
<td>slot</td>
<td>1 — up to 10 depending on chassis model</td>
</tr>
<tr>
<td>mda</td>
<td>1 — 2</td>
</tr>
</tbody>
</table>

**divert-fc**

Syntax

```plaintext
[no] divert-fc fc-name
```

Context

```plaintext
config>isa>aa-grp
```

Description

This command selects a forwarding class in the system to be diverted to an application assurance engine for this application assurance group. Only traffic to/from subscribers with application assurance enabled is diverted.

To divert multiple forwarding classes, the command needs to be executed multiple times specifying each forwarding class to be diverted at a time.

The no form of the command stops diverting of the traffic to an application assurance engine for this application assurance group.

Default no divert-fc

Parameters

**fc-name** — Creates a class instance of the forwarding class fc-name.

**Values**

| be, l2, af, l1, h2, ef, h1, nc |

**fail-to-open**

Syntax

```plaintext
[no] fail-to-open
```

Context

```plaintext
config>isa>aa-grp
```

Description

This command configures mode of operation during an operational failure of this application assurance group when no application assurance engines are available to service traffic. When enabled, all traffic that was to be inspected will be dropped. When disabled, all traffic that was to be inspected will be forwarded without any inspection as if the group was not configured at all.

Default no fail-to-open
isa-capacity-cost-high-threshold

Syntax  

isa-capacity-cost-high-threshold threshold

no isa-capacity-cost-high-threshold

Context  

config>isa>aa-grp

Description  

This command configures the ISA-AA capacity cost high threshold. The no form of the command reverts the threshold to the default value.

Default  

4294967295

Parameters  

threshold — Specifies the capacity cost high threshold for the ISA-AA group.

Values  

0 — 4294967295

isa-capacity-cost-low-threshold

Syntax  

isa-capacity-cost-low-threshold threshold

no isa-capacity-cost-low-threshold

Context  

config>isa>aa-grp

Description  

This command configures the ISA-AA capacity cost low threshold. The no form of the command reverts the threshold to the default value.

Default  

0

Parameters  

threshold — Specifies the capacity cost low threshold for the ISA-AA group.

Values  

0 — 4294967295

isa-overload-cut-through

Syntax  

[no] isa-overload-cut-through

Context  

config>isa>aa-grp

Description  

This command configures the ISA group to enable cut-through of traffic if an overload event occurs, triggered when the IOM weighted average queues depth exceeds the wa-shared-high-wmark. In this ISA state, packets are cut-through from application analysis but retain subscriber context with default subscriber policy applied.

The no form of the command disables cut-through processing on overload.

Default  

isa-overload-cut-through

partitions

Syntax  

[no] partitions
Application Assurance Group Commands

**Context**  config>isa>aa-grp

**Description**  This command enables partitions within an ISA-AA group. When enabled, partitions can be created. The **no** form of the command disables partitions within an ISA-AA group.

**Default**  disabled

**primary**

**Syntax**  [no] primary mda-id

**Context**  config>isa>aa-grp

**Description**  This command assigns an AA ISA module configured in the specified slot to this application assurance group. Primary and backup ISAs have equal operational status and when both ISAs are coming up, the one that becomes operational first becomes the active ISA.

On an activity switch from the primary ISA, all configurations are already on the backup ISA but flow state information must be re-learned. Any statistics not yet spooled will be lost. Auto-switching from the backup to primary, once the primary becomes available again, is not supported.

Operator is notified through SNMP events when:

- When AA service goes down (all ISAs in the group are down) or comes back up (an ISA in the group becomes active)
- When AA redundancy fails (one of the ISAs in the group is down) or recovers (the failed MDA comes back up)
- When an AA activity switch occurred.

The **no** form of the command removes the specified ISA from the application assurance group.

**Default**  no primary

**Parameters**  mda-id  —  Specifies the slot/mda identifying a provisioned AA ISA.

**Values**

<table>
<thead>
<tr>
<th>slot/mda</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>slot</td>
<td>1 — up to 10 depending on chassis model</td>
</tr>
<tr>
<td>mda</td>
<td>1 — 2</td>
</tr>
</tbody>
</table>

**qos**

**Syntax**  qos

**Context**  config>isa>aa-grp

**Description**  This command enables the context for Quality of Service configuration for this application assurance group.
performance

Syntax  performance

Context  config>isa>aa-grp>statistics

Description  This command configures the ISA group to enable the aa-performance statistic record. This record contains information on the traffic load and resource consumption for each ISA in the group, to allow tracking of ISA load for long term capacity planning and short term anomalies. The user can configure the accounting policy to be used, and enables the record using the [no]collect-stats command.

egress

Syntax  egress

Context  config>isa>aa-grp>qos

Description  This command enables the context for IOM port-level Quality of Service configuration for this application assurance group in the egress direction (traffic entering an application assurance engine).

from-subscriber

Syntax  from-subscriber

Context  config>isa>aa-grp>qos>egress

Description  This command enables the context for Quality of Service configuration for this application assurance group form-subscriber logical port, traffic entering the system from AA subscribers and entering an application assurance engine.

pool

Syntax  pool [pool-name]

no pool

Context  config>isa>aa-grp>qos>egress>from-subscriber
         config>isa>aa-grp>qos>egress>to-subscriber
         config>isa>aa-grp>qos>ingress

Description  This command enables the context to configure an IOM pool as applicable to the specific application assurance group traffic. The user can configure resv-cbs (as percentage) values and slope-policy similarly to other IOM pool commands.

Default  default

Parameters  pool-name — The name of the pool.

     Values  default
resv-cbs

Syntax
resv-cbs  percent-or-default
no resv-cbs

Context
config>isa>aa-grp>qos>egress>from-subscriber>pool
config>isa>aa-grp>qos>egress>to-subscriber>pool
config>isa>aa-grp>qos>ingress>pool

Description
This command defines the percentage or specifies the sum of the pool buffers that are used as a guideline for CBS calculations for access and network ingress and egress queues. Two actions are accomplished by this command.

- A reference point is established to compare the currently assigned (provisioned) total CBS with the amount the buffer pool considers to be reserved. Based on the percentage of the pool reserved that has been provisioned, the over provisioning factor can be calculated.
- The size of the shared portion of the buffer pool is indirectly established. The shared size is important to the calculation of the instantaneous-shared-buffer-utilization and the average-shared-buffer-utilization variables used in Random Early Detection (RED) per packet slope plotting.

Note that this command does not actually set aside buffers within the buffer pool for CBS reservation. The CBS value per queue only determines the point at which enqueuing packets are subject to a RED slope. Oversubscription of CBS could result in a queue operating within its CBS size and still not able to enqueue a packet due to unavailable buffers. The resv-cbs parameter can be changed at any time.

If the total pool size is 10 MB and the resv-cbs set to 5, the ‘reserved size’ is 500 KB.

The no form of this command restores the default value.

Default
default (30%)

Parameters
percent-or-default — Specifies the pool buffer size percentage.

Values
0 — 100, default

slope-policy

Syntax
slope-policy  name
no slope-policy

Context
config>isa>aa-grp>qos>egress>from-subscriber>pool
config>isa>aa-grp>qos>egress>to-subscriber>pool
config>isa>aa-grp>qos>ingress>pool

Description
This command specifies an existing slope policy which defines high and low priority RED slope parameters and the time average factor. The slope policy is defined in the config>qos>slope-policy context.

queue-policy

Syntax
queue-policy  network-queue-policy-name
no queue-policy

Context config>isa>aa-grp>qos>egress>from-subscriber
config>isa>aa-grp>qos>egress>to-subscriber
config>isa>aa-grp>qos>ingress

Description This command assigns an IOM network queue policy as applicable to specific application assurance group traffic.

Default default

Parameters network-queue-policy-name — The name of the network queue policy defined in the system.

wa-shared-high-wmark

Syntax wa-shared-high-wmark percent
no wa-shared-high-wmark

Context config>isa>aa-grp>qos>egress>from-sub
config>isa>aa-grp>qos>egress>to-sub

Description This command configures the high watermark for the weighted average utilization of the shared buffer space in the from-subscriber buffer pool for each ISA. When a buffer pool is not in the overload state and the wa-shared buffer utilization for an ISA crosses above the high watermark value in the ISA from-subscriber buffer pool enters an overload state and an overload notification is raised.

Default 100

Parameters percent — Specifies the weighted average shared buffer utilization high watermark

Values 0 — 100

wa-shared-low-wmark

Syntax wa-shared-low-wmark percent
no wa-shared-low-wmark

Context config>isa>aa-grp>qos>egress>from-sub
config>isa>aa-grp>qos>egress>to-sub

Description This command configures the low watermark for the weighted average utilization of the shared buffer space in the from-subscriber buffer pool. When a buffer pool is in an overloaded state and the wa-shared buffer utilization for an ISA drops below low watermark value ISA from-subscriber buffer pool leaves the overload state and a is sent to indicate the overload state has cleared.

Default

Parameters percent — Specifies the weighted average shared buffer utilization low watermark

Values 0 — 100
port-scheduler-policy

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

Context  
config>isa>aa-grp>qos>egress>from-subscriber
config>isa>aa-grp>qos>egress>to-subscriber

Description  
This command assigns an existing port scheduler policy as applicable to the specific application assurance group traffic.

Default  
default

Parameters  
port-scheduler-policy-name — specifies the name of an existing port scheduler policy.

to-subscriber

Syntax  
to-subscriber

Context  
config>isa>aa-grp>qos>egress

Description  
This command enables the context for Quality of Service configuration for this application assurance group to-subscriber logical port, traffic destined to AA subscribers and entering an application assurance engine.

ingress

Syntax  
ingress

Context  
config>card>mda>network>ingress

Description  
This command enables the context for MDA-level IOM Quality of Service configuration.
L2TP Network Server (LNS) Commands

Ins-group

Syntax  
Insgroup Ins-group-id [create]
no Insgroup Ins-group-id

Context  config>isa

Description  This command configures an LNS group.

mda

Syntax  
mda mda-id [drain]
no mda mda-id

Context  config>isa>lns-group

Description  This command configures an ISA LNS group MDA.

The no form of the command removes the MDA ID from the LNS group configuration.

Parameters  
mda-id —

Values  
mda-id: slot/mda
slot: 1 — 10
mda: 1, 2

Drain — Prevents new L2TP sessions being associated with the ISA. If an ISA is removed from the
lns-group or if the lns-group be shutdown all associated L2TP sessions will be immediately
terminated (and L2TP CDN messages sent to the L2TP peer). View show commands to
determine which ISA is terminating which session (show router l2tp session).
Network Address Translation (NAT) Commands

nat-group

Syntax  

```text
nat-group nat-group-id [create]
no nat-group nat-group-id
```

Context  

```
config>isa
```

Description  

This command configures an ISA NAT group.

The `no` form of the command removes the ID from the configuration.

Default  

`none`

Parameters  

`nat-group` — Specifies the ISA NAT group ID.

Values  

```
1 — 4
```

active-mda-limit

Syntax  

```text
active-mda-limit number
no active-mda-limit
```

Context  

```
config>isa
```

Description  

This command configures the ISA NAT group maximum number of MDA.

The `no` form of the command removes the number from the configuration.

Default  

`none`

Parameters  

`number` — Specifies the active MDA limit.

Values  

```
1 — 6
```

mda

Syntax  

```text
[no] mda mda-id
```

Context  

```
config>isa>nat-group
```

Description  

This command configures an ISA NAT group MDA.

Parameters  

`mda-id` — Specifies the MDA ID in the `slot/mda` format.

Values  

```
slot: 1 — 10
mda: 1 — 2
```
session-limits

Syntax  session-limits

Context  config>isa>nat-group

Description  This command configures the ISA NAT group session limits.

reserved

Syntax  reserved num-sessions
        no reserved

Context  config>isa>nat-group>session-limits

Description  This command configures the number of sessions per block that will be reserved for prioritized sessions.

Parameters  num-sessions — Specifies the number of sessions reserved for prioritized sessions.

Values  0 — 4194303

watermarks

Syntax  watermarks high percentage low percentage
        no watermarks

Context  config>isa>nat-group>session-limits

Description  This command configures the ISA NAT group watermarks.

Parameters  high percentage — Specifies the high watermark of the number of sessions for each MDA in this NAT ISA group.

Values  2 — 100

Parameters  low percentage — Specifies the low watermark of the number of sessions for each MDA in this NAT ISA group.

Values  1 — 99
Show Commands

application-assurance-group

Syntax  application-assurance-group [aa-group-id [load-balance [unassigned]]]

Context  show>isa

Description  This command displays ISA group information.

Parameters  

  aa-group-id — Specifies the AA ISA group ID.

  load-balance — Specifies load balancing information.

  unassigned — Specifies load balancing unassigned aa-sub information.

Sample Output

A:ALU>show>isa# application-assurance-group 1
===============================================================================
ISA Application-assurance-groups
===============================================================================
ISA-AA Group Index : 1
Description          : Test
Primary ISA-AA       : 2/1 up/active                          (7 subs, 9 saps)
                     : 3/2 up/active                          (6 subs, 8 saps)
Backup ISA-AA        : 1/1 up/standby
Last Active change   : 01/30/2009 20:14:37
Admin State          : Up
Oper State           : Up
Diverted FCs         : be 12
Fail to mode         : fail-to-wire    Partitions : disabled
QoS
Egress from subscriber
  Pool                  : default
  Reserved Cbs         : 50 percent
  Slope Policy         : aa_spoll
  Queue Policy         : aa_nqpolEgr
  Scheduler Policy     : aa_pspPrmSub
Egress to subscriber
  Pool                  : default
  Reserved Cbs         : 50 percent
  Slope Policy         : aa_spoll
  Queue Policy         : aa_nqpolEgr
  Scheduler Policy     : aa_pspToSub
===============================================================================
A:ALU>show>isa#

A:ALA-IPD# show isa application-assurance-group <aa-group-id> load-balance
===============================================================================
ISA Application-assurance-group <aa-group-id>
===============================================================================

OS Multi-Service ISA Guide  Page 201
load-balance status : Complete | Balancing
isa-capacity-cost-threshold : low 40,000
high 50,000

<table>
<thead>
<tr>
<th></th>
<th>capacity-cost</th>
<th>aa-sub count</th>
<th>aa-sub stats entries</th>
<th>spoke-sdp entries</th>
<th>transit-ip entries</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1</td>
<td>6</td>
<td>6</td>
<td>60</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>3/1</td>
<td>5</td>
<td>5</td>
<td>48</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Mda Limit</td>
<td>NA</td>
<td>1024</td>
<td>32768</td>
<td>1024</td>
<td>1024</td>
</tr>
</tbody>
</table>

aa-sub type count for group 2

<table>
<thead>
<tr>
<th></th>
<th>all</th>
<th>esm</th>
<th>sap</th>
<th>spoke-sdp</th>
<th>transit</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1</td>
<td>6</td>
<td>3</td>
<td>3</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>3/1</td>
<td>5</td>
<td>3</td>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Unassigned</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

* A:ALA-IPD#

*A:Dut-C# show isa application-assurance-group 84 load-balance unassigned

ISA Application-assurance-group 84 unassigned

type    SvcId      aa-sub                        App-Profile
esm     2          Sub1                          Cost30
esm     50         Sub2                          Cost31
sap     29         2/1/10:527                    Cost29
sap     30         2/1/10:528                    Cost29
sap     31         2/1/10:529                    Cost29
sap     31         2/1/10:530                    Cost29
sap     31         2/1/10:531                    Cost29
sap     32         2/1/10:546                    Cost29
sap     32         2/1/10:547                    Cost29
sap     33         2/1/10:548                    Cost29
spoke   201        199:10                        Cost27
spoke   202        199:17                        Cost10
spoke   202        199:18                        Cost10
spoke   202        199:19                        Cost10

* A: Dut-C#

**group**

**Syntax**
group aa-group-id [partition-id]

**Context**
show>app-assure

**Description**
This command enables the context to display application-assurance group information.

**Parameters**

- aa-group-id — Specifies an AA ISA group ID.

- partition-id — Specifies a partition within a group.
Values 1 — 65535

### aa-sub

**Syntax**

- `aa-sub esm sub-ident-string [snapshot]`
- `aa-sub sap sap-id`
- `aa-sub spoke-id sdp-id:vc-id [snapshot]`
- `aa-sub transit transit-aasub-name [snapshot]`

**Context**

`show>app-assure>group`

**Description**

This command displays per-subscriber statistics.

**Parameters**

- `esm sub-ident-string` — Specifies an existing subscriber identification string.
- `sap sap-id` — Specifies the physical port identifier portion of the SAP definition. Refer to Appendix A: Common CLI Command Descriptions on page 533 for syntax.
- `spoke-id sdp-id:vc-id` — Specifies the spoke SDP ID and VC ID.
- `snapshot` — Specifies that the statistics retrieved include the sum of the statistics from the previous collection windows, and the statistics for any closed flows since the last collection window.
- `transit transit-aasub-name` — Specifies an existing transit subscriber name string up to 32 characters in length.

**Sample Output**

```bash
*A:Dut-C#  show application-assurance group 1 aa-sub spoke-sdp 1:1 snapshot application count
===============================================================================
Application-Assurance Subscriber 1:1 (spoke-sdp)
Application Statistics (snapshot)
===============================================================================
Application                  Disc Octets          Packets       Flows
-------------------------------------------------------------------------------
Unknown                        0% 0               0             0
-------------------------------------------------------------------------------
*A:Dut-C#

A:ALA-IPD# show application-assurance group 1 aa-sub {esm <sub-ident-string> | sap <sap-id> | spoke-sdp <sdp-id:vc-id> | transit <transit-aasub-name>} summary
===============================================================================
Application-Assurance Subscriber summary (realtime | snapshot)
==============================================================================
AA-Subscriber               : 1:1 (spoke-sdp)
ISA assigned                 : 3/1
App-Profile                  : app_prof_D_4
App-Profile divert           : Yes
Capacity cost                : 1
Traffic                      : Octets   Packets   Flows
```
Admitted from subscriber: 0 0 0
Denied from subscriber: 0 0 0
Active flows from subscriber: 0
Admitted to subscriber: 0 0 0
Denied to subscriber: 0 0 0
Active flows to subscriber: 0
Total flow duration: 0 seconds
Terminated flows: 0
Short Duration flows: 0
Medium Duration flows: 0
Long Duration flows: 0

Top App-Groups
Octets | Packets | Flows
<app-group-name> 100000 | 3000 | 30
<app-group-name> 90000 | 3000 | 30
<app-group-name> 80000 | 3000 | 30

A:ALA-IPD#
show application-assurance group 1 aa-sub transit transit-aasub-name

Application-Assurance Subscriber summary (realtime | snapshot)

AA-Subscriber : <transit-aasub-name>
App-Profile : <app-profile-name>
aa-filter : aa-ip <aa-ip-filter-id> or aa-prefix <aa-prefix-filter-id>
Parent : SAP <sap-id> or Spoke-SDP <id> or N/A
Parent ISA assigned : <Slot/MDA> or <None (fail-to-closed | fail-to-open)> or Unassigned or N/A
Parent app-profile : <app-profile-name> or N/A
Parent divert : Yes or No or N/A
Parent capacity-cost : 2000 or N/A
Traffic
Octets | Packets | Flows
Admitted from subscriber: 0 0 0
Denied from subscriber: 0 0 0
Active flows from subscriber: 0
Admitted to subscriber: 0 0 0
Denied to subscriber: 0 0 0
Active flows to subscriber: 0
Total flow duration: 0 seconds
Terminated flows: 0
Short Duration flows: 0
Medium Duration flows: 0
Long Duration flows: 0

Top App-Groups
Octets | Packets | Flows
<app-group-name> 100000 | 3000 | 30
<app-group-name> 90000 | 3000 | 30
<app-group-name> 80000 | 3000 | 30

A:ALA-IPD#
show application-assurance group 1 aa-sub {esm <sub-ident-string> | sap <sap-id> | spoke-sdp <sdp-id:vc-id> | transit <transit-aasub-name>} count
MINOR: CLI aa-sub esm|sap|transit <name> has too many flows to obtain real-time stats, use aa-sub esm|sap|transit|spoke <sub-name> snapshot
A:ALA-IPD# show application-assurance group 1 aa-sub {esm <sub-ident-string> | sap <sap-id> | spoke-sdp <sdp-id:vc-id> | transit <transit-aasub-name>} snapshot count

Application-Assurance Subscriber esm|sap|spoke-sdp|transit <name>
Application Group, Application and Protocol Statistics (realtime | snapshot)

<table>
<thead>
<tr>
<th>Application Group</th>
<th>Disc Octets</th>
<th>Packets</th>
<th>Flows</th>
</tr>
</thead>
<tbody>
<tr>
<td>Games</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Mail</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Peer to Peer</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Unknown</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Web</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Protocol statistics are not configured in statistics>aa-sub

A:ALA-IPD#

A:ALA-IPD# show application-assurance group 1 aa-sub {esm <sub-ident-string> | sap <sap-id> | spoke-sdp <sdp-id:vc-id> | transit <transit-aasub-name>} application count detail

Application-Assurance Subscriber esm|sap|spoke-sdp|transit <name>
Application Statistics (realtime | snapshot)

<table>
<thead>
<tr>
<th>Subscriber Type</th>
<th>Octets</th>
<th>Packets</th>
<th>Flows</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>SIP:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Admitted from subscriber:</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Denied from subscriber:</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Active flows from subscriber:</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Admitted to subscriber:</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Denied to subscriber:</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Active flows to subscriber:</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Max per min from sub:</td>
<td>1000</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>Max per min to sub:</td>
<td>2000</td>
<td>20</td>
<td></td>
</tr>
<tr>
<td>Total flow duration:</td>
<td>0 seconds</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Terminated flows:</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Short Duration flows:</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Medium Duration flows:</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Long Duration flows:</td>
<td>0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

A:ALA-IPD#

aa-sub-list
Syntax  
```
aa-sub-list [isa mda-id]
aa-sub-list policers-exceeded
aa-sub-list summary
```

Context  
```
show>app-assure>group
```

Description  
This command displays aa-subscriber lists.

Parameters  
isa mda-id — Displays the slot and MDA ID.

Values
- 1 — 10 (depending on chassis model)
- 1, 2

policers-exceeded — Displays the policer resources which are exceeded.

summary — Displays summary information.

Sample Output
```
show application-assurance group 1 aa-sub {esm <sub-ident-string> | sap <sap-id> |
spoke-sdp <sdp-id:vc-id> } summary
```

```
Application-Assurance Subscriber summary (realtime | snapshot)
```

```
AA-Subscriber : <sub-ident-string> or <sap-id> or <sdp-id:vc-id>
ISA assigned : <Slot/MDA> Unassigned
App-Profile : <app-profile-name>
App-Profile divert : Yes or No
capacity-cost : 100 // for sap/spoke-sdp & esm aa-sub)
```

```
Traffic
```

```
Admitted from subscriber: 0 0 0
Denied from subscriber: 0 0 0
Active flows from subscriber:
Admitted to subscriber: 0 0 0
Denied to subscriber: 0 0 0
Active flows to subscriber:
Total flow duration: 0 seconds
Terminated flows: 0
Short Duration flows: 0
Medium Duration flows: 0
Long Duration flows: 0
```

```
Top App-Groups
```

```
<app-group-name> 100000 3000 30
<app-group-name> 90000 3000 30
<app-group-name> 80000 3000 30
```

```
Application Service Options (ASO)
```

```
Characteristic Value Derived from
```
Server Block default
ServiceBw SuperUser app-profile
Teleworker Yes override
VideoBoost Priority override
```

```
Total characteristics : 4
Total derived from aso defaults : 1
```

Total derived from app-profile : 1
Total derived from overrides  : 2

*A:Dut-C# show application-assurance group 224:10559 aa-sub-list

Application-Assurance Subscriber List for Group 224:10559

<table>
<thead>
<tr>
<th>type</th>
<th>aa-sub</th>
<th>ISA</th>
<th>App-Profile</th>
<th>divert</th>
</tr>
</thead>
<tbody>
<tr>
<td>sap</td>
<td>1/1/1:113</td>
<td>3/2</td>
<td>prof_224_10559_1</td>
<td>Yes</td>
</tr>
<tr>
<td>sap</td>
<td>1/1/1:241</td>
<td>3/2</td>
<td>prof_224_10559_1</td>
<td>Yes</td>
</tr>
<tr>
<td>sap</td>
<td>1/1/1:369</td>
<td>3/2</td>
<td>prof_224_10559_1</td>
<td>Yes</td>
</tr>
<tr>
<td>sap</td>
<td>1/1/1:497</td>
<td>3/2</td>
<td>prof_224_10559_1</td>
<td>Yes</td>
</tr>
<tr>
<td>sap</td>
<td>1/1/4:113</td>
<td>3/2</td>
<td>prof_224_10559_2</td>
<td>Yes</td>
</tr>
<tr>
<td>sap</td>
<td>1/1/4:241</td>
<td>3/2</td>
<td>prof_224_10559_2</td>
<td>Yes</td>
</tr>
<tr>
<td>sap</td>
<td>1/1/4:369</td>
<td>3/2</td>
<td>prof_224_10559_2</td>
<td>Yes</td>
</tr>
<tr>
<td>sap</td>
<td>1/1/4:497</td>
<td>3/2</td>
<td>prof_224_10559_2</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Total number of aa-subs found : 8

*A:Dut-C#

*A:Dut-C# show application-assurance group 224:10559 aa-sub-list isa 3/2

Application-Assurance Subscriber List for Group 224:10559, isa 3/2

<table>
<thead>
<tr>
<th>type</th>
<th>aa-sub</th>
<th>ISA</th>
<th>App-Profile</th>
<th>divert</th>
</tr>
</thead>
<tbody>
<tr>
<td>sap</td>
<td>1/1/1:113</td>
<td>3/2</td>
<td>prof_224_10559_1</td>
<td>Yes</td>
</tr>
<tr>
<td>sap</td>
<td>1/1/1:241</td>
<td>3/2</td>
<td>prof_224_10559_1</td>
<td>Yes</td>
</tr>
<tr>
<td>sap</td>
<td>1/1/1:369</td>
<td>3/2</td>
<td>prof_224_10559_1</td>
<td>Yes</td>
</tr>
<tr>
<td>sap</td>
<td>1/1/1:497</td>
<td>3/2</td>
<td>prof_224_10559_1</td>
<td>Yes</td>
</tr>
<tr>
<td>sap</td>
<td>1/1/4:113</td>
<td>3/2</td>
<td>prof_224_10559_2</td>
<td>Yes</td>
</tr>
<tr>
<td>sap</td>
<td>1/1/4:241</td>
<td>3/2</td>
<td>prof_224_10559_2</td>
<td>Yes</td>
</tr>
<tr>
<td>sap</td>
<td>1/1/4:369</td>
<td>3/2</td>
<td>prof_224_10559_2</td>
<td>Yes</td>
</tr>
<tr>
<td>sap</td>
<td>1/1/4:497</td>
<td>3/2</td>
<td>prof_224_10559_2</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Total number of aa-subs found : 8

*A:Dut-C#

A:ALA-IPD# show application-assurance group 2 aa-sub-list [isa <mda-id>]

Application-Assurance Subscriber List for Group 2, isa <slot/mda>

<table>
<thead>
<tr>
<th>type</th>
<th>aa-sub</th>
<th>ISA</th>
<th>App-Profile</th>
<th>divert</th>
</tr>
</thead>
</table>
| group 2:50

<table>
<thead>
<tr>
<th>type</th>
<th>aa-sub</th>
<th>ISA</th>
<th>App-Profile</th>
<th>divert</th>
</tr>
</thead>
<tbody>
<tr>
<td>esm</td>
<td>Bob</td>
<td>3/1</td>
<td>Grp2P50appProf1</td>
<td>Yes</td>
</tr>
<tr>
<td>esm</td>
<td>Fred</td>
<td>1/1</td>
<td>Grp2P50appProf1</td>
<td>Yes</td>
</tr>
<tr>
<td>sap</td>
<td>1/2/9</td>
<td>3/1</td>
<td>Grp2P50appProf1</td>
<td>Yes</td>
</tr>
<tr>
<td>sap</td>
<td>1/2/10</td>
<td>1/1</td>
<td>Grp2P50appProf1</td>
<td>Yes</td>
</tr>
<tr>
<td>spoke-sdp 1:7</td>
<td>1/1</td>
<td>Grp2P50appProf1</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>spoke-sdp 2:101</td>
<td>3/1</td>
<td>Grp2P50appProf1</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>
group 2:32656

<table>
<thead>
<tr>
<th>type</th>
<th>aa-sub</th>
<th>ISA</th>
<th>App-Profile</th>
<th>divert assigned</th>
</tr>
</thead>
<tbody>
<tr>
<td>esm</td>
<td>Alex</td>
<td>1/1</td>
<td>appProf1</td>
<td>Yes</td>
</tr>
<tr>
<td>esm</td>
<td>Subl</td>
<td>3/1</td>
<td>Lite</td>
<td>Yes</td>
</tr>
<tr>
<td>esm</td>
<td>Max</td>
<td>3/1</td>
<td>appProf1</td>
<td>Yes</td>
</tr>
<tr>
<td>esm</td>
<td>tcpr_sub</td>
<td>1/1</td>
<td>appProf2</td>
<td>Yes</td>
</tr>
<tr>
<td>sap</td>
<td>1/2/5</td>
<td>3/1</td>
<td>appProf1</td>
<td>Yes</td>
</tr>
<tr>
<td>sap</td>
<td>1/2/6</td>
<td>1/1</td>
<td>appProf1</td>
<td>Yes</td>
</tr>
<tr>
<td>sap</td>
<td>2/2/4:111</td>
<td>1/1</td>
<td>Power</td>
<td>Yes</td>
</tr>
<tr>
<td>spoke-sdp</td>
<td>1:6</td>
<td>1/1</td>
<td>appProf1</td>
<td>Yes</td>
</tr>
<tr>
<td>spoke-sdp</td>
<td>2:100</td>
<td>3/1</td>
<td>appProf2</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Number of aa-subs found in group 2:50 : 6
Number of aa-subs found in group 2:32656 : 9
Total number of aa-subs found : 15

A:ALA-IPD#

A:ALA-IPD# show application-assurance group 2:32656 aa-sub-list [isa <mda-id>

Application-Assurance Subscriber List for Group 2:32656, isa <slot/mda>

<table>
<thead>
<tr>
<th>type</th>
<th>aa-sub</th>
<th>ISA</th>
<th>App-Profile</th>
<th>divert assigned</th>
</tr>
</thead>
<tbody>
<tr>
<td>esm</td>
<td>Alex</td>
<td>1/1</td>
<td>appProf1</td>
<td>Yes</td>
</tr>
<tr>
<td>esm</td>
<td>Subl</td>
<td>3/1</td>
<td>Lite</td>
<td>Yes</td>
</tr>
<tr>
<td>esm</td>
<td>Max</td>
<td>3/1</td>
<td>appProf1</td>
<td>Yes</td>
</tr>
<tr>
<td>esm</td>
<td>tcpr_sub</td>
<td>1/1</td>
<td>appProf2</td>
<td>Yes</td>
</tr>
<tr>
<td>sap</td>
<td>1/2/5</td>
<td>3/1</td>
<td>appProf1</td>
<td>Yes</td>
</tr>
<tr>
<td>sap</td>
<td>1/2/6</td>
<td>1/1</td>
<td>appProf1</td>
<td>Yes</td>
</tr>
<tr>
<td>sap</td>
<td>2/2/4:111</td>
<td>1/1</td>
<td>Power</td>
<td>Yes</td>
</tr>
<tr>
<td>spoke-sdp</td>
<td>2:100</td>
<td>1/1</td>
<td>appProf8</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Number of aa-subs : 8

A:ALA-IPD#

aa-sub-study

Syntax

```
aa-sub-study esm sub-ident-string [snapshot]
aa-sub-study sap sap-id
aa-sub-study spoke-sdp sdp-id:vc-id [snapshot]
aa-sub-study transit transit-aasub-name [snapshot]
```

Context show>app-assure>group

Description This command display per-subscriber special study statistics.

Parameters

- **esm sub-ident-string** — Specifies an existing subscriber identification string.
- **sap sap-id** — Specifies the physical port identifier portion of the SAP definition. Refer to Appendix A: Common CLI Command Descriptions on page 533 for syntax.
- **spoke-id sdp-id:vc-id** — Specifies the spoke SDP ID and VC ID.
app-group

Syntax  

app-group [app-group-name] count [detail]

Context  

show>app-assure>group>aa-sub
show>app-assure>group

Description  

This command displays per-application-group statistics. System-wide statistics displayed account for all flows completed and the last internal snapshot of the active flows.

Parameters  

app-group-name — Displays information about the specified application group name.

count — Displays the counters for the application group.

detail — Displays detailed information.

Sample Output

A:ALU>show>app-assure>group# app-group count
===============================================================================
App-group Statistics
===============================================================================
Application Group                Disc Octets          Packets       Flows
-------------------------------------------------------------------------------
File Transfer                      0% 0               0             0
Games                              0% 3865532         4952          144
Infrastructure                     0% 174524          1217          1177
Instant Messaging                  0% 2979117         9930          97
Local Content                      0% 10581539        10942         74
Mail                                0% 57940           346           24
MultiMedia                          0% 76911464        79417         198
NNTP                                0% 0               0             0
Peer to Peer                       0% 10903442        13901         485
Premium Partner                    0% 0               0             0
Remote Connectivity                0% 0               0             0
Server                              0% 1097            8             2
Suspct                              72% 1012            11            11
Tunneling                          0% 19872617        33989         204
Unknown                             0% 5243395         27510         2648
Web                                 0% 82135303        91828         2152
-------------------------------------------------------------------------------
A:ALU>show>app-assure>group#

A:ALU>show>app-assure>group# app-group "MultiMedia" count detail
===============================================================================
App-group "MultiMedia" Statistics
===============================================================================
Application Group:
<table>
<thead>
<tr>
<th>Type</th>
<th>Octets</th>
<th>Packets</th>
<th>Flows</th>
</tr>
</thead>
<tbody>
<tr>
<td>MultiMedia:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Admitted from subscriber:</td>
<td>193605</td>
<td>1797</td>
<td>23</td>
</tr>
<tr>
<td>Denied from subscriber:</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Active flows from subscriber:</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Admitted to subscriber:</td>
<td>4835822</td>
<td>3366</td>
<td>23</td>
</tr>
<tr>
<td>Denied to subscriber:</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Active flows to subscriber:</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Total flow duration:</td>
<td>433 seconds</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Terminated flows:</td>
<td>46</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Short Duration flows:</td>
<td>36</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Medium Duration flows:</td>
<td>10</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Long Duration flows:</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Active subscribers:</td>
<td>0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

**Application Assurance Command Descriptions**

application

**Syntax**

```
application [application-name] count [detail]
```  

**Context**

```
show>app-assure>group>aa-sub
show>app-assure>group
show>app-assure>group>aa-sub-study
```  

**Description**

This command displays per-application statistics. The system-wide statistics displayed account for all flows completed and the last internal snapshot of the active flows.

Subscriber statistics are available for special-study subscribers and account for all completed and active flows at the moment of this statistics request.

**Parameters**

- `application-name` — Displays information about the specified application name.
- `count` — Displays counter information.
- `detail` — Displays detailed information.

**Sample Output**

```
A:ALU-ABC>show>app-assure>group# application count

Application Statistics

<table>
<thead>
<tr>
<th>Application</th>
<th>Disc Octets</th>
<th>Packets</th>
<th>Flows</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0% 0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>DHT</td>
<td>0% 96781</td>
<td>627</td>
<td>627</td>
</tr>
<tr>
<td>DNS_Suspect</td>
<td>0% 276</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>FTP</td>
<td>100% 736</td>
<td>8</td>
<td>8</td>
</tr>
</tbody>
</table>
```
A:ALU-ABC>show>app-assure>group#

A:ALU-ABC>show>app-assure>group# application "POP3" count detail
-------------------------------------------------------------------
Application "POP3" Statistics
-------------------------------------------------------------------
            Type                      Octets            Packets         Flows
-------------------------------------------------------------------
POP3:       Admitted from subscriber: 14095             149             10
            Denied from subscriber: 0                 0               0
            Active flows from subscriber:              0
            Admitted to subscriber: 30707             128             10
            Denied to subscriber: 0                 0               0
            Active flows to subscriber:                0
            Total flow duration: 7 seconds
            Terminated flows:                           20
            Active subscribers: 0
A:ALU-ABC>show>app-assure>group#

A:ALU>show>app-assure>group# application "HTTP_Video" count detail
-------------------------------------------------------------------
Application "HTTP_Video" Statistics
-------------------------------------------------------------------
            Type                      Octets            Packets         Flows
-------------------------------------------------------------------
HTTP_Video:  Admitted from subscriber: 369528            5404            36
            Denied from subscriber: 0                 0               0
            Active flows from subscriber:              1
            Admitted to subscriber: 15387734          10629           36
            Denied to subscriber: 0                 0               0
            Active flows to subscriber:                1
            Total flow duration: 463 seconds
            Terminated flows:                           72
            Short Duration flows:                       66
            Medium Duration flows:                      6
            Long Duration flows:                        0
            Active subscribers: 1
-------------------------------------------------------------------
A:ALU>show>app-assure>group#

cflowd

**Syntax**
cflowd

**Context**
show>app-assure>group

**Description**
This command enables the context to display cflowd output.
collector

Syntax  collector [detail]

Context  show>app-assure>group>cflowd

Description  This command enables the context to display cflowd output.

Sample Output

A:ALU-A# show application-assurance group 1 cflowd collector
========================================================================
Application Assurance Cflowd Collectors for group 1
========================================================================
<table>
<thead>
<tr>
<th>Host Address</th>
<th>Port</th>
<th>Version</th>
<th>Admin</th>
<th>Oper</th>
<th>Recs Sent</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.7.7</td>
<td>2055</td>
<td>10</td>
<td>up</td>
<td>up</td>
<td>0</td>
</tr>
<tr>
<td>192.168.7.8</td>
<td>2055</td>
<td>10</td>
<td>up</td>
<td>up</td>
<td>0</td>
</tr>
</tbody>
</table>
========================================================================
Collectors : 2
========================================================================
A:ALU-A#

A:ALU-A# show application-assurance group 1 cflowd collector detail
========================================================================
Application Assurance Cflowd Collectors for group 1
========================================================================
<table>
<thead>
<tr>
<th>Address</th>
<th>Port</th>
<th>Description</th>
<th>Version</th>
<th>Admin State</th>
<th>Oper State</th>
<th>Records Sent</th>
<th>Last Changed</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.7.7</td>
<td>2055</td>
<td>AA Collector 1</td>
<td>10</td>
<td>up</td>
<td>up</td>
<td>0</td>
<td>07/27/2009 13:36:50</td>
</tr>
<tr>
<td>192.168.7.8</td>
<td>2055</td>
<td>AA Collector 2</td>
<td>10</td>
<td>up</td>
<td>up</td>
<td>0</td>
<td>07/27/2009 13:37:10</td>
</tr>
</tbody>
</table>
========================================================================
A:ALU-A#

status

Syntax  status

Context  show>app-assure>group>cflowd

Description  This command display status information.
Sample Output

A:ALU-A# show application-assurance group 1 status [isa 1/2] cflowd
------------------------------------------------------------------------
Application-Assurance Group Cflowd Status
------------------------------------------------------------------------
Cflowd Admin Status : Enabled
Cflowd Oper Status : Enabled
------------------------------------------------------------------------
Volume :
------------------------------------------------------------------------
Sample Rate : <Disabled> or <1 in 500 packets>
Active Flows : 23102
Records Reported : 12345
Records Dropped : 10
Records Per Second : 45
Packets Sent : 1763
Packets Sent Per Sec : 7
------------------------------------------------------------------------
TCP Performance :
------------------------------------------------------------------------
Sample Rate : <Disabled> or <1 in 1000 flows>
Active Flows : 32103
Flows Not Allocated : 33
Records Reported : 12345678
Records Dropped : 100
Records Per Second : 456
Packets Sent : 2057613
Packets Sent Per Sec : 76
------------------------------------------------------------------------
A:ALU-A#

A:ALU-A#show application-assurance group <aa-group-id:[partition]> cflowd status
------------------------------------------------------------------------
Application-Assurance Group:Partition Cflowd Status
------------------------------------------------------------------------
Volume :
------------------------------------------------------------------------
Admin State : Up
Records Reported : 12345
Records Dropped : 10
------------------------------------------------------------------------
TCP Performance :
------------------------------------------------------------------------
Admin State : Up
Flows Not Allocated : 33
Records Reported : 12345678
Records Dropped : 100
------------------------------------------------------------------------
A:ALU-A#
Syntax   count [detail]

Context  show>app-assure>group>aa-sub

Description This command displays per-subscriber app-group application and protocol statistics.

Parameters  detail — Displays detailed information.

Sample Output

A:ALU>show>app-assure>group>aa-sub# count

Application-Assurance Subscriber TestSubscriberName
Application Group, Application and Protocol Statistics

<table>
<thead>
<tr>
<th>Application Group</th>
<th>Disc Octets</th>
<th>Packets</th>
<th>Flows</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database</td>
<td>0% 0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>File Transfer</td>
<td>0% 27243</td>
<td>169</td>
<td>22</td>
</tr>
<tr>
<td>Games</td>
<td>0% 0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Infrastructure</td>
<td>0% 71494</td>
<td>555</td>
<td>515</td>
</tr>
<tr>
<td>Instant Messaging</td>
<td>0% 4947792</td>
<td>25587</td>
<td>411</td>
</tr>
<tr>
<td>Local Content</td>
<td>0% 923</td>
<td>8</td>
<td>2</td>
</tr>
<tr>
<td>Mail</td>
<td>0% 53729</td>
<td>318</td>
<td>22</td>
</tr>
<tr>
<td>Mail Server</td>
<td>0% 0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>MultiMedia</td>
<td>0% 31670667</td>
<td>33087</td>
<td>142</td>
</tr>
<tr>
<td>NNTP</td>
<td>0% 0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Peer to Peer</td>
<td>0% 11096224</td>
<td>16339</td>
<td>2431</td>
</tr>
<tr>
<td>Premium Partner</td>
<td>0% 0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Remote Connectivity</td>
<td>0% 15321</td>
<td>171</td>
<td>2</td>
</tr>
<tr>
<td>Server</td>
<td>0% 0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Suspect</td>
<td>72% 1012</td>
<td>11</td>
<td>11</td>
</tr>
<tr>
<td>Tunneling</td>
<td>0% 19659289</td>
<td>33535</td>
<td>164</td>
</tr>
<tr>
<td>Unknown</td>
<td>0% 1945164</td>
<td>6317</td>
<td>287</td>
</tr>
<tr>
<td>Web</td>
<td>0% 29538078</td>
<td>34873</td>
<td>1022</td>
</tr>
</tbody>
</table>

Application Group: HTTP_Local

<table>
<thead>
<tr>
<th>Disc Octets</th>
<th>Packets</th>
<th>Flows</th>
</tr>
</thead>
<tbody>
<tr>
<td>0% 923</td>
<td>8</td>
<td>2</td>
</tr>
</tbody>
</table>

Protocol

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Disc Octets</th>
<th>Packets</th>
<th>Flows</th>
</tr>
</thead>
<tbody>
<tr>
<td>dns</td>
<td>1.8% 40010</td>
<td>277</td>
<td>277</td>
</tr>
</tbody>
</table>

A:ALU>show>app-assure>group>aa-sub# count detail

Application-Assurance Subscriber TestSubscriberName
Application Group, Application and Protocol Statistics

<table>
<thead>
<tr>
<th>Subscriber Type</th>
<th>Application Group: Instant Messaging</th>
<th>Octets</th>
<th>Packets</th>
<th>Flows</th>
</tr>
</thead>
<tbody>
<tr>
<td>TestSubscriberName</td>
<td></td>
<td>2558576</td>
<td>12720</td>
<td>229</td>
</tr>
<tr>
<td>Admitted from subscriber:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Denied from subscriber:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Active flows from subscriber:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Admitted to subscriber: 2389216 12867 182
Denied to subscriber: 0 0 0
Active flows to subscriber: 0
Total flow duration: 2912 seconds
Terminated flows: 411
Short Duration flows: 387
Medium Duration flows: 22
Long Duration flows: 2

TestSubscriberName Web:
Admitted from subscriber: 2343429 22806 511
Denied from subscriber: 0 0 0
Active flows from subscriber: 1
Admitted to subscriber: 56359191 40528 511
Denied to subscriber: 0 0 0
Active flows to subscriber: 1
Total flow duration: 4783 seconds
Terminated flows: 1020
Short Duration flows: 989
Medium Duration flows: 31
Long Duration flows: 0

<table>
<thead>
<tr>
<th>Subscriber</th>
<th>Application:</th>
<th>Type</th>
<th>Octets</th>
<th>Packets</th>
<th>Flows</th>
</tr>
</thead>
<tbody>
<tr>
<td>TestSubscriberName</td>
<td>HTTP_Local:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Admitted from subscriber: 0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Denied from subscriber: 0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Active flows from subscriber:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Admitted to subscriber: 0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Denied to subscriber: 0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Active flows to subscriber:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total flow duration:</td>
<td>0 seconds</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Terminated flows:</td>
<td></td>
<td></td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Short Duration flows:</td>
<td></td>
<td></td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Medium Duration flows:</td>
<td></td>
<td></td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Long Duration flows:</td>
<td></td>
<td></td>
<td>0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Subscriber</th>
<th>Protocol:</th>
<th>Type</th>
<th>Octets</th>
<th>Packets</th>
<th>Flows</th>
</tr>
</thead>
<tbody>
<tr>
<td>TestSubscriberName</td>
<td>dns:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Admitted from subscriber: 0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Denied from subscriber: 0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Active flows from subscriber:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Admitted to subscriber: 0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Denied to subscriber: 0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Active flows to subscriber:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total flow duration:</td>
<td>0 seconds</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Terminated flows:</td>
<td></td>
<td></td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Short Duration flows:</td>
<td></td>
<td></td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Medium Duration flows:</td>
<td></td>
<td></td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Long Duration flows:</td>
<td></td>
<td></td>
<td>0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Syntax admin

Context show>app-assure>group>policy

Description This command displays the application-assurance policy uncommitted changes.

Sample Output

*A:ALA-48>show>app-assure>group>policy# admin
begin
app-filter
  entry 10 create
  shutdown
  exit
exit
app-qos-policy
  entry 10 create
  shutdown
  exit
exit
commit
*A:ALA-48>show>app-assure>group>policy#

app-filter

Syntax app-filter [entry-id]

Context show>app-assure>group>policy

Description This command displays application-assurance policy filter information.

Parameters entry-id — Specifies an existing application filter entry.

Values 1 — 65535

app-group

Syntax app-group [app-group-name]

Context show>app-assure>group>policy

Description This command displays application-assurance policy application group information.

app-profile

Syntax app-profile [app-prof-name]

app-profile app-prof-name associations

Context show>app-assure>group>policy

Description This command displays application-assurance policy application profile information.
Parameters

- **app-prof-name** — Specifies an existing application profile name.
- **associations** — Displays subscriber management associations.

### app-qos-policy

**Syntax**

```
app-qos-policy [entry-id]
```

**Context**

```
show>app-assure>group>policy
```

**Description**

This command displays application-assurance policy application QoS policy information.

**Parameters**

- **entry-id** — Specifies an existing application QoS policy entry id.
  
  **Values**
  
  1 — 65535

### app-service-option

**Syntax**

```
app-service-option [characteristic-name]
```

**Context**

```
show>app-assure>group>policy
```

**Description**

This command displays application-assurance policy application service option information.

### application

**Syntax**

```
application [app-name]
```

**Context**

```
show>app-assure>group>policy
```

**Description**

This command displays application-assurance policy application information.

### custom-protocol

**Syntax**

```
custom-protocol
```

**Context**

```
show>app-assure>group>policy
```

**Description**

This command displays application-assurance policy custom protocol information.

### summary

**Syntax**

```
summary
```

**Context**

```
show>app-assure>group>policy
```

**Description**

This command displays application-assurance policy summary information.
policers

Syntax policers

Context show>app-assure>group>policy>aa-sub

Description This command displays policer configuration information.

Sample Output

A:cpm-a>show>app-assure>group>aa-sub# policers

===============================================================================
Application-Assurance Subscriber Policer Summary
===============================================================================
AA-Subscriber : Alex (esm)
Type: single-bucket-bandwidth Direction: subscriber-to-network
AQP Policer Resources Exceeded?
-------------------------------------------------------------------------------
61  SuspectUp_policer              N
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
Type: single-bucket-bandwidth Direction: network-to-subscriber
AQP Policer Resources Exceeded?
-------------------------------------------------------------------------------
62  SuspectDown_policer             N
-------------------------------------------------------------------------------

Policer usage counts:
single-bucket-bandwidth
subscriber-to-network  1     out of    32
network-to-subscriber  1     out of    32
dual-bucket-bandwidth
subscriber-to-network  0     out of     1
network-to-subscriber  0     out of     1
flow-count-limit       0     out of     8
flow-rate-limit        0     out of     8
===============================================================================
A:cpm-a>show>app-assure>group>aa-sub#

summary

Syntax summary

Context show>app-assure>group>policy

Description This command displays application-assurance policy summary information.
protocol

Syntax

`protocol [protocol-name] count [detail]`

Context

`show>app-assure>group>aa-sub`
`show>app-assure>group`

Description

This command displays per-protocol statistics. The system-wide statistics displayed account for all flows completed and the last internal snapshot of the active flows.

Subscriber statistics are available for special study subscribers and account for all completed and active flows at the moment of this statistics request.

Parameters

- `protocol-name` — Displays information about the specified protocol name.
- `count` — Displays protocol counters.
- `detail` — Displays detailed information.

Sample Output

A:ALU>show>app-assure>group# protocol count
===============================================================================
Protocol Statistics
===============================================================================
<table>
<thead>
<tr>
<th>Protocol</th>
<th>Disc Octets</th>
<th>Packets</th>
<th>Flows</th>
</tr>
</thead>
<tbody>
<tr>
<td>aim_oscar</td>
<td>0% 0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>aim_oscar_file_xfer</td>
<td>0% 0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>aim_oscar_video_voice</td>
<td>0% 0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>aim_toc</td>
<td>0% 0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>bittorrent</td>
<td>0% 0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
...                      |

A:ALU>show>app-assure>group# protocol "http_audio" count detail
===============================================================================
Protocol "http_audio" Statistics
===============================================================================
<table>
<thead>
<tr>
<th>Type</th>
<th>Octets</th>
<th>Packets</th>
<th>Flows</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admitted from subscriber:</td>
<td>14958</td>
<td>201</td>
<td>2</td>
</tr>
<tr>
<td>Denied from subscriber:</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Active flows from subscriber:</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Admitted to subscriber:</td>
<td>587590</td>
<td>396</td>
<td>2</td>
</tr>
<tr>
<td>Denied to subscriber:</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Active flows to subscriber:</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Total flow duration:</td>
<td>21 seconds</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Terminated flows:</td>
<td>4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Short Duration flows:</td>
<td>4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Medium Duration flows:</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Long Duration flows:</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Active subscribers:</td>
<td>1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

A:ALU>show>app-assure>group#
summary

Syntax summary
Context show>app-assure>group>aa-sub
Description This command displays a summary of statistics for a specific aa-sub.

Sample Output

A:ALU>show>app-assure>group>aa-sub# summary
===============================================================================
Application-Assurance Subscriber Summary
===============================================================================
AA-Subscriber       : TestSubscriberName
ISA assigned        : 3/2
App-Profile         : Power_Profile
App-Profile divert  : Yes
-------------------------------------------------------------------------------
Traffic                   Octets            Packets         Flows
-------------------------------------------------------------------------------
Admitted from subscriber: 7092548           52935           2843
Denied from subscriber:   51160             617             374
Active flows from subscriber: 12
Admitted to subscriber:   73705675          73538           1453
Denied to subscriber:     0                 0               0
Active flows to subscriber: 12
Total flow duration:      12750 seconds
Terminated flows:                                            4646
Short Duration flows:                                         4516
Medium Duration flows:                                        130
Long Duration flows:                                          0
-------------------------------------------------------------------------------
Top App-Groups                   Octets            Packets         Flows
-------------------------------------------------------------------------------
MultiMedia                       29060053          29961           138
Tunneling                        19659289          33535           164
Web                               14856331          19829           932
===============================================================================
A:ALU>show>app-assure>group>aa-sub#

status

Syntax status [isa mda-id] cflowd
status [isa mda-id]
status [isa mda-id] detail
status [isa mda-id] cpu [sample-period seconds]
status (isa mda-id) qos count
status (isa mda-id) qos pools
Context show>app-assure>group
Description This command displays system statistics.
Parameters

**isa** — Displays information about the specified AA ISA.

**cflowd** — Displays cflowd status information.

**detail** — Displays detailed status information.

**cpu** [**sample-period seconds**] — Displays cpu utilization info about the specified AA ISA. The **isa mda-id** must be specified. The sample period can be specified within a range of 1-5 seconds (default 1s).

**Values**

1 — 5

**qos count** — Displays information about queue statistics. The **isa mda-id** must be specified.

**qos pools** — Displays information about pool utilization. The **isa mda-id** must be specified.

Sample Output

```
A:ALU>show>app-assure>group# status
===============================================================================
Application-assurance Status
===============================================================================
Last time change affecting status: 01/30/2009 20:14:37
Active Subs                      : 1
-------------------------------------------------------------------------------
Packets              Octets
-------------------------------------------------------------------------------
Diverted traffic       : 58783                46140537
Diverted discards      : 4                    0
Entered ISA-AAs        : 58784                46140614
Discarded in ISA-AAs   : 60                   4620
Exited ISA-AAs         : 58724                46135994
Returned discards      : 0                    0
Returned traffic       : 58724                46135994
===============================================================================
A:ALU>show>app-assure>group#

A:ALU>show>app-assure>group# status detail
===============================================================================
Application-assurance Status
===============================================================================
Last time change affecting status: 01/30/2009 20:14:37
Number of Active ISAs            : 2
Flows                            : 2364
Active Flows                     : 41
Flow Setup Rate                  : 2 per second
Traffic Rate                     : 1 Mbps
AA-Subs Downloaded               : 30
Active Subs                      : 1
-------------------------------------------------------------------------------
Packets              Octets
-------------------------------------------------------------------------------
Diverted traffic       : 60744                47206604
Diverted discards      : 4                    0
Congestion             : 0                    0
Errors                 : 4                    N/A
Entered ISA-AAs        : 60745                47206968
Buffered in ISA-AAs    : 0                    0
Discarded in ISA-AAs   : 164                  12759
```

OS Multi-Service ISA Guide
Application Assurance Command Descriptions

Policy             : 164                  12759
Congestion         : 0                    0
Errors             : 0                    0
Errors (policy bypass) : 1                    60
Exited ISA-AAs         : 60581                47194209
Returned discards      : 0                    0
Congestion         : 0                    0
Errors             : 0                    N/A
Returned traffic       : 60580                47193845

A:ALU>show>app-assure>group#

A:ALU>show>app-assure>group# status isa 3/2 qos count

Application-assurance Queue Statistics for ISA-AA Group: 1, isa 3/2

Egress From-Subscriber
Queue 1 Packets Octets
In Profile forwarded : 0 0
In Profile dropped : 0 0
Out Profile forwarded : 28940 3767233
Out Profile dropped : 0 0
Queue 2 Packets Octets
In Profile forwarded : 0 0
In Profile dropped : 0 0
Out Profile forwarded : 0 0
Out Profile dropped : 0 0

Egress To-Subscriber
Queue 1 Packets Octets
In Profile forwarded : 0 0
In Profile dropped : 0 0
Out Profile forwarded : 44499 53066848
Out Profile dropped : 0 0
Queue 2 Packets Octets
In Profile forwarded : 0 0
In Profile dropped : 0 0
Out Profile forwarded : 0 0
Out Profile dropped : 0 0

Ingress From-Subscriber
Queue 1 Packets Octets
In Profile forwarded : 25548 3361023
In Profile dropped : 0 0
Out Profile forwarded : 1 60
Out Profile dropped : 0 0
Queue 2 Packets Octets
In Profile forwarded : 2921 365606
In Profile dropped : 0 0
Out Profile forwarded : 0 0
Out Profile dropped : 0 0
Queue 9 Packets Octets
In Profile forwarded : 0 0
In Profile dropped : 0 0
Out Profile forwarded : 0 0
Out Profile dropped : 0    0
Queue 10    Packets     Octets
In Profile forwarded : 0    0
In Profile dropped : 0    0
Out Profile forwarded : 0    0
Out Profile dropped : 0    0

Ingress To-Subscriber
Queue 1    Packets     Octets
In Profile forwarded : 39541    46899769
In Profile dropped : 0    0
Out Profile forwarded : 0    0
Out Profile dropped : 0    0
Queue 2    Packets     Octets
In Profile forwarded : 5050    6291204
In Profile dropped : 0    0
Out Profile forwarded : 0    0
Out Profile dropped : 0    0
Queue 9    Packets     Octets
In Profile forwarded : 0    0
In Profile dropped : 0    0
Out Profile forwarded : 0    0
Out Profile dropped : 0    0
Queue 10    Packets     Octets
In Profile forwarded : 0    0
In Profile dropped : 0    0
Out Profile forwarded : 0    0
Out Profile dropped : 0    0

===============================================================================
A:ALU>show>app-assure>group#
A:ALU>show>app-assure>group# status isa 3/2 qos pools
===============================================================================
Pool Information
===============================================================================
MDA                  : 3/2
Application          : Net-Ing           Pool Name          : default
Resv CBS             : 50%
-------------------------------------------------------------------------------
Utilization                   State       Start-Avg    Max-Avg    Max-Prob
-------------------------------------------------------------------------------
High-Slope                    Up                70%        90%         80%
Low-Slope                     Up                50%        75%         80%
Time Avg Factor      : 7
Pool Total           : 40960 KB
Pool Shared          : 20480 KB          Pool Resv          : 20480 KB
High Slope Start Avg : 12288 KB          High slope Max Avg : 16384 KB
Low Slope Start Avg  : 10240 KB          Low slope Max Avg  : 14336 KB
Pool Total In Use    : 0 KB
Pool Shared In Use   : 0 KB              Pool Resv In Use   : 0 KB
WA Shared In Use     : 0 KB
Hi-Slope Drop Prob   : 0                 Lo-Slope Drop Prob : 0
-------------------------------------------------------------------------------
FC-Maps                         Dest     MBS         Depth  A.CIR     A.PIR
Q-Grp                          Q-1d     CBS                O.CIR     O.PIR
-------------------------------------------------------------------------------
be af l1 h2 ef h1 nc 5/* 20480 0 8000000 20000000
  1  1280 8000000 Max
be af l1 h2 ef h1 nc 4/* 20480 0 8000000 20000000
  1  1280 8000000 Max
be af l1 h2 ef h1 nc 3/1 20480 0 8000000 20000000
  1  1280 8000000 Max
be af l1 h2 ef h1 nc 2/1 20480 0 8000000 20000000
  1  1280 8000000 Max
be af l1 h2 ef h1 nc 1/1 20480 0 8000000 20000000
  1  1280 8000000 Max
be af l1 h2 ef h1 nc 5/* 20480 0 8000000 20000000
  1  1280 8000000 Max
be af l1 h2 ef h1 nc 4/* 20480 0 8000000 20000000
  1  1280 8000000 Max
...

Pool Information
===============================================================================
Port : 3/2/fm-sub
Application : Net-Egr Pool Name : default
Resv CBS : 50%

Queue-Groups

Utilization State Start-Avg Max-Avg Max-Prob
---------------------------
High-Slope Up 70% 90% 80%
Low-Slope Up 50% 75% 80%

Time Avg Factor : 7
Pool Total : 12288 KB
Pool Shared : 6144 KB Pool Resv : 6144 KB

High Slope Start Avg : 4096 KB High slope Max Avg : 5120 KB
Low Slope Start Avg : 3072 KB Low slope Max Avg : 4096 KB

Pool Total In Use : 0 KB
Pool Shared In Use : 0 KB Pool Resv In Use : 0 KB
WA Shared In Use : 0 KB
Hi-Slope Drop Prob : 0 Lo-Slope Drop Prob : 0

FC-Maps

<table>
<thead>
<tr>
<th>Q-Grp</th>
<th>Q-Id</th>
<th>MBS</th>
<th>Depth</th>
<th>A.CIR</th>
<th>A.PIR</th>
</tr>
</thead>
<tbody>
<tr>
<td>be af l1 h2 ef h1 nc</td>
<td>3/2/fm-*</td>
<td>8192</td>
<td>0</td>
<td>4000000</td>
<td>10000000</td>
</tr>
<tr>
<td>1</td>
<td>3/2/fm-*</td>
<td>1280</td>
<td>0</td>
<td>4000000</td>
<td>10000000</td>
</tr>
<tr>
<td>2</td>
<td>3/2/fm-*</td>
<td>6144</td>
<td>0</td>
<td>6000000</td>
<td>10000000</td>
</tr>
<tr>
<td>3/2/fm-*</td>
<td>5120</td>
<td>0</td>
<td>5000000</td>
<td>5000000</td>
<td></td>
</tr>
</tbody>
</table>

Pool Information
===============================================================================
Port : 3/2/to-sub
Application : Net-Egr Pool Name : default
Resv CBS : 50%

Queue-Groups

Utilization State Start-Avg Max-Avg Max-Prob
---------------------------
High-Slope Up 70% 90% 80%
Low-Slope                     Up                50%        75%         80%
Time Avg Factor      : 7
Pool Total            : 24576 KB
Pool Shared           : 12288 KB       Pool Resv : 12288 KB
High Slope Start Avg : 8192 KB       High slope Max Avg : 10240 KB
Low Slope Start Avg  : 6144 KB       Low slope Max Avg : 8192 KB
Pool Total In Use     : 0 KB
Pool Shared In Use    : 0 KB
WA Shared In Use      : 0 KB
Hi-Slope Drop Prob    : 0
Lo-Slope Drop Prob    : 0
-------------------------------------------------------------------------------
<table>
<thead>
<tr>
<th>FC-Maps</th>
<th>ID</th>
<th>MBS</th>
<th>Depth</th>
<th>A.CIR</th>
<th>A.PIR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q-Grp</td>
<td>Q-Id</td>
<td>CBS</td>
<td>O.CIR</td>
<td>O.PIR</td>
<td></td>
</tr>
<tr>
<td>----------</td>
<td>----------</td>
<td>-----</td>
<td>-------</td>
<td>-------</td>
<td>-------</td>
</tr>
<tr>
<td>be af l1 h2 ef h1 nc</td>
<td>3/2/to-*</td>
<td>16384</td>
<td>0</td>
<td>4000000</td>
<td>10000000</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>10240</td>
<td>0</td>
<td>4000000</td>
<td>Max</td>
</tr>
<tr>
<td>12</td>
<td>3/2/to-*</td>
<td>12288</td>
<td>0</td>
<td>6000000</td>
<td>10000000</td>
</tr>
<tr>
<td>2</td>
<td>7168</td>
<td>6000000</td>
<td>Max</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
-------------------------------------------------------------------------------

A:ALU>show>app-assure>group#

partition

**Syntax**

```
partition summary
```

**Context**

```
show>app-assure>group
```

**Description**

This command displays partition information.

**Parameters**

- `summary` — Displays partition summary information.

policer

**Syntax**

```
policer [policer-name]
policer summary
```

**Context**

```
show>app-assure>group
```

**Description**

This command displays application-assurance policer information.

**Parameters**

- `policer-name` — Displays information about the specified policer.
- `summary` — Displays summarized information about policers on this node.

**Sample Output**

```
A:ALU-ABC>show>app-assure>group# policer
    policer "100k_policer" type single-bucket-bandwidth granularity subscriber
    create
        rate 100
```
mbs 10
exit
policer "200FlowsDown_Policer" type flow-count-limit granularity subscriber create
flow-count 200
exit
policer "ServerDown_policer" type single-bucket-bandwidth granularity subscriber create
action priority-mark
rate 500
mbs 50
exit
policer "ServerUp_policer" type single-bucket-bandwidth granularity subscriber create
action priority-mark
rate 500
mbs 50
exit
...
policer "SuspectUp_policer" type single-bucket-bandwidth granularity subscriber create
rate 100
mbs 10
exit
policer "Video_channel_policer" type single-bucket-bandwidth granularity subscriber create
action priority-mark
rate 2000
mbs 200
exit

Number of policers : 26
A:ALU-ABC>show>app-assure>group#

A:ALU-ABC>show>app-assure>group# policer "P2PAggrBwDown"
  policer "P2PAggrBwDown" type single-bucket-bandwidth granularity system
  create
  rate 1000000
  mbs 100000
  exit
A:ALU-ABC>show>app-assure>group#

A:ALU-ABC>show>app-assure>group# policer summary
  System-level single-bucket-bandwidth policers : 3 out of 64
  System-level flow-count-limit policers : 1 out of 64
  System-level flow-rate-limit policers : 1 out of 64
  Subscriber-level single-bucket-bandwidth to-subscriber policers
    Base non-subscriber-specific entries : 1 out of 32
    Worst case : 3 out of 32
      occurs with app-profile "Super"
  Subscriber-level single-bucket-bandwidth from-subscriber policers
    Base non-subscriber-specific entries : 1 out of 32
    Worst case : 2 out of 32
      occurs with app-profile "Lite"
  Subscriber-level flow-count-limit policers
    Base non-subscriber-specific entries : 0 out of 8
    Worst case : 2 out of 8
      occurs with app-profile "Lite"
  Subscriber-level flow-rate-limit policers
policy

Syntax    policy
Context   show>app-assure>group
Description This command enables the context to display application-assurance policy configuration information.

http-error-redirect

Syntax    http-error-redirect
Context   show>app-assure
Description This command enables the context to display http-error-redirect static definitions.

Sample Output

*A:cses-E11>show application-assurance group 1 http-error-redirect <redirect-name>
===============================================================================
Application-Assurance Group 1 http-error-redirect <redirect-name>
===============================================================================
description    : <description-string>
template       : <template-id>
                 : text description of template
participant-id : <string>
http-host      : <http-host-name>
error code     : <http-error-code>  custom-msg-size : <msg size>
admin status   : Up

Grp:Part  Error     Redirects    Redirects Not Sent
          Code      Sent         > Custom     Out ofFile    Error
          size  Resourcetype
-------------------------------------------------------------------------------
1:1       404     1250          52            10           10
1:56789   404     2000          952           81           01
-------------------------------------------------------------------------------
Total               3250      1004          91           1     1
----------------------------------------------------------------
================================================================

error-codes
Application Assurance Command Descriptions

error-codes

Syntax  error-codes
Context  show>app-assure>http-redirect#
Description  This command displays http-error-redirect error-codes.

Sample Output

*A:cses-E11>show application-assurance http-error-redirect error-codes
===============================================================================
Application-Assurance http-error-redirect error-codes
===============================================================================
<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
<th>Default custom-msg-size</th>
</tr>
</thead>
<tbody>
<tr>
<td>404</td>
<td>Not found</td>
<td>1024</td>
</tr>
</tbody>
</table>
===============================================================================
*A:cses-E11>

template

Syntax  template
Context  show>app-assure>http-redirect#
Description  This command displays http-error-redirect template information.

Sample Output

*A:cses-E11>show application-assurance http-error-redirect template
===============================================================================
Application-Assurance http-error-redirect templates
===============================================================================
<table>
<thead>
<tr>
<th>ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Template suited for Barefruit landing server. Includes participant-id.</td>
</tr>
<tr>
<td>2</td>
<td>Template suited for Xerocole landing server.</td>
</tr>
</tbody>
</table>
===============================================================================
*A:cses-E11>

protocol

Syntax  protocol [protocol-name]
protocol [protocol-name] detail
Context  show>app-assure
Description  This command displays application-assurance policy protocols loaded from the isa-aa.tim file.
Parameters  protocol-name — Displays all protocols from the isa-aa.tim file.
            detail — Displays detailed information about the specified protocol name.
### Sample Output

**A:ALU-ABC>show>app-assure# protocol**

---

**Application Assurance Protocols**

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>aim_oscar</td>
<td>America Online Oscar Instant Messaging.</td>
</tr>
<tr>
<td>aim_oscar_file_xfer</td>
<td>America Online Oscar File Transfer.</td>
</tr>
<tr>
<td>aim_oscar_video_voice</td>
<td>America Online Oscar Video and Voice Traffic.</td>
</tr>
<tr>
<td>aim_toc</td>
<td>America Online Talk to Oscar Instant Messaging.</td>
</tr>
<tr>
<td>bittorrent</td>
<td>BitTorrent peer to peer protocol.</td>
</tr>
</tbody>
</table>

...  

**A:ALU-ABC>show>app-assure#**

**A:ALU-ABC>show>app-assure# protocol tftp**

---

**Application Assurance Protocols**

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Description</th>
</tr>
</thead>
</table>

---

**A:ALU-ABC>show>app-assure#**

### version

**Syntax**

```
version
```

**Context**

```
show>app-assure
```

**Description**

This command displays the versions of the isa-aa.tim used by the CPM and the AA ISAs.

### Sample Output

**A:ALU>show>app-assure# version**

---

**Versions of isa-aa.tim in use**

<table>
<thead>
<tr>
<th>Component</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPM</td>
<td>TiMOS-M-7.0.R4</td>
</tr>
<tr>
<td>1/1</td>
<td>TiMOS-I-7.0.R1</td>
</tr>
<tr>
<td>2/1</td>
<td>TiMOS-I-7.0.R1</td>
</tr>
<tr>
<td>3/2</td>
<td>TiMOS-I-7.0.R1</td>
</tr>
</tbody>
</table>

---

**A:ALU>show>app-assure#**
aa-sub-using

Syntax

- **aa-sub-using**
- **aa-sub-using app-profile app-profile-name**

Context

- show>service

Description

This command displays application subscriber information.

Parameters

- **app-profile-name** — Specifies the application profile name.

---

app-profile

Syntax

- **app-profile app-profile-name**

Context

- show>service>sap-using

Description

This command displays information about SAPs using the specified application profile.

Parameters

- **app-profile-name** — Specifies an existing application profile name created in the `config>app-assure>group>policy` context.

Sample Output

```
*A:ALA-48# show service sap-using app-profile test
===============================================================================
Service Access Point Using Application Profile 'test'
===============================================================================
<table>
<thead>
<tr>
<th>PortId</th>
<th>SvcId</th>
<th>Ing.</th>
<th>Ing.</th>
<th>Egr.</th>
<th>Egr.</th>
<th>Adm</th>
<th>Opr</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1/18:0</td>
<td>89</td>
<td>none</td>
<td>1</td>
<td>none</td>
<td>1</td>
<td>Up</td>
<td>Down</td>
</tr>
</tbody>
</table>
Number of SAPs : 1
```

---

sdp-using

Syntax

- **sdp-using [sdp-id[:vc-id]]|far-end ip-address]**
- **sdp-using app-profile app-profile-name**

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.

**app-profile** *app-profile-name* — Specifies the application profile name.
Tools Commands

group

Syntax  
\texttt{group aa-group-id[:partition-id]}

Context  
\texttt{tools>dump>application-assurance}

Description  
This command dumps application-assurance information within a group/partition.

Parameters

<table>
<thead>
<tr>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>aa-group-id:</td>
</tr>
<tr>
<td>aa-group-id 1 — 255</td>
</tr>
<tr>
<td>partition-id:</td>
</tr>
<tr>
<td>partition-id 1 — 65535</td>
</tr>
</tbody>
</table>

aa-sub-search

Syntax  
\texttt{aa-sub-search search-type granularity [direction direction] [max-count max-count]}

Context  
\texttt{tools>dump>app-assure>group}

Description  
This command displays the top aa-subscribers per ISA by byte, packet or flow counts.

Parameters

<table>
<thead>
<tr>
<th>search-type — specifies the type of search.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Values top</td>
</tr>
<tr>
<td>Default top</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>granularity — specifies the granularity of the search.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Values bytes, packets, flows</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>direction direction — specifies either the subscriber to network or the network to subscriber direction or both.</th>
</tr>
</thead>
<tbody>
<tr>
<td>from-sub, to-sub, both</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>max-count max-count — Specifies the maximum flows to display.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Values 1 — 100</td>
</tr>
</tbody>
</table>

congestion-search

Syntax  
\texttt{congestion-search search-type search-type [isa mda-id]}

Context  
\texttt{tools>dump>application-assurance>group}

Description  
This command dumps application-assurance severe congestion information.

Parameters

<table>
<thead>
<tr>
<th>search-type — Specifies the search type of display.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Values aa-sub, flow</td>
</tr>
</tbody>
</table>
**isa mda-id** — Specifies the associated MDA to dump.

<table>
<thead>
<tr>
<th>Values</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>slot/mda</td>
<td></td>
</tr>
<tr>
<td>slot</td>
<td>1 — 10</td>
</tr>
<tr>
<td>mda</td>
<td>1 — 2</td>
</tr>
</tbody>
</table>

### flow-record-search

**Syntax**

```
flow-record-search aa-sub { esm sub-ident-string | sap sap-id | spoke-sdp sdp-id:vc-id | transit transit-aasub-name} [protocol protocol-name] [application app-name] [app-group app-group-name] [flow-status flow-status] [start-flowid start-flowid] [max-count max-count] [search-type search-type] [url file-url]
```

**Context**

tools>dump>app-assure>group

**Description**

This command dumps application-assurance flow-records matching the specified criteria for a specific AA subscriber.

**Parameters**

- **esm sub-ident-string** — Displays flows for the specified subscriber.
- **sap sap-id** — Displays flows for the specified SAP.
- **spoke-sdp sdp-id:vc-id** — Displays flows for the specified spoke SDP.
- **protocol protocol-name** — Displays flows for the specified protocol.
- **application app-name** — Displays flows for the specified application name.
- **app-group app-group-name** — Displays flows for the specified application group,
- **flow-status flow-status** — Displays only flows that are active or closed.
  
<table>
<thead>
<tr>
<th>Values</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>active, closed</td>
<td></td>
</tr>
</tbody>
</table>
- **start-flowid start-flowid** — Specifies the starting flow ID.
  
<table>
<thead>
<tr>
<th>Values</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>0 — 4294967295</td>
<td></td>
</tr>
</tbody>
</table>
- **max-count max-count** — Specifies the maximum count of flows to display.
  
<table>
<thead>
<tr>
<th>Values</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1— 4294967295</td>
<td></td>
</tr>
</tbody>
</table>
- **search-type search-type** — Specifies the level of detail displayed for flows that match the search criteria.
  
<table>
<thead>
<tr>
<th>Values</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>Displays some per flow information.</td>
</tr>
<tr>
<td>count</td>
<td>Displays the number of matching flows.</td>
</tr>
<tr>
<td>detail</td>
<td>Displays all per flow information available.</td>
</tr>
</tbody>
</table>
- **transit transit-aasub-name** — Specifies an existing transit subscriber name string up to 32 characters in length.
- **url file-url** — Specifies the URL for the file to direct the search output to. The file may be local or remote.
  
<table>
<thead>
<tr>
<th>Values</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>local-url</td>
<td>remote-url</td>
</tr>
<tr>
<td>local-url</td>
<td>[&lt;cflash-id&gt;/]&lt;file-path&gt;</td>
</tr>
</tbody>
</table>
flow-record-search

**Syntax**

```plaintext
flow-record-search isa mda-id [protocol protocol-name] [application app-name] [app-group app-group-name] [flow-status flow-status] [start-flowid start-flowid] [max-count max-count] [search-type search-type] [url file-url]
```

**Context**

```
tools>dump>app-assure>group
```

**Description**

This command dumps application-assurance flow-records matching the specified criteria for an ISA.

**Parameters**

- **mda-id** — Displays flows for the specified AA ISA.
- **protocol protocol-name** — Displays flows for the specified protocol.
- **application app-name** — Displays flows for the specified application name.
- **app-group app-group-name** — Displays flows for the specified application group.
- **flow-status flow-status** — Displays flows for flows that are active or closed.
  - **Values**
    - active, closed
- **start-flowid start-flowid** — Specifies the starting flow ID.
  - **Values**
    - 0 — 4294967295
- **max-count max-count** — Specifies the maximum count of flows to display.
  - **Values**
    - 1—4294967295
- **search-type search-type** — Specifies the level of detail displayed for flows that match the search criteria.
  - **Values**
    - default — Displays some per flow information.
    - count — Displays the number of matching flows.
    - detail — Displays all per flow information available.
- **url file-url** — Specifies the URL for the file to direct the search output to. The file may be local or remote.
Values

**local-url | remote-url**

**local-url**

\[<\text{cflash-id}>/][<\text{file-path}>]

200 chars max, including cflash-id
directory length 99 chars max each

**remote-url**

\[{\text{ftp://|tftp://}}<\text{login}>:<\text{pswd}>@<\text{remote-locn}>/][<\text{file-path}>]

255 chars max
directory length 99 chars max each

**remote-locn**

\[<\text{hostname}> | <\text{ipv4-address}> | <\text{ipv6-address}>\]

ipv4-address

a.b.c.d

ipv6-address

x:x:x:x:x:x:x[-interface]

x:x:x:x:x:d.d.d[-interface]

x - [0..FFFF]H
d - [0..255]D

interface - 32 chars max, for link local addresses

cflash-id flash slot ID

---

**load-balance**

**Syntax**

load-balance [service service-id]

**Context**

tools>dump>app-assure>group

**Description**

This command rebalances AA subscribers between ISAs within a group, in case imbalance occurs such as with the addition of new cards.

**Parameters**

service service-id — Specifies the service

**Values**

1 — 2147483648
Clear Commands

group

**Syntax**

- `group aa-group-id cflowd`
- `group aa-group-id statistics`
- `group aa-group-id status`

**Context**
clear>app-assure

**Description**
This command clears application assurance group statistics or status.

**Parameters**

- `aa-group-id` — Clears data for the specified AA ISA group.
- `cflowd` — Clears application assurance cflowd statistics.
- `statistics` — Clears application assurance system and subscriber statistics.
- `status` — Clears application assurance status statistics.
Debug Commands

isa-aa-group

**Syntax**

```plaintext
isa-aa-group aa-group-id {all | unknown}
no isa-aa-group aa-group-id
```

**Context**
debug>mirror-source

**Description**
This command configures AA ISAgpoup as a mirror source for this mirror service. Traffic is mirrored after AA processing takes place on AA ISAs of the group, therefore, any packets dropped as part of that AA processing are not mirrored.

**Parameters**
- **all** — Specifies that all traffic after AA processing will be mirrored.
- **unknown** — Specifies that all traffic during the identification phase (may match policy entry or entries that have mirror action configured) and traffic that had been identified as unknown_tcp or unknown_udp after AA processing will be mirrored.
In This Section

This section provides an overview of IP Security (IPSec) software features for the IPSec ISA.

Topics in this section include:

- IP Tunnels Overview on page 240
  → Tunnel ISAs on page 243
  → Operational Conditions on page 250
  → OAM Interactions on page 251
  → Redundancy on page 251
  → Statistics Collection on page 252
  → Security on page 252
  → Video Wholesale Example on page 257
IP Tunnels Overview

This section discusses IP Security (IPSec) features for an MS-ISA. This ISA functions as a resource module for the system, providing IPSec tunneling and encryption functions. The encryption functions provided by this module are applicable for many applications including: encrypted SDPs, video wholesale, site-to-site encrypted tunnel, and remote access VPN concentration.

Figure 20 displays an example of the architecture of the 7750 IPSec implementation:

![Figure 20: 7750 IPSec Implementation Architecture](image)

In Figure 20, public network represents the “insecure network”, for example, Internet, public network connect to a public service (another name is “front-door service”) inside 7750, which could be an IES or VPRN service; while the private network represent the “secure network”, such as a company’s intranet. Private network connect to a private service.

Public and private service are typically two separated services, the only “bridge” between these two services is the IPSec function. Traffic from public network has to be authenticated and encrypted inside IPSec tunnel to reach private network. In this way, the authenticity/confidentiality/integrity of accessing private network can be enforced.

The MS-ISA provides a variety of encryption features required to establish bi-directional IPSec tunnels include:

Control Plane:

- Manual Keying
• Dynamic Keying: IKEv1/v2
• IKEv1 Mode: Main and Aggressive
• Authentication: Pre-Shared-Key /xauth with RADIUS support
• Perfect Forward Secrecy (PFS)
• DPD
• NAT-Traversal
• Security Policy

Data Plane:
• ESP (with authentication) Tunnel mode
• Authentication Algorithm: MD5/SHA1
• Encryption Algorithm: DES/3DES/AES128/AES192/AES256
• DH-Group: 1/2/5
• Replay Protection
• N:1 IPSec ISA card redundancy

There are two types of tunnel interfaces and SAPs:
• Public tunnel interface (another name is “front-door interface”): configured in the public service, use to define the subnet for IPSec tunnel local peer/gateway address.
• Public tunnel SAP: configured under public IPSec interface, a logic access point of IPSec ISA card in the public service
• Private tunnel interface: configured in the private service, can be used to define the subnet for the remote access IPSec clients.
• Private tunnel SAP: configured under private IPSec interface, a logic access point of IPSec ISA card in the private service

7750 use normal IP routing to forward IP packet into MS-ISA card:
• For upstream encrypted traffic: 7750 will forward it to public IPSec interface based on the destination address which is the local address or gateway address of IPSec tunnel. the encrypted traffic will be decrypted inside IPSec ISA card, the tunnel header will be removed, the payload IP packet will be forwarded to the private vrf, and then will be forwarded again based on the destination address of payload IP packet.
• For downstream clear traffic: to route downstream traffic into IPSec tunnel correctly, routes with IPSec tunnel as the next-hop need to be created, these routes can be configured as static route or be learned by BGP over IPSec tunnel or can be created
dynamically during IKEv1 negotiation. After clear traffic is routed into IPSec ISA card, it will be encrypted, a ESP tunnel header will be added, then it will be forward into public vrf, and the will be forwarded again based on the destination of the tunnel header.
**Tunnel ISAs**

IPSec groups in the configuration are renamed to tunnel groups, reflecting their new ability to handle not only IPSec tunnels but also IP/GRE tunnels. New MS-ISA groups created to terminate IPSec (or GRE) tunnels should be configured as tunnel groups, as shown by the CLI example below:

```
CLI Syntax: config isa
tunnel-group 1 create
    primary 1/1
    backup 2/1
    no shutdown
exit all
```

Tunnel groups have the following restrictions:

- A GRE or IPSec tunnel belongs to one and only one tunnel group
- A tunnel group can reference up to 4 tunnel-ISAs (1-4 primary, 0-3 backup). When a GRE or IPSec tunnel is created it is assigned to one of the available (operational up state) primary tunnel-ISAs in its tunnel group. If a primary tunnel-ISA in a tunnel group fails an available backup tunnel-ISA in the group takes over for the failed card. The failed tunnels are re-established, cold-standby on the backup tunnel-ISA (cold standby means the backup tunnel-ISA has no state or configuration information about the tunnels prior to the failure)
- A tunnel-ISA can be primary in only one tunnel group
- A tunnel-ISA can backup in multiple tunnel groups

The `show isa tunnel-group` allows the operator to view information about all configured tunnel-groups. This command displays the following information for each tunnel-group: group ID, primary tunnel-ISAs, backup tunnel-ISAs, active tunnel-ISAs, admin state and oper state.

---

**Public Tunnel SAPs**

A VPRN or IES service (the delivery service) must have at least one IP interface associated with a public tunnel SAP in order to receive and process the following types of packets associated with GRE and IPSec tunnels:

- unprotected GRE (IP protocol 47)
- IPSec ESP (IP protocol 50)
- IKE (UDP port 500)

The public tunnel SAP type has the format `<tunnel-group>.public:<index>`, as shown in the following CLI example.
The public tunnel SAP deprecates the public IPSec SAP that existed prior to R8.0r5.

---

**Private Tunnel SAPs**

A VPRN or IES service must have an IP interface to a GRE or IPSec tunnel in order to forward IP packets into the tunnel, causing them to be encapsulated (and encrypted) per the tunnel configuration, and to receive IP packets from the tunnel after the encapsulation has been removed (and decryption). That IP interface is associated with a private tunnel SAP.

The private tunnel SAP has the format tunnel-<tunnel-group>.private:<index>, as shown in the following CLI example where an unprotected GRE tunnel is configured under the SAP.

```plaintext
config service vprn 1 customer 1 create
    interface "gre tunnel to cel" tunnel create
        address 10.0.0.1/30
        ip-mtu 1476
        sap tunnel-1.private:210 create
            gre-tunnel "to cel" to 10.0.0.2 create
                source 64.251.12.1
                remote-ip 12.47.10.33
                backup-remote-ip 12.47.51.7
                delivery-service 199
                dscp af11
                no shutdown
            exit
        ingress
        egress
    exit
exit all
```

The private tunnel SAP deprecates the private IPSec SAP that existed prior to R8.0r5.
IP Interface Configuration

In the above configuration example the IP address 10.0.0.1 is the address of the GRE tunnel endpoint from the perspective of payload IP packets. This address belongs to the address space of the VPRN 1 service and will not be exposed to the public IP network carrying the GRE encapsulated packets. An IP interface associated with a private tunnel SAP does not support unnumbered operation.

It is possible to configure the IP MTU (M) of a private tunnel SAP interface. This sets the maximum payload IP packet size (including IP header) that can be sent into the tunnel – for example, it applies to the packet size before the tunnel encapsulation is added. When a payload IPv4 packet that needs to be forwarded to the tunnel is larger than M bytes:

- If the DF bit is clear, the payload packet is IP fragmented to the MTU size prior to tunnel encapsulation
- If the DF bit is set, the payload packet is discarded and (if allowed by the ICMP setting of the sending interface) an ICMP type 3/code 4 message should be returned to the sender (with MTU of the private tunnel SAP interface in the payload).

Unprotected GRE Tunnel Configuration

To associate an unprotected GRE tunnel with a private tunnel SAP the gre-tunnel object should be configured under the SAP. When creating a GRE tunnel the to keyword followed by the private IP address of the remote tunnel endpoint is mandatory. If this remote IP address is not within the subnet of the local private endpoint then the tunnel will not come up. In the CLI sub-tree under gre-tunnel there are commands to configure:

- the source address of the GRE tunnel. This is the source IPv4 address of GRE encapsulated packets sent by the delivery service. It must be an address in the subnet of the associated public tunnel SAP interface.
- the remote IP address. If this address is reachable in the delivery service (there is a route) then this is the destination IPv4 address of GRE encapsulated packets sent by the delivery service.
- the backup remote IP address. If the remote IP address of the tunnel is not reachable then this is the destination IPv4 address of GRE encapsulated packets sent by the delivery service.
- the delivery service. This is the id or name of the IES or VPRN service where GRE encapsulated packets are injected and terminated. The delivery service can be the same service where the private tunnel SAP interface resides.
- the DSCP marking in the outer IP header of GRE encapsulated packets. If this is not configured then the default shall be to copy the DSCP from the inner IP header to the outer IP header.
A private tunnel SAP can have only one gre-tunnel sub-object (one GRE tunnel per SAP).

The **show gre tunnel** allows the operator to view information about specific GRE tunnels or all configured GRE tunnels. This command displays the following information for each tunnel: service ID that owns the tunnel, private tunnel SAP that owns the tunnel, tunnel name, source address, remote IP address, backup remote IP address, local (private) address, destination (private) address, delivery service, dscp, admin state, oper state and type (only GRE).
GRE Tunnel Protection Using IPSec Tunnel Mode

In some deployment scenarios the GRE packets belonging to a tunnel are transported over an insecure network and are therefore vulnerable to tampering, spoofing and other forms of compromise. To provide protection against these potential threats the GRE packets may be encrypted and authenticated using IPSec. In 9.0R1 GRE packets receive IPSec protection by forwarding them, after encapsulation by one tunnel-ISA, into an IPSec tunnel supported by another tunnel-ISA – for example, the GRE tunnel is protected by IPSec tunnel mode security associations.

There is considerable configuration flexibility when it comes to configuring GRE protection by an IPSec tunnel:

- A GRE tunnel and its protecting IPSec tunnel may belong to the same or different tunnel-groups (different tunnel-groups is assumed in the example below)
- A GRE tunnel and its protecting IPSec tunnel may be assigned to the same tunnel-ISA (if they belong to the same tunnel-group) or different tunnel-ISAs.
- A single IPSec tunnel can protect one or more GRE tunnels in addition to other IP traffic that meets the IPSec security policy
- The private IPSec tunnel SAP interface and public GRE tunnel SAP interface are always part of the same VPRN. The private GRE tunnel SAP interface can be part of this same VPRN or a different VPRN.

An example configuration, corresponding to the diagram in Figure 21, is presented below. Note that the example does not include the configuration of any regular network and SAP IP interfaces (tied to IOM external I/O) that would be required in a fully functional deployment.
Figure 21: Example GRE over IPSec Tunnel Configuration

Configuration of Router A:

```
config isa
  tunnel-group 1 create
    primary 1/1
    backup 2/1
    no shutdown
    exit
  tunnel-group 2 create
    primary 3/1
    backup 2/1
    no shutdown
    exit
  exit all
config ipsec
  ike-policy 1 create
    auth-algorithm sha1
dh-group 5
  encryption-algorithm aes128
  ike-mode main
  ike-version 1
  exit
  ipsec-transform 1
    esp-auth-algorithm sha1
esp-encryption-algorithm aes256
  exit
```
exit all
config service ies 100 customer 1 create
    interface "public-ipsec-1" create
        address 1.1.1.1/24
        sap tunnel-1.public:200 create
    exit all
config service vprn 101 customer 1 create
ipsec
    security-policy 1 create
        entry 1 create
            local-ip 192.168.1.0/24
            remote-ip 192.168.2.0/24
        exit
        exit
exit
interface "private-ipsec-1" tunnel create
    sap tunnel-1.private:201 create
    ipsec-tunnel "ipsec-tunnel-for-n-gre-tunnels" create
        security-policy 1
        local-gateway-address 1.1.1.2 peer 2.2.2.2 delivery-service 100
dynamic-keying
    ike-policy 1
        pre-shared-key "secret"
        transform 1
    exit
    exit
interface "public-gre-1" create
    address 192.168.1.1/24
    sap tunnel-2.public:200 create
    exit all
interface "private-gre-1" tunnel create
    address 10.0.0.1/30
    sap tunnel-2.private:201 create
        gre-tunnel "protected-gre-tunnel" to 10.0.0.2 create
            source 192.168.1.2
            remote-ip 192.168.2.2
delivery-service 101
            no shutdown
        exit
        exit
static-route 192.168.2.0/24 next-hop ipsec-tunnel "ipsec-tunnel-for-n-gre-tunnels"
Operational Conditions

A tunnel group that is in use cannot be deleted. Changes to the primary ISA are allowed only in when the tunnel group is in a shutdown state. Change to the backup ISA (or the addition of a backup ISA) is allowed at any time unless the ISA is currently active for this tunnel group. When the backup module is active, changing the primary module is allowed without shutting down the tunnel group.

A change to the IPSec transform policy is allowed at any time. The change will not impact tunnels that have been established until they are renegotiated. If the change is required immediately the tunnel must be cleared (reset) for force renegotiation.

A change to the ike-policy is allowed at any time. The change will not impact tunnels that have been established until they are renegotiated. If the change is required immediately the tunnel must be cleared (reset) for force renegotiation.

The public interface address can be changed at any time (current behavior). If changed, tunnels that were configured to use it will require a configuration change. If the subnet changed the tunnels will be in an operationally down state until their configuration is corrected. The public service cannot be deleted while tunnels are configured to use it. A public service is the IES service that hold the regular interface that connects the node to the public network. A private service connects to the private protected service.

A tunnel group ID or tag cannot be changed. To remove an tunnel group instance, it must be in a shutdown state (both front-door and back-door).

A change to the security policy is not allowed while a tunnel is active and using the policy.

The tunnel local-gateway-address, peer address, or delivery router parameters cannot be changed while the tunnel is operationally up (shutdown will make it both admin down and operationally down).

A tunnel security policy cannot be changed while the tunnel is operationally up. An IPSec transform policy or ike-policy assignments to a tunnel requires the tunnel to be shutdown.
QoS Interactions

The MS-ISA can interact with the queuing functions on the IOM through the ingress/egress QoS provisioning in the IES or IP VPN service where the IPSec session is bound. Multiple IPSec sessions can be assigned into a single IES service. In this case, QoS defined at the IES service level, is applied to the aggregate traffic coming out of or going into the set of sessions assigned to that service.

In order to keep marking relevant in the overall networking design, the ability to translate DSCP bit marking on packets into DSCP bit markings on the IPSec tunneled packets coming out of the tunnel is supported.

OAM Interactions

The MS-ISA is IP-addressed by an operator-controlled IP on the public side. That IP address can be used in Ping and Traceroute commands and the ISA can either respond or forward the packets to the CPM.

The private side IP address is visible. The status of the interfaces and the tunnels can be viewed using show commands.

Traffic that ingresses or egresses an IES service associated with certain IPSec tunnels can be mirrored like other traffic.

Mirroring is allowed per interface (public) or IPSec interface (private) side. A filter mirror is allowed for more specific mirroring.

Redundancy

Every tunnel group can be configured with primary and backup ISAs. An ISA can be used as a backup for multiple IPSec groups. The ISAs are cold standby such that upon failure of the primary the standby resumes operation after the tunnels re-negotiate state. While the backup ISA can be shared by multiple tunnel groups only one tunnel group can fail to a single ISA at one time (no double failure support).

IPSec also supports dead peer detection (DPD).

Note that BFD can be configured on the private tunnel interfaces associated with GRE tunnels and used by the OSPF, BGP or static routing that is configured inside the tunnel.
Statistics Collection

Input and output octets and packets per service queue are used for billing end customers who are on a metered service plan. Since multiple tunnels can be configured per interface the statistics can include multiple tunnels. These can be viewed in the CLI and SNMP.

Reporting (syslog, traps) for authentication failures and other IPSec errors are supported, including errors during IKE processing for session setup and errors during encryption or decryption.

A session log indicates the sort of SA setup when there is a possible negotiation. This includes the setup time, teardown time, and negotiated parameters (such as encryption algorithm) as well as identifying the service a particular session is mapped to, and the user associated with the session.

Security

The MS-ISA module provides security utilities for IPSec-related service entities that are assigned to interfaces and SAPs. These entities (such as card, isa-tunnel module, and IES or VPRN services) must be enabled in order for the security services to process. The module only listens to requests for security services from configured remote endpoints. In the case of a VPN concentrator application, these remote endpoints could come from anywhere on the Internet. In the cases where a point-to-point tunnel is configured, the module listens only to messages from that endpoint.
IKEv2

IKEv2, defined in RFC 4306, *Internet Key Exchange (IKEv2) Protocol*, is the second version of the Internet Key Exchange Protocol. The main driver of IKEv2 is to simplify and optimize the IKEv1. An IKE_SA and a CHILD_SA could be created with only 4 IKEv2 messages exchanges. The 7750-SR supports IKEv2 with following features:

- Static lan-to-lan tunnel
- Dynamic lan-to-lan tunnel
- Pre-shared-key authentication
- Liveness check
- IKE_SA rekey
- Child_SA rekey
X.509v3 Certificate Overview

X.509 is an ITU-T standard for a public key infrastructure (PKI) which allows entities to build trust relationships between each other based on their mutual trust of Certificate Authority (CA). The trusted CA issues certificate which includes the signed public key (by CA) of issued entity. Entities can trust the certificates because they trust the CA and can verify the CA’s signature by using CA’s root certificate.

SR OS’s x.509 certificate management provides an infrastructure for x.509 certificate management including:

- Key generation
- CA profile management
- Certificate management
- CRL management

This feature can be used by other applications in the SR OS that require certificate authentication. The IKEv2 static lan-to-lan tunnel is also supported.

Key Generation

SR OS supports the generation of the following types of keys. They can be configured locally through the CLI.

- RSA
- DSA

With one of the following key sizes:

- 512
- 1024
- 2048

The generated key is stored in local CF card.

Note: the generated key file is a plain DER format file and must be imported before can be further used.
**Formats and Local Storage**

The following formats can be used by the SR OS directly:

- KEY file: encrypted file
- Certificate: DER
- Certificate-Request: PEM
- CRL: DER

The KEY/certificate/CRL files must be imported before they can be provisioned in a CA profile or tunnel configuration. SR OS stores imported files in the fixed directory `cf3:\system-pki`.

**Import and Export**

The process of import is to convert the format of input file to system’s format and save into fixed directory specified in section “Formats and Local Storage”; the process of export is to convert system’s format to one of specified format.

- Certificates can be import/export using following formats:
  - PKCS#10
  - PKCS#7 (DER and PEM)
  - PEM
  - DER

Note that certain formats of file could encapsulate multiple certificates, in this case, the SR-OS will only use the first certificate in the file.

- The Key pair can be import/export by using following formats:
  - PKCS#12 (along with certificate)
  - PEM
  - DER

- The CRL can be import/export by using following formats:
  - PKCS#7 (DER and PEM)
  - PEM
  - DER

Note that the PKCS#12 file may be encrypted with a password.
Certificate Enrollment

SR OS support X.509v3 certificate. Use the following steps to enroll a certificate:

1. Generate a key file.
2. Generate a certificate-request by using generated key file or an existing plain DER key file.
3. Send the certificate-request file to Certificate Authority (CA) via an out-of-band method.
4. CA signs the certificate-request and returns the signed certificate.
5. Import the signed certificate and the generated key.

CA Profile

The SR OS uses the ca-profile to manage Certificate Authority information. The ca-profile includes:

- CA name
- CA’s certificate
- Certificate Revocation List (CRLv2)

Use Certificate Authentication for IKEv2 Static Lan-to-Lan tunnel

The SR OS supports X.509v3 certificate authentication for IKEv2 LAN-to-LAN tunnel. And SR OS also supports asymmetric authentication, which means the SR OS and the IKEv2 peer can use different methods to authenticate. For example, one side could use pre-shared-key and the other side could use x.509 certificate.

The SR OS also supports certificatechain verification. For each static LAN-to-LAN tunnel, there will be a configurable trust-anchor, which specifies the expecting CA that should be present in the certificate chain before reaching the root or the self signed certificate.

The SR OS’s own key and certificate are also configurable per tunnel.

Note that when using certificate authentication, the SR OS will use the subject of the configured certificate as the its ID.
Video Wholesale Example

As satellite headend locations can be costly, many municipal and second tier operators cannot justify the investment in their own ground station in order to offer triple play features. However, it is possible for a larger provider or a cooperative of smaller providers to unite and provide a video headend. Each retail subscriber can purchase content from this single station, and receive it over IP. However, encryption is required so the signal cannot be understood if intercepted. A high speed encrypted tunnel is preferred over running two layers of double video protection which is cumbersome and computationally intensive.

Figure 22: Video Wholesale Configuration

As satellite headend locations can be costly, many municipal and second tier operators cannot justify the investment in their own ground station in order to offer triple play features. However, it is possible for a larger provider or a cooperative of smaller providers to unite and provide a video headend. Each retail subscriber can purchase content from this single station, and receive it over IP. However, encryption is required so the signal cannot be understood if intercepted. A high speed encrypted tunnel is preferred over running two layers of double video protection which is cumbersome and computationally intensive.
Configuring IPSec with CLI

This section provides information to configure IPSec using the command line interface.

Topics in this section include:

- Provisioning an IPSec ISA on page 259
- Configuring IPSec ISA on page 260
- Configuring Router Interfaces for IPSec on page 261
- Configuring IPSec Parameters on page 262
- Configuring IPSec in Services on page 263
- Configuring X.509v3 Certificate Parameters on page 263

Provisioning an IPSec ISA

An IPSec ISA can only be provisioned on an IOM2. The following output displays a card and ISA configuration.

*A:ALA-49>config# info

----------------------------------------------
...
card 1
  card-type iom2-20g
  mda 1
    mda-type ml0-1gb-sfp
    exit
  mda 2
    mda-type isa-ipsec
    exit
  exit
...
----------------------------------------------
*A:ALA-49>config#
Configuring IPSec ISA

The following output displays an IPSec group configuration in the ISA context. The **primary** command identifies the card/slot number where the IPSec ISA is the primary module for the IPSec group.

```
*A:ALA-49>config# info
----------------------------------------------
...  
   isa
   ipsec-group 1 create
   primary 1/2
   no shutdown
   exit
   exit

...  
----------------------------------------------
*A:ALA-49>config#  
```
Configuring Router Interfaces for IPSec

The following output displays an interface “internet” configured using the network port (1/1/1).

*A:ALA-49>config# info
----------------------------------------------
... router
    interface "internet"
        address 10.10.7.118/24
        port 1/1/1
    exit
    interface "system"
        address 10.20.1.118/32
    exit
    autonomous-system 123
    exit
...----------------------------------------------
*A:ALA-49>config#
Configuring IPSec Parameters

The following output displays an IPSec configuration example.

*A:ALA-49>config# info
----------------------------------------------
... ipsec
    ike-policy 1 create
    ipsec-lifetime 300
    isakmp-lifetime 600
    pfs
    auth-algorithm md5
    dpd interval 10 max-retries 5
    exit
    ipsec-transform 1 create
    esp-auth-algorithm sha1
    esp-encryption-algorithm aes128
    exit
    exit
...*A:ALA-49>config#
Configuring IPSec in Services

The following output displays an IES 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
  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
  interface "corporate-network" create
  address 172.17.118.118/24
  sap 1/1/2 create
  exit
  exit
  static-route 172.16.91.0/24 ipsec-tunnel "remote-office"
  no shutdown
  exit
  exit
  ...
----------------------------------------------
*A:ALA-49>config#
```

Configuring X.509v3 Certificate Parameters

The following displays steps to configure certificate enrollment.

1. Generate a key.

```
admin certificate gen-keypair cf3:/key_plain_rsa2048 size 2048 type rsa
```
2. Generate a certificate request.
   
   admin certificate gen-local-cert-req keypair cf3:/key_plain_rsa2048 subject-dn "C=US,ST=CA,CN=7750" file 7750_req.csr

3. Send the certificate request to CA-1 to sign and get the signed certificate.

4. Import the key.
   
   admin certificate import type key input cf3:/key_plain_rsa2048 output key1_rsa2048 format der

5. Import the signed certificate.
   
   admin certificate import type cert input cf3://7750_cert.pem output 7750cert format pem

The following displays steps to configure CA certificate/CRL import.

1. Import the CA certificate.
   
   admin certificate import type cert input cf3://CA_1_cert.pem output ca_cert format pem

2. Import the CA’s CRL.
   
   admin certificate import type crl input cf3://CA_1_crl.pem output ca_crl format pem
The following displays a certificate authentication for IKEv2 static LAN-to-LAN tunnel configuration.

```
config>system>security>pki>
----------------------------------------------
  ca-profile "CA-1" create
  shutdown
  cert-file "ca_cert"
  crl-file "ca_crl"
  no shutdown
  exit
config>ipsec>
----------------------------------------------
  ike-policy 1 create
    ike-version 2
    auth-method cert-auth
    own-auth-method cert
    exit
config>service>vprn>if>sap>
----------------------------------------------
  ipsec-tunnel "t50" create
    security-policy 1
    local-gateway-address 192.168.55.30 peer 192.168.33.100 delivery-service 300
    dynamic-keying
      ike-policy 1
      transform 1
      cert
        trust-anchor "CA-1"
        cert "7750cert"
        key "key1_rsa2048"
        exit
      exit
    no shutdown
    exit
```
The following displays an example of the syntax to import a certificate from the pem format.

```
*A:SR-7/Dut-A# admin certificate import type cert input cf3:/pre-import/R1-0cert.pem output R1-0cert.der format pem
```

The following displays an example of the syntax to export a certificate to the pem format.

```
*A:SR-7/Dut-A# admin certificate export type cert input R1-0cert.der output cf3:/R1-0cert.pem format pem
```
IP Security Command Reference

- Hardware Commands on page 267
- ISA Commands on page 267
- IPSEC Commands on page 268
- Service Configuration Commands on page 270
- Interface SAP Tunnel Commands on page 273
- Show Commands on page 275

Configuration Commands

Hardware Commands

```
config
   — card slot-number
      — mda mda-slot
         — isa-ipsec mda-type
         — mda-type isa-tunnel
         — no mda-type
```

ISA Commands

```
config
   — isa
      — tunnel-group tunnel-group-id [create]
      — no tunnel-group tunnel-group-id
         — backup mda-id
         — no backup
         — description description-string
         — no description
         — primary mda-id
         — no primary
         — [no] shutdown
```

```
config
   — isa
      — ins-group ins-group-id [create]
      — no ins-group ins-group-id
         — description description-string
         — no description
         — mda mda-id [drain]
```
IPSEC Commands

config
  — ipsec
    — ike-policy ike-policy-id [create]
    — no ike-policy ike-policy-id
      — auth-algorithm {md5 | sha1}
      — no auth-algorithm
      — auth-method {psk | plain-psk-xauth}
      — no auth-method
      — description description-string
      — no description
      — dh-group {1 | 2 | 5 | 14 | 15}
      — no dh-group
      — dpd [interval interval] [max-retries max-retries] [reply-only]
      — no dpd
      — encryption-algorithm {des | 3des | aes128 | aes192 | aes256}
      — no encryption-algorithm
      — ike-mode {main | aggressive}
      — no ike-mode
      — ike-version
      — no ike-version
      — ipsec-lifetime ipsec-lifetime
      — no ipsec-lifetime
      — isakmp-lifetime isakmp-lifetime
      — no isakmp-lifetime
      — nat-traversal [force] [keep-alive-interval keep-alive-interval] [force-keep-alive]
      — no nat-traversal
      — pfs [dh-group {1 | 2 | 5}]
      — no pfs
  — ipsec-transform transform-id [create]
  — no ipsec-transform transform-id
    — esp-auth-algorithm {null | md5 | sha1}
    — no esp-auth-algorithm
    — esp-encryption-algorithm {null | des | 3des | aes128 | aes192 | aes256}
    — no esp-encryption-algorithm
  — static-sa sa-name
    — [no] authentication md5 | sha1 {ascii-key ascii-key | hex-key hex-key}
    — no authentication
    — description description-string
    — no description
    — direction inbound | outbound | bidirectional
    — no direction
    — protocol ah | esp
    — no protocol
    — spi spi-key
config
  -- no spi

  ipsec
    tunnel-template ipsec template identifier [create]
    no tunnel-template/ipsec template identifier
      -- description description-string
      -- no description
      -- replay-window {32 | 64 | 128 | 256 | 512}
      -- no replay-window
      -- [no] sp-reverse-route
      -- transform transform-id [transform-id...(up to 4 max)]
      -- no transform
Service Configuration Commands

```bash
config
  — service
    — vprn service-id [customer customer-id]
    — no vprn service-id
    — ipsec
      — security-policy security-policy-id [create]
      — no security-policy security-policy-id
        — entry entry-id [create]
        — no entry entry-id
          — local-ip {ip-prefix/prefix-length | ip-prefix netmask | any}
          — remote-ip {ip-prefix/prefix-length | ip-prefix netmask | any}
      — [no] interface ip-int-name [create] [tunnel]
        — 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] [type cpm-np]
          — no bfd
          — cflowd {acl | interface}
          — no cflowd
          — cpu-protection policy-id
          — no cpu-protection
          — delayed-enable seconds
          — no delayed-enable
          — description description-string
          — no description [description-string]
          — 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]
            — 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
— [no] dhcp6-server
— [no] 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] local-dhcp-server
— local-proxy-arp local-server-name
— **no** local-proxy-arp
— [no] loopback
— mac ieee-address
— [no] mac [ieee-address]
— [no] proxy-arp-policy
— [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]
— tos-marking-state {trusted | untrusted}
— **no** tos-marking-state
— unnumbered {ip-int-name | ip-address}
— [no] unnumbered
— [no] urpf-check
— — **mode** {strict | loose}
— — [no] mode
— vpls {service-id | service-name}
— **no** vpls
— — egress
— — — reclassify-using-qos
— — ingress
— — — v4-routed-override-filter ipv6-filter-id
— — — [no] v4-routed-override-filter
— — — v6-routed-override-filter ipv6-filter-id
— — — [no] v6-routed-override-filter
— — [no] shutdown
— ipsec-tunnel ipsec-tunnel-name [create]
— **no** ipsec-tunnel ipsec-tunnel-name
— — [no] bfd-designate
— — [no] bfd-enable service service-id interface interface-name dst-ip ip-address
— — description description-string
— — [no] description
— — [no] auto-establish
— — ike-policy ike-policy-id
— — [no] ike-policy
— — pre-shared-key key
— no pre-shared-key
— transform transform-id [transform-id...(up to 4)]
— no transform
— local-gateway-address ip-address peer ip-address
delivery-service service-id
— no local-gateway-address
— [no] manual-keying
  — security-association security-entry-id authentication-key encryption-key encryption-key spi spi transform transform-id direction {inbound | outbound}
  — no security-association security-entry-id
direction {inbound | outbound}
— replay-window {32 | 64 | 128 | 256 | 512}
— no replay-window
— security-policy security-policy-id
— no security-policy
— [no] shutdown
Interface SAP Tunnel Commands

```
config
  service
    ies service-id [customer customer-id] [vpn vpn-id]
    interface ip-int-name [tunnel]
      sap sap-id [create]
        gre-tunnel gre-tunnel-name [to ip-address] [create]
        no gre-tunnel gre-tunnel-name
          backup-remote-ip ip-address
          no backup-remote-ip
          delivery-service {service-id | svc-name}
          no delivery-service
          description description-string
          no description
          dscp dscp-name
          no dscp
          remote-ip ip-address
          no remote-ip
          [no] shutdown
          source ip-address
          no source
    [no] ipsec-gw
      default-secure-service service-id ipsec-interface ip-int-name
      no default-secure-service
      default-tunnel-template ipsec template identifier
      no default-tunnel-template
      ike-policy ike-policy-id
      no ike-policy
      local-gateway-address ip-address
      no local-gateway-address
      pre-shared-key key
      no pre-shared-key
      [no] shutdown
  vprn service-id [customer customer-id]
  [no] vprn service-id
    interface ip-int-name [create] [tunnel]
      sap sap-id [create]
        gre-tunnel gre-tunnel-name [to ip-address] [create]
        no gre-tunnel gre-tunnel-name
          backup-remote-ip ip-address
          no backup-remote-ip
          delivery-service {service-id | svc-name}
          no delivery-service
          description description-string
          no description
          dscp dscp-name
          no dscp
          remote-ip ip-address
          no remote-ip
          [no] shutdown
          source ip-address
          no source
    [no] ipsec-gw
```
— default-secure-service service-id ipsec-interface ip-int-name
— no default-secure-service
— default-tunnel-template ipsec template identifier
— no default-tunnel-template
— ike-policy ike-policy-id
— no ike-policy
— local-gateway-address ip-address
— no local-gateway-address
— pre-shared-key key
— no pre-shared-key
— [no] shutdown
— ipsec-tunnel ipsec-tunnel-name [create]
— no ipsec-tunnel ipsec-tunnel-name
— [no] bfd-designate
— [no] bfd-enable service service-id interface interface-name dst-ip ip-address
— description description-string
— no description
— [no] dynamic-keying
  — [no] auto-establish
  — cert
  — ike-policy ike-policy-id
  — no ike-policy
  — pre-shared-key key
  — no pre-shared-key
  — transform transform-id [transform-id...(up to 4 max)]
  — [no] transform
— local-gateway-address ip-address peer ip-address
delivery-service service-id
— no local-gateway-address
— [no] manual-keying
  — security-association security-entry-id
    authentication-key authentication-key
    encryption-key encryption-key spi spi
    transform transform-id direction
    {inbound | outbound}
  — [no] replay-window
  — security-policy security-policy-id
  — no security-policy
  — [no] shutdown
Show Commands

show
  — ipsec
    — gateway name name
    — gateway [service service-id]
    — gateway tunnel [ip-address:port]
    — gateway name name tunnel ip-address:port
    — gateway name name tunnel
    — gateway tunnel count
    — gre
      — tunnel [gre-tunnel-name]
      — ike-policy ike-policy-id
      — ike-policy
      — security-policy service-id [security-policy-id]
      — security-policy
      — static-sa
      — static-sa name sa-name
      — static-sa spi spi
      — transform [transform-id]
      — tunnel ipsec-tunnel-name
      — tunnel
      — tunnel-template [ipsec template identifier]
  — isa
    — tunnel-group
IPSec Configuration Commands

Generic Commands

description

Syntax  
\texttt{description \ description-string}

Context  
\texttt{config>isa>ipsec-group}
\texttt{config>isa}

Description  
This command creates a text description which is stored in the configuration file to help identify the content of the entity.

The \texttt{no} form of the command removes the string from the configuration.

Default  
none

Parameters  
\texttt{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.

shutdown

Syntax  
\texttt{[no] shutdown}

Context  
\texttt{config>isa}
\texttt{config>isa>aa-group}
\texttt{config>isa>tunnel-grp}

Description  
This command administratively disables the entity. When disabled, an entity does not change, reset, or remove any configuration settings or statistics. Many entities must be explicitly enabled using the \texttt{no shutdown} command.

The \texttt{shutdown} command administratively disables an entity. 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.
Hardware Commands

mda-type

**Syntax**  
```
mda-type isa-tunnel
no mda-type
```

**Context**  
```
config>card>mda
```

**Description**  
This command provisions or de-provisions an MDA to or from the device configuration for the slot.

**Parameters**  
`isa-tunnel` — Specifies the ISA tunnel.

isa-ipsec

**Syntax**  
```
mda-type isa-ipsec
no mda-type
```

**Context**  
```
config>card>mda
```

**Description**  
This command provisions an adaptor into an MDA position on an IOM slot. The ISA IPSec module is provisioned into the system in the same manner as all other MDA types. Once an ISA IPSec module is provisioned, independent of it actually existing in the system or the specified slot and ISA position, the ISA IPSec module can be defined as a member of an IPSec module group. These module groups can then be used to assign hardware resources to particular services.

The `no` form of this command removes the module from the configuration. The module must be administratively shut down before it can be deleted from the configuration.

Refer to the 7750 SR OS Interface Guide for further information on command usage and syntax for the ISA IPSec module and other MDA types.

**Default**  
No ISA types are configured for any slots by default.

**Parameters**  
`isa-ipsec` — Specifies the IPSec module for the slot position.
ISA Commands

isa

Syntax  isa
Context config
Description This command enables the context to configure Integrated Services Adapter (ISA) parameters.

tunnel-group

Syntax  tunnel-group tunnel-group-id [create]
        no tunnel-group tunnel-group-id
Context config>isa
Description This command allows a tunnel group to be created or edited. A tunnel group is a set of one or more MS-ISAs that support the origination and termination of IPSec and IP/GRE tunnels. All of the MS-ISAs in a tunnel group must have isa-tunnel as their configured mda-type.

The no form of the command deletes the specified tunnel group from the configuration

Parameters

  tunnel-group-id — An integer value that uniquely identifies the tunnel-group.

    Values  1—16

    create — Mandatory keyword used when creating tunnel group in the ISA context. The create keyword requirement can be enabled/disabled in the environment>create context.

backup

Syntax  backup mda-id
        no backup
Context config>isa>tunnel-grp
Description This command assigns an ISA IPSec module configured in the specified slot to this IPSec group. The backup module provides the IPSec group with warm redundancy when the primary module in the group is configured. An IPSec group must always have a primary configured.

Primary and backup modules have equal operational status and when both modules are coming up, the one that becomes operational first becomes the active module. An IPSec module can serve as a backup for multiple IPSec groups but the backup can become active for only one ISA IPSec group at a time.

All configuration information is pushed down to the backup MDA from the CPM once the CPM gets notice that the primary module has gone down. This allows multiple IPSec groups to use the same
backup module. Any statistics not yet spooled will be lost. Auto-switching from the backup to primary, once the primary becomes available again, is supported.

The operator is notified through SNMP events when:

- When the ISA IPSec service goes down (all modules in the group are down) or comes back up (a module in the group becomes active).
- When ISA IPSec redundancy fails (one of the modules in the group is down) or recovers (the failed module comes back up).
- When an ISA IPSec activity switch took place.

The **no** form of the command removes the specified module from the IPSec group.

**Default**

no backup

**Parameters**

`mda-id` — Specifies the card/slot identifying a provisioned module to be used as a backup module.

<table>
<thead>
<tr>
<th>Values</th>
<th>mdadf:</th>
</tr>
</thead>
<tbody>
<tr>
<td>slot</td>
<td>1 — up to 10 depending on chassis model</td>
</tr>
<tr>
<td>mda</td>
<td>1 — 2</td>
</tr>
</tbody>
</table>

**primary**

**Syntax**

`primary mda-id`

`no primary`

**Context**

`config>isa>tunnel-grp`

**Description**

This command assigns an ISA IPSec module configured in the specified slot to this IPSec group. The backup ISA IPSec provides the IPSec group with warm redundancy when the primary ISA IPSec in the group is configured. Primary and backup ISA IPSec have equal operational status and when both MDAs are coming up, the one that becomes operational first becomes the active ISA IPSec.

All configuration information is pushed down to the backup MDA from the CPM once the CPM gets notice that the primary module has gone down. This allows multiple IPSec groups to use the same backup module. Any statistics not yet spooled will be lost. Auto-switching from the backup to primary, once the primary becomes available again, is supported.

The operator is notified through SNMP events when:

- When the ISA IPSec service goes down (all modules in the group are down) or comes back up (a module in the group becomes active).
- When ISA IPSec redundancy fails (one of the modules in the group is down) or recovers (the failed module comes back up).
- When an ISA IPSec activity switch took place.

The **no** form of the command removes the specified primary ID from the group’s configuration.

**Default**

no primary

**Parameters**

`mda-id` — Specifies the card/slot identifying a provisioned IPSec ISAA.
Internet Key Exchange (IKE) Commands

ipsec

Syntax
```
ipsec
```

Context
```
config
```

Description
This command enables the context to configure Internet Protocol security (IPSec) parameters. IPSec
is a structure of open standards to ensure private, secure communications over Internet Protocol (IP)
networks by using cryptographic security services.

ike-policy

Syntax
```
ike-policy
ike-policy-id [create]
no ike-policy ike-policy-id
```

Context
```
config>ipsec
```

Description
This command enables the context to configured an IKE policy.

Parameters
```
ike-policy-id — Specifies a policy ID value to identify the IKE policy.
```

Values
```
1 — 2048
```

auth-algorithm

Syntax
```
auth-algorithm {md5 | sha1}
no auth-algorithm
```

Context
```
config>ipsec>ike-policy
```

Description
The command specifies which hashing algorithm to use for the IKE authentication function.

Parameters
```
md5 — Specifies the hmac-md5 algorithm for authentication.
sha1 — Specifies the hmac-sha1 algorithm for authentication.
```

auth-method

Syntax
```
auth-method {psk | plain-psk-xauth}
no auth-method
```

Context
```
config>ipsec>ike-policy
```
Description  This command specifies the authentication method used with this IKE policy. The no form of the command removes the parameter from the configuration.

Default  no auth-method

Parameters  
- psk — Both client and gateway authenticate each other by a hash derived from a pre-shared secret. Both client and gateway must have the PSK. This work with both IKEv1 and IKEv2.
- plain-psk-xauth — Both client and gateway authenticate each other by pre-shared key and RADIUS. This work with IKEv1 only.

dh-group

Syntax  dh-group {1 | 2 | 5 | 14 | 15}  
no dh-group

Context  config>ipsec>ike-policy

Description  This command specifies which Diffie-Hellman group to calculate session keys. Three groups are supported with IKE-v1:

- Group 1: 768 bits
- Group 2: 1024 bits
- Group 5: 1536 bits
- Group 14: 2048 bits
- Group 15: 3072 bits

More bits provide a higher level of security, but require more processing.

Default  5

The no form of the command removes the Diffie-Hellman group specification.

dpd

Syntax  dpd [interval interval] [max-retries max-retries] [reply-only]  
no dpd

Context  config>ipsec>ike-policy

Description  This command controls the dead peer detection mechanism. The no form of the command removes the parameters from the configuration.

Parameters  
- interval interval — Specifies the interval that will be used to test connectivity to the tunnel peer. If the peer initiates the connectivity check before the interval timer it will be reset.

Values  
- 10 — 300 seconds

Default  30
max-retries

Specifies the maximum number of retries before the tunnel is removed.

Values 2 — 5

Default 3

reply-only

Specifies to only reply to DPD keepalives. Issuing the command without the reply-only keyword disables the behavior.

Values reply-only

encryption-algorithm

Syntax encryption-algorithm {des | 3des | aes128 | aes192 | aes256}

Context config>ipsec>ike-policy

Description This command specifies the encryption algorithm to use for the IKE session. The no form of the command removes the encryption algorithm from the configuration.

Default aes128

Parameters des — This parameter configures the 56-bit des algorithm for encryption. This is an older algorithm, with relatively weak security. While better than nothing, it should only be used where a strong algorithm is not available on both ends at an acceptable performance level.

3des — This parameter configures the 3-des algorithm for encryption. This is a modified application of the des algorithm which uses multiple des operations for more security.

aes128 — This parameter configures the aes algorithm with a block size of 128 bits. This is the mandatory implementation size for aes.

aes192 — This parameter configures the aes algorithm with a block size of 192 bits. This is a stronger version of aes.

aes256 — This parameter configures the aes algorithm with a block size of 256 bits. This is the strongest available version of aes.

ike-mode

Syntax ike-mode {main | aggressive}

Context config>ipsec>ike-policy

Description This command specifies one of either two modes of operation. IKE version 1 can support main mode and aggressive mode. The difference lies in the number of messages used to establish the session.

The no form of the command removes the mode of operation from the configuration.

Default main
Parameters

**main** — Specifies identity protection for the hosts initiating the IPSec session. This mode takes slightly longer to complete.

**aggressive** — Aggressive mode provides no identity protection but is faster.

<iike-version>

**Syntax**

```
ikey-version {1 | 2}
nok ikey-version
```

**Context**

```
config>ipsec>ike-policy
```

**Description**

This command sets the IKE version (1 or 2) that the *ike-policy* will use.

**Default**

1

**Parameters**

1 | 2 — The version of IKE protocol.

<ipsec-lifetime>

**Syntax**

```
ipsec-lifetime ipsec-lifetime
nok ipsec-lifetime
```

**Context**

```
config>ipsec>ike-policy
```

**Description**

This parameter specifies the lifetime of a phase two SA.

The *no* form of the command reverts the ipsec-lifetime value to the default.

**Default**

3600 (1 hour)

**Parameters**

*ipsec-lifetime* — specifies the lifetime of the phase two IKE key in seconds.

**Values**

60 — 4294967295

<isakmp-lifetime>

**Syntax**

```
isakmp-lifetime isakmp-lifetime
nok isakmp-lifetime
```

**Context**

```
config>ipsec>ike-policy
```

**Description**

This command specifies the lifetime of a phase one SA. ISAKMP stands for Internet Security Association and Key Management Protocol.

The *no* form of the command reverts the isakmp-lifetime value to the default.

**Default**

28800

**Parameters**

— Specifies the lifetime of the phase one IKE key in seconds.

**Values**

60 — 4294967295
nat-traversal

**Syntax**

```
nat-traversal [force] [keep-alive-interval keep-alive-interval] [force-keep-alive]
no nat-traversal
```

**Context**

```
config>ipsec>ike-policy
```

**Description**

This command specifies whether NAT-T (Network Address Translation Traversal) is enabled, disabled or in forced mode.

The `no` form of the command reverts the parameters to the default.

**Default**

none

**Parameters**

- **force** — Forces to enable NAT-T.
- **keep-alive-interval**
  - **keep-alive-interval**
    - **Values** 10 — 3600 seconds
  - **force-keep-alive** — When specified, the keep-alive does not expire.

pfs

**Syntax**

```
pfs [dh-group {1 | 2 | 5}]
no pfs
```

**Context**

```
config>ipsec>ike-policy
```

**Description**

This command enables perfect forward secrecy on the IPSec tunnel using this policy. PFS provides for a new Diffie-hellman key exchange each time the SA key is renegotiated. After that SA expires, the key is forgotten and another key is generated (if the SA remains up). This means that an attacker who cracks part of the exchange can only read the part that used the key before the key changed.

There is no advantage in cracking the other parts if they attacker has already cracked one.

The `no` form of the command disables PFS. If this it turned off during an active SA, when the SA expires and it is time to re-key the session, the original Diffie-hellman primes will be used to generate the new keys.

**Default**

5

**Parameters**

- **dh-group**
  - **dh-group**
    - **Values** 1 — 5
      - **Group 1**: 768 bits
      - **Group 2**: 1024 bits
      - **Group 5**: 1536 bits

static-sa

Syntax  
[no] static-sa  sa-name

Context  
config>ipsec

Description  
This command configures an IPSec static SA.

direction

Syntax  
direction  inbound | outbound | bidirectional

Context  
config>ipsec>static-sa

Description  
This command configures the direction for an IPSec manual SA. The no statement resets to the default value.

Default  
bidirectional

protocol

Syntax  
protocol  ah | esp

Context  
config>ipsec>static-sa

Description  
This command configures the security protocol to use for an IPSec manual SA. The no statement resets to the default value.

Parameters  
ah — Specifies the Authentication Header protocol.

esp — Specifies the Encapsulation Security Payload protocol.

Default  
esp

authentication

Syntax  
authentication  md5 | sha1 {ascii-key|hex-key  key}

Context  
config>ipsec>static-sa

Description  
This command configures the authentication algorithm to use for an IPSec manual SA. The no statement resets to the default value.

Default  
sha1

Parameters  
ascii-key — Specifies an ASCII key.

hex-key — Specifies a HEX key.
spi

Syntax

spi spi-key
no spi

Context config>ipsec>static-sa

Description This command configures the SPI key value for an IPSec manual SA. The no statement resets to the default value.

ipsec-transform

Syntax ipsec-transform transform-id [create]

Context config>ipsec

Description This command enables the context to create an ipsec-transform policy. IPSec transforms policies can be shared. A change to the ipsec-transform is allowed at any time. The change will not impact tunnels that have been established until they are renegotiated. If the change is required immediately the tunnel must be cleared (reset) for force renegotiation.

IPSec transform policy assignments to a tunnel require the tunnel to be shutdown.

The no form of the command removes the ID from the configuration.

Parameters

transform-id — Specifies a policy ID value to identify the IPSec transform policy.

Values

1 — 2048

create — Keyword that

create — This keyword is mandatory when creating an ipsec-transform policy. The create keyword requirement can be enabled/disabled in the environment>create context.

esp-auth-algorithm

Syntax esp-auth-algorithm {null | md5 | sha1}
no esp-auth-algorithm

Context config>ipsec>transform

Description The command specifies which hashing algorithm should be used for the authentication function Encapsulating Security Payload (ESP). Both ends of a manually configured tunnel must share the same configuration parameters for the IPSec tunnel to enter the operational state.

The no form of the command disables the authentication.

Parameters

null — This is a very fast algorithm specified in RFC 2410, which provides no authentication.

md5 — This parameter configures ESP to use the hmac-md5 algorithm for authentication.

sha1 — This parameter configures ESP to use the hmac-sha1 algorithm for authentication.
esp-encryption-algorithm

Syntax: esp-encryption-algorithm {null | des | 3des | aes128 | aes192 | aes256}
no esp-encryption-algorithm

Context: config>ipsec>transform

Description: This command specifies the encryption algorithm to use for the IPSec session. Encryption only applies to esp configurations. If encryption is not defined esp will not be used.

For IPSec tunnels to come up, both ends need to be configured with the same encryption algorithm.

The no form of the command removes the

Default: aes128

Parameters:

null — This parameter configures the high-speed null algorithm, which does nothing. This is the same as not having encryption turned on.

des — This parameter configures the 56-bit des algorithm for encryption. This is an older algorithm, with relatively weak security. Although slightly better than no encryption, it should only be used where a strong algorithm is not available on both ends at an acceptable performance level.

3des — This parameter configures the 3-des algorithm for encryption. This is a modified application of the des algorithm which uses multiple des operations to make things more secure.

aes128 — This parameter configures the aes algorithm with a block size of 128 bits. This is the mandatory impelmentation size for aes. As of today, this is a very strong algorithm choice.

aes192 — This parameter configures the aes algorithm with a block size of 192 bits. This is a stronger version of aes.

aes256 — This parameter configures the aes algorithm with a block size of 256 bits. This is the strongest available version of aes.

tunnel-template

Syntax: tunnel-template ipsec template identifier [create]
no tunnel-template ipsec template identifier

Context: config>ipsec

Description: This command creates a tunnel template. Up to 2,000 templates are allowed.

Default: none

Parameters:

ipsec template identifier — Specifies the template identifier.

Values: 1 — 2048

create — Mandatory keyword used when creating a tunnel-template in the IPSec context. The create keyword requirement can be enabled/disabled in the environment>create context.
replay-window

Syntax  
\texttt{replay-window \{32 | 64 | 128 | 256 | 512\}}
\texttt{no replay-window}

Context  
\texttt{config>ipsec>tnl-temp}

Description  
This command sets the anti-replay window.
The \texttt{no} form of the command removes the parameter from the configuration.

Default  
\texttt{no replay-window}

Parameters  
\{32 | 64 | 128 | 256 | 512\} — Specifies the size of the anti-replay window.

sp-reverse-route

Syntax  
\texttt{[no] sp-reverse-route}

Context  
\texttt{config>ipsec>tnl-temp}

Description  
This command specifies whether the node using this template will accept framed-routes sent by the RADIUS server and install them for the lifetime of the tunnel as managed routes.
The \texttt{no} form of the command disables sp-reverse-route.

Default  
\texttt{no sp-reverse-route}

transform

Syntax  
\texttt{transform transform-id [transform-id...(up to 4 max)]}
\texttt{no transform}

Context  
\texttt{config>ipsec>tnl-temp}

Description  
This command configures IPSec transform.
IPSec Configuration 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 a 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.
ipsec

Syntax: ipsec
Context: config>service>vprn>ipsec
Description: This command enables the context to configure IPSec policies.
Default: none

security-policy

security-policy security-policy-id [create]
no security-policy security-policy-id

Context: config>service>vprn>ipsec
Description: This command configures a security policy to use for an IPSec tunnel.
Default: none
Parameters: security-policy-id — specifies a value to be assigned to a security policy.
Values: 1 — 8192
create — Keyword used to create the security policy instance. The create keyword requirement can be enabled/disabled in the environment>create context.

entry

Syntax: entry entry-id [create]
no entry entry-id

Context: config>service>vprn>ipsec>sec-plcy
Description: This command configures an IPSec security policy entry.
Parameters: entry-id — Specifies the IPSec security policy entry.
Values: 1 — 16
create — Keyword used to create the security policy entry instance. The create keyword requirement can be enabled/disabled in the environment>create context.
**local-ip**

**Syntax**  
local-ip \{ip-prefix/prefix-length | ip-prefix netmask | any\}

**Context**  
config>service>vprn>ipsec>sec-plcy>entry

**Description**  
This command configures the local (from the VPN) IP prefix/mask for the policy parameter entry. Only one entry is necessary to describe a potential flow. The local-ip and remote-ip commands can be defined only once. The system will evaluate the local IP as the source IP when traffic is examined in the direction of VPN to the tunnel and as the destination IP when traffic flows from the tunnel to the VPN. The remote IP will be evaluated as the source IP when traffic flows from the tunnel to the VPN when traffic flows from the VPN to the tunnel.

**Parameters**  
- **ip-prefix** — The destination address of the aggregate route in dotted decimal notation.
  - **Values**
    - a.b.c.d (host bits must be 0)
    - prefix-length 1 — 32
  - **netmask** — The subnet mask in dotted decimal notation.
  - **any** — keyword to specify that it can be any address.

**remote-ip**

**Syntax**  
remote-ip ip-prefix/prefix-length | ip-prefix netmask | any

**Context**  
config>service>vprn>ipsec>sec-plcy>entry

**Description**  
This command configures the remote (from the tunnel) IP prefix/mask for the policy parameter entry. Only one entry is necessary to describe a potential flow. The local-ip and remote-ip commands can be defined only once. The system will evaluate the local IP as the source IP when traffic is examined in the direction of VPN to the tunnel and as the destination IP when traffic flows from the tunnel to the VPN. The remote IP will be evaluated as the source IP when traffic flows from the tunnel to the VPN when traffic flows from the VPN to the tunnel.

**Parameters**  
- **ip-prefix** — The destination address of the aggregate route in dotted decimal notation.
  - **Values**
    - a.b.c.d (host bits must be 0)
    - prefix-length 1 — 32
  - **netmask** — The subnet mask in dotted decimal notation.
  - **any** — keyword to specify that it can be any address.
interface

Syntax  
```
interface ip-int-name [create] [tunnel]
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 subscriber 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 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.

Values  
1 — 32 characters maximum

`tunnel` — Specifies that the interface is configured as tunnel interface, which could be used to terminate IPSec or GRE tunnels in the private service.

`create` — Keyword used to create the IPSec interface instance. The `create` keyword requirement can be enabled/disabled in the `environment>create` context.
sap

Syntax

```
sap sap-id [create]
no sap sap-id
```

Context

```
config>service>ies>if
config>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.

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 Appendix A: Common CLI Command Descriptions on page 533 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.

### address

| **Syntax** | `address {ip-address/mask | ip-address netmask} [broadcast {all-ones | host-ones}]` |
|------------|--------------------------------------------------------------------------------------------------|
|            | `no address`                                                                                   |

| **Context** | `config>service>vprn>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 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. |
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.

Parameters

ip-address — Specifies the base IP address of 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. 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.

allow-directed-broadcasts

Syntax [no] allow-directed-broadcasts

Context config>service>vprn>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.
arp-populate

**Syntax**  
[no] arp-populate

**Context**  
config>service>vprn>if

**Description**  
This command enables populating static and dynamic hosts into the system ARP cache. When enabled, the host’s IP address and MAC address are placed in the system ARP cache as a managed entry. Static hosts must be defined on the interface using the `host` command. Dynamic hosts are enabled on the system through enabling lease-populate in the IP interface DHCP context. In the event that both a static host and a dynamic host share the same IP and MAC address, the system’s ARP cache retains the host information until both the static and dynamic information are removed. Both static and dynamic hosts override static ARP entries. Static ARP entries are marked as inactive when they conflict with static or dynamic hosts and will be repopulated once all static and dynamic host information for the IP address are removed. Since static ARP entries are not possible when static subscriber hosts are defined or when DHCP lease state table population is enabled, conflict between static ARP entries and the arp-populate function is not an issue.

The `arp-populate` command will fail if an existing static subscriber host on the SAP does not have both MAC and IP addresses specified.

Once `arp-populate` is enabled, creating a static subscriber host on the SAP without both an IP address and MAC address will fail.

`arp-populate` can only be enabled on VPRN interfaces supporting Ethernet encapsulation.

Use the `no` form of the command to disable ARP cache population functions for static and dynamic hosts on the interface. All static and dynamic host information in the systems ARP cache will be removed. Any existing static ARP entries previously inactive due to static or dynamic hosts will be populated in the system ARP cache.

When `arp-populate` is enabled, the system will not send out ARP Requests for hosts that are not in the ARP cache. Only statically configured and DHCP learned hosts are reachable through an IP interface with arp-populate enabled.

**Default**  
not enabled

arp-timeout

**Syntax**  
arp-timeout seconds
no arp-timeout

**Context**  
config>service>vprn>if

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.

---

**bfd**

**Syntax**  

bfd *transmit-interval* [receive *receive-interval*] [multiplier *multiplier*] [echo-receive *echo-interval*] [type *cpm-np*]  

no bfd

**Context**  

config>service>vprn>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 7750-SR, 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 — 10000.
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
10 — 100000 (see Important Notes above)

Default 100

receive receive-interval — Sets the receive interval for the BFD session.

Values 10 — 100000
10 — 100000 (see Important Notes above)

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
10 — 100000 (see Important Notes above)

Default 100

type cpm-np — Specifies that BFD sessions associated with this interface will be created on the CPM network processor to allow for fast timers down to 10ms granularity.

cflowd

Syntax  cflowd {acl | interface}

no cflowd

Context  config>service>vprn>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.

Default  no cflowd

Parameters  acl — cflowd configuration associated with a filter.
interface — cflowd configuration associated with an IP interface.
cpu-protection

Syntax  
```
cpu-protection policy-id
no cpu-protection
```

Context  
```
config>service>vprn>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 a the default policy is used to limit the overall-rate. The default policy is policy number 1 and can be viewed in the `show>system>security>cpu-protection>policy 1` command output.

The `no` form of the command removes CPU protection policy association from the interface, resulting in no default rate limiting of control packets.

Default  
cpu-protection 254 (for access interfaces)
cpu-protection 255 (for network interfaces)
none (for video-interfaces (where applicable), 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
```

delayed-enable

Syntax  
```
delayed-enable seconds [init-only]
no delayed-enable
```

Context  
```
config>service>vprn>sub-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  
no delayed-enable

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.
host-connectivity-verify

Syntax  

    host-connectivity-verify [source {vrrp|interface}] [interval interval]  
    [action {remove|alarm}] [timeout retry-timeout] [retry-count count]

Context  config>service>vprn>if

Description  This command enables 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.

icmp

Syntax  icmp

Context  config>service>vprn>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

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
```

**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
```

**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
```

**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

**ip-mtu**

**Syntax**

```
ip-mtu octets
```

```
no ip-mtu
```

**Context**

```
config > service > vprn > ipsec-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
```
Parameters  

octets — Specifies the MTU size for this interface.

Values  
512 — 9000

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  

ip-address — This parameter 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.

secondary ip-address — This parameter 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.

peer-ip-address

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.

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.
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 (eight 16-bit pieces)
  x:x:x:x:d.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.
bdf

**Syntax**

```bash
bdf transmit-interval [receive receive-interval] [multiplier multiplier] [echo-receive echo-interval] [type cpm-np]
nobfd
```

**Context**

`config>service>vprn>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 7750-SR, 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 `bdf` command without specifying the `type` parameter.

**Default**

`nobfd`

**Parameters**

- `transmit-interval` — Sets the transmit interval for the BFD session.
  
  **Values**
  
  - `10 — 100000`
  - `10 — 100000` (see Important Notes above)
  
  **Default**
  
  `100`

- `receive receive-interval` — Sets the receive interval for the BFD session.
  
  **Values**
  
  - `10 — 100000`
  - `10 — 100000` (see Important Notes above)
  
  **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`
  - `10 — 100000` (see Important Notes above)
  
  **Default**
  
  `100`
type cpm-np — Specifies that BFD sessions associated with this interface will be created on the CPM network processor to allow for fast timers down to 10ms granularity.

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` is `(eight 16-bit pieces)`
  - `x:x:x:x:x:x:x` (eight 16-bit pieces)
  - `x:x:x:x:d.d.d` (eight 16-bit pieces)
  - `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**

```
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-dhcp-server**

**Syntax**

```
local-dhcp-server server-name [create]
```

```
no local-dhcp-server server-name
```

**Context**

`config>service>vprn>dhcp`

**Description**

This command instantiates a local DHCP server. A local DHCP server can serve multiple interfaces but is limited to the routing context it was which it was created.

**Default**

none

**Parameters**

- `server-name` — Specifies the name of local DHCP server.

  - `create` — Keyword used to create the server name. The `create` keyword requirement can be enabled/disabled in the environment>create context.

**local-proxy-arp**

**Syntax**

```
[no] local-proxy-arp
```

**Context**

`config>service>vprn>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**

none
**loopback**

**Syntax**  
[no] loopback

**Context**  
config>service>vprn>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).

**Default**  
None

**mac**

**Syntax**  
[no] mac ieee-mac-address

**Context**  
config>service>vprn>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.

**proxy-arp-policy**

**Syntax**  
[no] proxy-arp-policy policy-name [policy-name...(up to 5 max)]

**Context**  
config>service>vprn>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.
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
```

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

```
config>service>vprn>if
```

Description

This command assigns an 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** command 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**

```
[no] static-arp ip-address ieee-mac-address
```

**Context**

```
config>service>vprn>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.
tos-marking-state

Syntax  
tos-marking-state {trusted | untrusted}
no tos-marking-state

Context  
config>service>vprn>sub-if>grp-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.

urpf-check

Syntax  
[no] urpf-check

Context  
config>service>vprn>if

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}
no mode

Context

config>service>vprn>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.

vpls

Syntax

vpls service-name

Context

config>service
config>service>vprn>if

Description

The vpls command, within the IP interface context, is used to bind the IP interface to the specified service name.

The system does not attempt to resolve the service name provided until the IP interface is placed into the administratively up state (no shutdown). Once the IP interface is administratively up, the system will scan the available VPLS services that have the allow-ip-int-binding flag set for a VPLS service associated with the name. If the service name is bound to the service name when the IP interface is already in the administratively up state, the system will immediately attempt to resolve the given name.

If a VPLS service is found associated with the name and with the allow-ip-int-binding flag set, the IP interface will be attached to the VPLS service allowing routing to and from the service virtual ports once the IP interface is operational.

A VPLS service associated with the specified name that does not have the allow-ip-int-binding flag set or a non-VPLS service associated with the name will be ignored and will not be attached to the IP interface.

If the service name is applied to a VPLS service after the service name is bound to an IP interface and the VPLS service allow-ip-int-binding flag is set at the time the name is applied, the VPLS service will be automatically resolved to the IP interface if the interface is administratively up or when the interface is placed in the administratively up state.

If the service name is applied to a VPLS service without the allow-ip-int-binding flag set, the system will not attempt to resolve the applied service name to an existing IP interface bound to the name. To
rectify this condition, the flag must first be set and then the IP interface must enter or reenter the administratively up state.

While the specified service name may be assigned to only one service context in the system, it is possible to bind the same service name to more than one IP interface. If two or more IP interfaces are bound to the same service name, the first IP interface to enter the administratively up state (if currently administratively down) or to reenter the administratively up state (if currently administratively up) when a VPLS service is configured with the name and has the allow-ip-int-binding flag set will be attached to the VPLS service. Only one IP interface is allowed to attach to a VPLS service context. No error is generated for the remaining non-attached IP interfaces using the service name.

Once an IP interface is attached to a VPLS service, the name associated with the service cannot be removed or changed until the IP interface name binding is removed. Also, the allow-ip-int-binding flag cannot be removed until the attached IP interface is unbound from the service name.

Unbinding the service name from the IP interface causes the IP interface to detach from the VPLS service context. The IP interface may then be bound to another service name or a SAP or SDP binding may be created for the interface using the sap or spoke-sdp commands on the interface.

IES CHASSIS MODE DEPENDENCY
An IES IP interface cannot be bound to a service name unless the system is configured in chassis mode D. Once an IES interface is bound to a service name, the chassis mode of the system cannot be changed to B or C.

VPRN HARDWARE DEPENDENCY
When a service name is bound to a VPRN IP interface, all SAPs associated with the VPRN service must be on hardware based on the FlexPath2 forwarding plane. Currently, these include the IOM3-XP, the various IMM modules and the SR7710c12. If any SAPs are associated with the wrong hardware type, the service name binding to the VPRN IP interface will fail. Once an IP interface within the VPRN service is bound to a service name, attempting to create a SAP on excluded hardware will fail.

ROUTE EXPORT AND IMPORT BETWEEN ROUTING CONTEXTS
The IES chassis mode dependency and the VPRN hardware dependency each are designed to prevent a condition where an ingress routing decision on hardware that does not support the mixed L2 and L3 behavior of routed VPLS is asked to route to a VPLS based next-hop.

Even with these restrictions, it is still possible using route leaking or import/export routing policies to create a condition where a FlexPath1 forwarding plane resolves a route to a VPLS next-hop. In this case, the forwarding plane handles the resolved next-hop as if it points to a null IP interface. Packets associated with a null next-hop egress IP interface will be discarded and an ICPM unreachable message will be generated when enabled.

IP INTERFACE MTU AND FRAGMENTATION
A VPLS service is affected by two MTU values; port MTUs and the VPLS service MTU. The MTU on each physical port defines the largest L2 packet (including all DLC headers and CRC) that may be transmitted out a port. The VPLS itself has a service level MTU that defines the largest packet supported by the service. This MTU does not include the local encapsulation overhead for each port (QinQ, Dot1Q, TopQ or SDP service delineation fields and headers) but does include the remainder of the packet and the trailing CRC. As virtual ports are created in the system, the virtual port cannot become operational unless the configured port MTU minus the virtual port service delineation overhead is greater than or equal to the configured VPLS service MTU. Thus, an operational virtual port is ensured to support the largest packet traversing the VPLS service. The service delineation
overhead on each L2 packet is removed before forwarding into a VPLS service. VPLS services do not support fragmentation and must discard any L2 packet larger than the service MTU after the service delineation overhead is removed.

IP interfaces have a configurable up MTU that defines the largest packet that may egress the IP interface without being fragmented. This MTU encompasses the IP portion of the packet and does not include any of the egress DLC header or CRC. This MTU does not affect the size of the largest ingress packet on the IP interface. If the egress IP portion of the packet is larger than the IP interface MTU and the IP header do not fragment flag is not set, the packet is fragmented into smaller packets that will not exceed the configured MTU size. If the do not fragment bit is set, the packet is silently discarded at egress when it exceeds the IP MTU.

When the IP interface is bound to a VPLS service, the IP MTU must be at least 18 bytes less than the VPLS service MTU. This allows for the addition of the minimal Ethernet encapsulation overhead; 6 bytes for the DA, 6 bytes for the SA, 2 bytes for the Etype and 4 bytes for the trailing CRC. Any remaining egress virtual port overhead (Dot1P, Dot1Q, QinQ, TopQ or SDP) required above the minimum is known to be less than the egress ports MTU since the virtual port would not be operational otherwise.

If the IP interface IP MTU value is too large based on the VPLS service MTU, the IP interface will enter the operationally down state until either the IP MTU is adequately lowered or the VPLS service MTU is sufficiently increased.

The no form of the command on the IP interface is used to remove the service name binding from the IP interface. If the service name has been resolved to a VPLS service context and the IP interface has been attached to the VPLS service, the IP interface will also be detached from the VPLS service.

| Default | none |
| Parameters | service-name |

The service-name parameter is required when using the IP interface vpls command and specifies the service name that the system will attempt to resolve to an allow-ip-int-binding enabled VPLS service associated with the name. The specified name is expressed as an ASCII string comprised of up to 32 characters. It does not need to already be associated with a service and the system does not check to ensure that multiple IP interfaces are not bound to the same name.

### Ingress

**Syntax:** ingress

**Context:** config>service>vprn>if>vpls

**Description:** The ingress node in this context under the vpls binding is used to define the routed IPv4 and IPv6 optional filter overrides.

### V4-routed-override-filter

**Syntax:**
- v4-routed-override-filter
- ipv4-filter-id
- no v4-routed-override-filter

**Context:** config>service>vprn>if>vpls>ingress
IPSec Configuration Commands

**Description**  
The v4-routed-override-filter command is used to specify an IPv4 filter ID that will be applied to all ingress packets entering the VPLS service. The filter overrides any existing ingress IPv4 filter applied to SAPs or SDP bindings for packets associated with the routing IP interface. The override filter is optional and when it is not defined or it is removed, the IPv4 routed packets will use the any existing ingress IPv4 filter on the VPLS virtual port.

The no form of the command is used to remove the IPv4 routed override filter from the ingress IP interface. When removed, the IPv4 ingress routed packets within a VPLS service attached to the IP interface will use the IPv4 ingress filter applied to the packets virtual port when defined.

**Default** none

**Parameters**  
*ipv4-filter-id* — The ipv4-filter-id parameter is required when executing the v4-routed-override-filter command. The specified filter ID must exist as an IPv4 filter within the system or the override command will fail.

---

**v6-routed-override-filter**

**Syntax**  
`v6-routed-override-filter ipv6-filter-id`  
`no v6-routed-override-filter`

**Context**  
`config>service>vprn>if>vpls>ingress`

**Description**  
The v6-routed-override-filter command is used to specify an IPv6 filter ID that will be applied to all ingress packets entering the VPLS service. The filter overrides any existing ingress IPv6 filter applied to SAPs or SDP bindings for packets associated with the routing IP interface. The override filter is optional and when it is not defined or it is removed, the IPv6 routed packets will use the any existing ingress IPv6 filter on the VPLS virtual port.

The no v6-routed-override-filter command is used to remove the IPv6 routed override filter from the ingress IP interface. When removed, the IPv6 ingress routed packets within a VPLS service attached to the IP interface will use the IPv6 ingress filter applied to the packets virtual port when defined.

**Default** none

**Parameters**  
*ipv6-filter-id* — The ipv6-filter-id parameter is required when executing the v6-routed-override-filter command. The specified filter ID must exist as an IPv6 filter within the system or the override command will fail.

---

**egress**

**Syntax**  
`egress`

**Context**  
`config>service>vprn>if>vpls`

**Description**  
The egress node under the vpls binding is used to define the optional sap-egress QoS policy that will be used for reclassifying the egress forwarding class or profile for routed packets associated with the IP interface on the attached VPLS service context.
reclassify-using-qos

Syntax  
reclassify-using-qos sap-egress-qos-id
no reclassify-using-qos

Context  
config>service>vprn>if>vpls>egress

Description  
The reclassify-using-qos command is used to specify a sap-egress QoS policy that will be used to reclassify the forwarding class and profile of egress routed packets on the VPLS service. When routed packets associated with the IP interface egress a VPLS SAP, the reclassification rules within the sap-egress QoS policy applied to the SAP are always ignored (even when reclassify-using-qos is not defined).

Any queues or policers defined within the specified QoS policy are ignored and are not created on the VPLS egress SAPs. Instead, the routed packets continue to use the forwarding class mappings, queues and policers from the sap-egress QoS policy applied to the egress VPLS SAP.

While the specified sap-egress policy ID is applied to an IP interface it cannot be deleted from the system.

The no form of the command removes the sap-egress QoS policy used for reclassification from the egress IP interface. When removed, IP routed packets will not be reclassified on the egress SAPs of the VPLS service attached to the IP interface.

Parameters  
sap-egress-qos-id — The sap-egress-qos-id parameter is required when executing the reclassify-using-qos command. The specified SAP egress QoS ID must exist within the system or the command will fail.

allow-ip-int-binding

Syntax  
[no] allow-ip-int-binding

Context  
config>service>vpls

Description  
The allow-ip-int-binding command that sets a flag on the 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 features
- Network Domain on SDP bindings [Not sure how we enforce this.]
• GRE SDP bindings are not supported
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 re-applied 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.

---

**ipv6**

**Syntax**

```
[no] ipv6
```

**Context**

```
config>service>vprn>if
```

**Description**

This command configures IPv6 parameters.

**Parameters**

`bytes` — Specifies the MTU for the nodes to use to send packets on the link.

**Values**

1280-9212
unnumbered

Syntax  unnumbered [ip-int-name | ip-address]
no unnumbered

Context  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 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.

egress

Syntax  egress

Context  config>service>vprn>if

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

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-limit

Syntax  agg-rate-limit agg-rate [queue-frame-based-accounting]
no agg-rate-limit

Context  config>service>vprn>if

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.

### 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>egress
cfg>service>vprn>if>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

**match-qinq-dot1p**

**Syntax**

```text
match-qinq-dot1p {top | bottom}
no match-qinq-dot1p
```

**Context**

```text
config>service>vprn>if>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>
<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 / TopQ</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 9: 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>
<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>
The dot1p dot1p-value command must be configured without the qinq-mark-top-only parameter to remove the TopQ PBits only marking restriction.

### qinq-mark-top-only

<table>
<thead>
<tr>
<th>Syntax</th>
<th>[no] qinq-mark-top-only</th>
</tr>
</thead>
<tbody>
<tr>
<td>Context</td>
<td>config&gt;service&gt;vprn&gt;if&gt;egress</td>
</tr>
<tr>
<td>Description</td>
<td>When enabled (the encapsulation type of the access port where this SAP is defined as qinq), the <strong>qinq-mark-top-only</strong> command specifies which P-bits to mark during packet egress. When disabled, both set of P-bits are marked. When the enabled, only the P-bits in the top Q-tag are marked.</td>
</tr>
<tr>
<td>Default</td>
<td>no qinq-mark-top-only</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>
qos

Syntax  
qos policy-id [shared-queuing | multipoint-shared]

no qos

Context  
config>service>vprn>if>egress
config>service>vprn>if>ingress

Description  
Associates a Quality of Service (QoS) policy with an ingress or egress Service Access Point (SAP) or IP interface. 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 or IP interface ingress and egress policies on SAP or IP interface 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.

When an ingress QoS policy is defined on an ingress IP interface that is bound to a VPRN, the policy becomes associated with every SAP on the VPRN and augments the QoS policy that is defined on each SAP. Packets that are bridged will be processed using the policy defined on the VPRN SAP; packets that are routed will be processed using the policy defined in the IES IP interface-binding context.

When an egress QoS policy is associated with an IP interface that has been bound to a VPRN, the policy becomes associated with every SAP on the VPRN 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 VPRN SAP; packets that are routed will be processed using the policy defined in the IP interface-binding context.

By default, no specific QoS policy is associated with the SAP or IP interface 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 or IP interface, and the QoS policy reverts to the default.

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 — Specify 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.

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

**ipsec-tunnel**

**Syntax**

- `ipsec-tunnel ipsec-tunnel-name [create]`
- `no ipsec-tunnel ipsec-tunnel-name`

**Context**

config>service>vprn>if>sap

**Description**

This command specifies an IPSec tunnel name. An IPSec client sets up the encrypted tunnel across public network. The 7750-SR IPSec MDA acts as a concentrator gathering, and terminating these IPSec tunnels into an IES or VPRN service. This mechanism allows as service provider to offer a global VPRN service even if node of the VPRN are on an uncontrolled or insecure portion of the network.

**Default** none

**Parameters**

- `ipsec-tunnel-name` — Specifies an IPSec tunnel name up to 32 characters in length.
- `create` — Keyword used to create the IPSec tunnel instance. The `create` keyword requirement can be enabled/disabled in the `environment>create` context.

**bfd-designate**

**Syntax**

- `[no] bfd-designate`

**Context**

config>service>vprn>if>sap>tunnel

**Description**

This command specifies whether this IPSec tunnel is the BFD designated tunnel.

**Default** none
**bfd-enable**

**Syntax**

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

**Context**

`config>service>vprn>if>tunnel`

**Description**

This command assign a BFD session provide heart-beat mechanism for given IPSec tunnel. There can be only one BFD session assigned to any given IPSec tunnel, but there can be multiple IPSec tunnels using same BFD session. BFD control the state of the associated tunnel, if BFD session goes down, system will also bring down the associated non-designated IPSec tunnel.

**Default**

`none`

**Parameters**

- `service service-id` — Specifies where the service-id that the BFD session resides.
- `interface interface-name` — Specifies the name of the interface used by the BFD session.
- `dst-ip ip-address` — Specifies the destination address to be used for the BFD session.

**dynamic-keying**

**Syntax**

```
[no] dynamic-keying
```

**Context**

`config>service>vprn>if>tunnel`

**Description**

This command enables dynamic keying for the IPSec tunnel.

**Default**

`none`

**auto-establish**

**Syntax**

```
[no] auto-establish
```

**Context**

`config>service>vprn>if>tunnel`

**Description**

This command specifies whether to attempt to establish a phase 1 exchange automatically. The `no` form of the command disables the automatic attempts to establish a phase 1 exchange.

**Default**

`no auto-establish`

**transform**

**Syntax**

```
transform transform-id [transform-id...(up to 4 max)]
no transform
```

**Context**

`config>service>vprn>if>tunnel>dynamic-keying`

**Description**

This command associates the IPSec transform sets allowed for this tunnel. A maximum of four transforms can be specified. The transforms are listed in decreasing order of preference (the first one specified is the most preferred).
Default none
Parameters transform-id — Specifies the value used for transforms for dynamic keying.
  Values 1 — 2048

local-gateway-address

Syntax  local-gateway-address ip-address peer ip-address delivery-service service-id
        no local-gateway-address
Context  config>service>vprn>if>tunnel
Description This command specifies the local gateway address used for the tunnel and the address of the remote
         security gateway at the other end of the tunnel remote peer IP address to use.
Default The base routing context is used if the delivery-router option is not specified.
Parameters ip-address — IP address of the local end of the tunnel.
         delivery-service service-id — The ID of the IES or VPRN (front-door) delivery service of this
tunnel. Use this service-id to find the VPRN used for delivery.
         Values service-id: 1 — 2147483648
         svc-name: Specifies an existing service name up to 64 characters in length.

manual-keying

Syntax  [no] manual-keying
Context  config>service>vprn>if>tunnel
Description This command configures Security Association (SA) for manual keying. When enabled, the
         command specifies whether this SA entry is created manually by the user or dynamically by the
         IPSec sub-system.
Default none

security-association

Syntax  security-association security-entry-id authentication-key authentication-key encryption-key
        encryption-key spi spi transform transform-id direction {inbound | outbound}
        no security-association security-entry-id direction {inbound | outbound}
Context  config>service>vprn>if>tunnel>manual-keying
Description This command configures the information required for manual keying SA creation.
Default none
Parameters security-entry-id — Specifies the ID of an SA entry.
Values 1 — 16

**encryption-key**
- Specifies the key used for the encryption algorithm.
- Values: none or 0x0..0xFFFFFFFF...(max 64 hex nibbles)

**authentication-key**
- Specifies the key used for the authentication algorithm.
- Values: none or 0x0..0xFFFFFFFF...(max 40 hex nibbles)

**spi**
- Specifies the SPI (Security Parameter Index) used to look up the instruction to verify and decrypt the incoming IPSec packets when the direction is inbound. When the direction is outbound, the SPI that will be used in the encoding of the outgoing packets. The remote node can use this SPI to lookup the instruction to verify and decrypt the packet.
- Values: 256 — 16383

**transform**
- Specifies the transform entry that will be used by this SA entry. This object should be specified for all the entries created which are manual SAs. If the value is dynamic, then this value is irrelevant and will be zero.
- Values: 1 — 2048

**direction**
- Specifies the direction of an IPSec tunnel.

### replay-window

**Syntax**
```
replay-window {32 | 64 | 128 | 256 | 512}
```
```
no replay-window
```

**Context**
```
config>service>vprn>if>tunnel
```

**Description**
This command specifies the size of the anti-replay window. The anti-replay window protocol secures IP against an entity that can inject messages in a message stream from a source to a destination computer on the Internet.

**Default**
none

**Parameters**
```
{32 | 64 | 128 | 256 | 512} — Specifies the size of the SA anti-replay window.
```

### security-policy

**Syntax**
```
security-policy security-policy-id
```
```
no security-policy
```

**Context**
```
config>service>vprn>ipsec-if>tunnel
```

**Description**
This command configures an IPSec security policy. The policy may then be associated with tunnels defined in the same context.

**Default**
none

**Parameters**
```
security-policy-id — Specifies the IPSec security policy entry that the tunnel will use.
```
```
Values 1 — 8192
```

---

Page 330  OS Multi-Service ISA Guide
Interface SAP Tunnel Commands

gre-tunnel

Syntax

- **gre-tunnel** gre-tunnel-name \[to ip-address\] \[create\]
- **no gre-tunnel** gre-tunnel-name

Context

- config>service>interface>ies>sap
- config>service>interface>vprn>sap>gre-tunnel

Description

This command defines an unprotected IP/GRE tunnel and associates it with a private tunnel SAP within an IES or VPRN service. When the IP/GRE tunnel is created the **to** keyword followed by the private address of the remote tunnel endpoint are mandatory.

The **no** form of the command deletes the specified IP/GRE tunnel from the configuration. The tunnel must be administratively shutdown before issuing the **no gre-tunnel** command.

Default

- no GRE tunnels are defined

Parameters

- **gre-tunnel-name** — Specifies the name of the GRE 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.
- **ip-address** — The private IP address of the remote GRE tunnel endpoint. If this remote IP address is not within the subnet of the local private endpoint, the IP interface associated with the tunnel will not come up.

source

Syntax

- **source** ip-address
- **no source**

Context

- config>service>interface>ies>sap
- config>service>interface>vprn>sap>gre-tunnel

Description

This command sets the source IPv4 address of GRE encapsulated packets associated with a particular GRE tunnel. It must be an address in the subnet of the associated public tunnel SAP interface. The GRE tunnel does not come up until a valid source address is configured.

The **no** form of the command deletes the source address from the GRE tunnel configuration. The tunnel must be administratively shutdown before issuing the **no source** command.

Parameters

- **ip-address** — Specifies the source IPv4 address of the GRE tunnel.
  - Values: 1.0.0.0 — 223.255.255.255
remote-ip

Syntax  
remote-ip ip-address
no remote-ip

Context  
config>service>interface>ies>sap
config>service>interface>vprn>sap>gre-tunnel

Description  
This command sets the primary destination IPv4 address of GRE encapsulated packets associated with a particular GRE tunnel. If this address is reachable in the delivery service (there is a route) then this is the destination IPv4 address of GRE encapsulated packets sent by the delivery service.

The no form of the command deletes the destination address from the GRE tunnel configuration.

Parameters  
  ip-address — Specifies the destination IPv4 address of the GRE tunnel.

  Values  
  1.0.0.0 — 223.255.255.255

backup-remote-ip

Syntax  
backup-remote-ip ip-address
no backup-remote-ip

Context  
config>service>interface>ies>sap>gre-tunnel
config>service>interface>vprn>sap>gre-tunnel

Description  
This command sets the backup destination IPv4 address of GRE encapsulated packets associated with a particular GRE tunnel. If the primary destination address is not reachable in the delivery service (there is no route) or not defined then this is the destination IPv4 address of GRE encapsulated packets sent by the delivery service.

The no form of the command deletes the backup-destination address from the GRE tunnel configuration.

Parameters  
  ip-address — Specifies the destination IPv4 address of the GRE tunnel.

  Values  
  1.0.0.0 — 223.255.255.255

delivery-service

Syntax  
delivery-service {service-id | svc-name}
no delivery-service

Context  
config>service>interface>ies>sap>delivery-service
config>service>interface>vprn>sap>gre-tunnel

Description  
This command sets the delivery service for GRE encapsulated packets associated with a particular GRE tunnel. This is the IES or VPRN service where the GRE encapsulated packets are injected and terminated. The delivery service may be the same service that owns the private tunnel SAP associated with the GRE tunnel. The GRE tunnel does not come up until a valid delivery service is configured.
The **no** form of the command deletes the delivery-service from the GRE tunnel configuration.

### Parameters

**service-id** — Identifies the service used to originate and terminate the GRE encapsulated packets belonging to the GRE tunnel.

**Values**

- 1–2147483648

**svc-name** — Identifies the service used to originate and terminate the GRE encapsulated packets belonging to the GRE tunnel.

**Values**

- 1–64 characters

### dscp

**Syntax**

```plaintext
dscp dscp-name
no dscp
```

**Context**

- `config>service>interface>ies>sap`
- `config>service>interface>vprn>sap>gre-tunnel`

**Description**

This command sets the DSCP code-point in the outer IP header of GRE encapsulated packets associated with a particular GRE tunnel. The default, set using the no form of the command, is to copy the DSCP value from the inner IP header (after remarking by the private tunnel SAP egress qos policy) to the outer IP header.

**Default**

`no dscp`

**Parameters**

**dscp** — 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`
IPSec Gateway Commands

ipsec-gw

Syntax
[no] ipsec-gw

Context
config>service>ies>if>sap
config>service>vprn>if>sap

Description
This command configures an IPSec gateway.

default-secure-service

Syntax
default-secure-service service-id ipsec-interface ip-int-name
no default-secure-service

Context
config>service>ies>if>sap>ipsec-gateway
config>service>vprn>if>sap>ipsec-gateway

Description
This command specifies a service ID or service name of the default security service used by this SAP IPSec gateway.

Parameters
service-id — Specifies a default secure service.

Values
service-id: 1 — 2147483648
svc-name: An existing service name up to 64 characters in length.

default-tunnel-template

Syntax
default-tunnel-template ipsec template identifier
no default-tunnel-template

Context
config>service>ies>if>sap>ipsec-gateway
config>service>vprn>if>sap>ipsec-gateway

Description
This command configures a default tunnel policy template for the gateway.

ike-policy

Syntax
ike-policy ike-policy-id
no ike-policy

Context
config>service>ies>if>sap>ipsec-gateway
config>service>vprn>if>sap>ipsec-gateway

Description
This command configures IKE policy for the gateway.
### Parameters

**ike-policy-id** — Specifies the IKE policy ID.

**Values**

1 — 2048

#### local-gateway-address

**Syntax**

```
local-gateway-address ip-address
no local-gateway-address
```

**Context**

```
cfg>service>ies>if>sap>ipsec-gateway
cfg>service>vprn>if>sap>ipsec-gateway
```

**Description**

This command configures an ipsec-gateway local address.

#### pre-shared-key

**Syntax**

```
pre-shared-key key
no pre-shared-key
```

**Context**

```
cfg>service>ies>if>sap>ipsec-gateway
cfg>service>vprn>if>sap>ipsec-gateway
```

**Description**

This command specifies the shared secret between the two peers forming the tunnel.

**Parameters**

**key** — Specifies a pre-shared-key for dynamic-keying.

#### cert

**Syntax**

```
[no] cert local-file-url
```

**Default**

```
cfg>service>vprn>if>sap>ipsec-tun>dynamic-keying>cert>
cfg>svc>vprn>if>sap>ipsec-gw>cert>
```

**Description**

This command specifies the certificate that 7750 used to identify itself in case peer need it. 7750 will load(reload) the certificate from the configured URL when the ipsec-tunnel/ipsec-gw is “no shutdown”.

When system is loading the certificate, it will check if it is a valid X.509v3 certificate by performing following:

- **key** file must be already configured
- Configured cert file must be a DER formatted X.509v3 certificate file
- All non-optional fields defined in section 4.1 of RFC5280 must exist in the cert-file and conform to the RFC5280 defined format.
- The version field to see if its value is 0x2
- The Validity field to see that if the certificate is still in validity period.
- If Key Usage extension exists, then At least digitalSignature and keyEncipherment shall be set;
The public key of the certificate can match with the public key in the configured key file.
If any of above checks fails, then the "no shutdown" command will fails

Configured certificate file url can only be changed or removed when tunnel or gw is shutdown.
Same certificate could be used for multiple ipsec-tunnels or ipsec-gws, however for each certificate file, there is only one memory instance, if a certificate file has been updated, "no shutdown" in any of tunnel that use the certificate file will cause the memory instance updated, which will not impact the current up and running tunnels that use the certificate file, but the new authentication afterwards will use the updated memory instance.

Default  None
Parameters  local-file-url — URL for input file, this url is local CF card URL.

key

Syntax  [no] key local-file-url
Context  config>service>vprn>if>sap>ipsec-tun>dynamic-keying>cert
         config>svc>vprn>if>sap>ipsec-gw>cert
Description  This command specifies the key pair file 7750 will use for X.509 certificate authentication. System will load the key file when the ipsec-tunnel/gw is "no shutdown"
When system is loading the key file, it will check if it is a valid 7750 formatted key file.
Key file url can only be changed or removed when tunnel or gw is shutdown.
Same key could be used for multiple ipsec-tunnels or ipsec-gws, however for each key file, there is only one memory instance, if a key file has been updated, "no shutdown" in any of tunnel that use the key file will cause the memory instance updated, which will not impact the current up and running tunnels that use the key file, but the new authentication afterwards will use the updated memory instance.

Default  None
Parameters  local-file-url — URL for input file, this url is local CF card URL.

local-id

Syntax  [no] local-id type {ipv4|fqdn|dn} [value id-value]}
Context  config>service>vprn>if>sap>ipsec-tun>dynamic-keying>cert
         config>svc>vprn>if>sap>ipsec-gw>cert
Description  This command specifies the local id of 7750 used for IDi or IDr for IKEv2.
The local-id can only be changed or removed when tunnel or gw is shutdown.
type — Specifies the type of ID payload, it could be ipv4 address/FQDN domain name| distinguish name of subject in X.509 certificate
value — Specifies the corresponding value of ID payload when type is configured as ipv4 or fqdn; when type is configured as dn, the value should be extracted from configured certificate.

auto-establish

Syntax  [no] auto-establish
Context  config>service>vprn>if>sap>ipsec-tun
Description  The system will automatically establish phase 1 SA as soon as the tunnel is provisioned and enabled (no shutdown). This option should only be configured on one side of the tunnel.

Note that any associated static routes will remain up as long as the tunnel could be up, even though it may actually be Oper down according to the CLI.

Default  None
LSN Commands

**Ins-group**

Syntax

```plaintext
Ins-group Ins-group-id [create]
no Ins-group Ins-group-id
```

Context

```
config>isa
```

Description

This command configures an ISA L2TP Network Server (LNS) group.

Parameters

- `Ins-group-id` — Specifies the LNS group ID.

  Values

  - `create` — Keyword that specifies the creation of a new LNS group.

**mda**

Syntax

```plaintext
mda mda-id [drain]
no mda mda-id
```

Context

```
config>isa>lns-group
```

Description

This command configures an ISA LNS group MDA.

Parameters

- `drain` — Specifies to prevent the creation of new destinations, tunnels, and sessions but does NOT disconnect any active sessions.
IPSec Show Commands

gateway

**Syntax**
gateway name name

gateway [service service-id]

gateway tunnel [ip-address:port]

gateway name name tunnel ip-address:port

gateway name name tunnel

gateway tunnel count

**Context**
show>ipsec

**Description**
This command displays IPSec gateway information.

**Parameters**
name name — Specifies an IPSec gateway name.

service service-id — specifies the service ID of the default security service used by the IPSec gateway.

Values

1 — 214748364

svc-name: 64 char max

tunnel ip-address:port — Specifies to display the IP address and UDP port of the SAP IPSec gateway to the tunnel.

Values

port: 0— 65535

count — Specifies to display the number of IPSec gateway tunnels with the ike-policy>auth-method command set to psk.

tunnel

**Syntax**
tunnel [gre-tunnel-name]

**Context**
show>gre

**Description**
This command displays information about a particular GRE tunnel or all GRE tunnels.

**Parameters**
gre-tunnel-name — Specifies the name of a GRE tunnel.

The following table lists the information displayed for each GRE tunnel

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TunnelName (Tunnel Name)</td>
<td>The name of the GRE tunnel.</td>
</tr>
<tr>
<td>SvcID (Service ID)</td>
<td>The service ID of the IES or VPRN service that owns the GRE tunnel.</td>
</tr>
<tr>
<td>SapId (Sap ID)</td>
<td>The ID of the private tunnel SAP that owns the GRE tunnel.</td>
</tr>
<tr>
<td>Label</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Description</td>
<td>The description for the GRE tunnel.</td>
</tr>
<tr>
<td>LocalAddress (Source Address)</td>
<td>The source address of the GRE tunnel (public/outer IP)</td>
</tr>
<tr>
<td>RemoteAddress (Remote Address)</td>
<td>The destination address of the GRE tunnel (public/outer IP)</td>
</tr>
<tr>
<td>Bkup RemAddr (Backup Address)</td>
<td>The backup destination address of the GRE tunnel (public/outer IP)</td>
</tr>
<tr>
<td>To (Target Address)</td>
<td>The remote address of the GRE tunnel (private/inner IP). This is the peer’s IP address to the GRE tunnel. This comes from the tunnel configuration.</td>
</tr>
<tr>
<td>DlvrySvcId (Delivery Service)</td>
<td>The service ID of the IES or VPRN service that handles the GRE encapsulated packets belonging to the tunnel.</td>
</tr>
<tr>
<td>DSCP</td>
<td>The forced DSCP codepoint in the outer IP header of GRE encapsulated packets belonging to the tunnel.</td>
</tr>
<tr>
<td>Admn (Admin State)</td>
<td>Admin state of the tunnel (up/down).</td>
</tr>
<tr>
<td>Oper (Operational State)</td>
<td>Operational state of the tunnel (up/down).</td>
</tr>
<tr>
<td>Oper Rem Addr (Oper Remote Addr)</td>
<td>The destination address of the GRE tunnel (public/outer IP) that is currently being used.</td>
</tr>
<tr>
<td>Pkts Rx</td>
<td>Number of GRE packets received belonging to the tunnel.</td>
</tr>
<tr>
<td>Pkts Tx</td>
<td>Number of GRE packets transmitted belonging to the tunnel.</td>
</tr>
<tr>
<td>Bytes Rx</td>
<td>Number of bytes in received GRE packets associated with the tunnel.</td>
</tr>
<tr>
<td>Bytes Tx</td>
<td>Number of bytes in transmitted GRE packets associated with the tunnel.</td>
</tr>
<tr>
<td>Key Ignored Rx</td>
<td>Incremented every time a GRE packet is received with a GRE key field.</td>
</tr>
<tr>
<td>Too Big Tx</td>
<td>Incremented every time an IP packet with DF=1 is to be forwarded into the GRE tunnel and its size exceeds the interface IP MTU.</td>
</tr>
<tr>
<td>Seq Ignored Rx</td>
<td>Incremented every time a GRE packet is received with a sequence number.</td>
</tr>
<tr>
<td>Vers Unsup. Rx</td>
<td>Incremented every time a GRE packet is dropped because the GRE version is unsupported.</td>
</tr>
<tr>
<td>Label</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Description</td>
<td>The description for the GRE tunnel.</td>
</tr>
<tr>
<td>LocalAddress (Source Address)</td>
<td>The source address of the GRE tunnel (public/outer IP)</td>
</tr>
<tr>
<td>RemoteAddress (Remote Address)</td>
<td>The destination address of the GRE tunnel (public/outer IP)</td>
</tr>
<tr>
<td>Bkup RemAddr (Backup Address)</td>
<td>The backup destination address of the GRE tunnel (public/outer IP)</td>
</tr>
<tr>
<td>To (Target Address)</td>
<td>The remote address of the GRE tunnel (private/inner IP). This is the peer’s IP address to the GRE tunnel. This comes from the tunnel configuration.</td>
</tr>
<tr>
<td>DlvrySvcId (Delivery Service)</td>
<td>The service ID of the IES or VPRN service that handles the GRE encapsulated packets belonging to the tunnel.</td>
</tr>
<tr>
<td>DSCP</td>
<td>The forced DSCP codepoint in the outer IP healer of GRE encapsulated packets belonging to the tunnel.</td>
</tr>
<tr>
<td>Admin (Admin State)</td>
<td>Admin state of the tunnel (up/down).</td>
</tr>
<tr>
<td>Oper (Operational State)</td>
<td>Operational state of the tunnel (up/down).</td>
</tr>
<tr>
<td>Oper Rem Addr (Oper Remote Addr)</td>
<td>The destination address of the GRE tunnel (public/outer IP) that is currently being used.</td>
</tr>
<tr>
<td>Pkts Rx</td>
<td>Number of GRE packets received belonging to the tunnel.</td>
</tr>
<tr>
<td>Pkts Tx</td>
<td>Number of GRE packets transmitted belonging to the tunnel.</td>
</tr>
<tr>
<td>Bytes Rx</td>
<td>Number of bytes in received GRE packets associated with the tunnel.</td>
</tr>
<tr>
<td>Bytes Tx</td>
<td>Number of bytes in transmitted GRE packets associated with the tunnel.</td>
</tr>
<tr>
<td>Key Ignored Rx</td>
<td>Incremented every time a GRE packet is received with a GRE key field.</td>
</tr>
<tr>
<td>Too Big Tx</td>
<td>Incremented every time an IP packet with DF=1 is to be forwarded into the GRE tunnel and its size exceeds the interface IP MTU.</td>
</tr>
<tr>
<td>Seq Ignored Rx</td>
<td>Incremented every time a GRE packet is received with a sequence number.</td>
</tr>
<tr>
<td>Vers Unsup. Rx</td>
<td>Incremented every time a GRE packet is dropped because the GRE version is unsupported.</td>
</tr>
</tbody>
</table>
### Sample Output

```bash
dut-A# show gre tunnel

GRE Tunnels

<table>
<thead>
<tr>
<th>TunnelName</th>
<th>LocalAddress</th>
<th>SvcId</th>
<th>Admn</th>
<th>SapId</th>
<th>RemoteAddress</th>
<th>DlvrySvcId</th>
<th>Oper</th>
<th>RemAddr</th>
<th>DSCP</th>
<th>Oper Rem Addr</th>
</tr>
</thead>
<tbody>
<tr>
<td>toce2</td>
<td>50.1.1.7</td>
<td>500</td>
<td>Up</td>
<td>tunnel-1.private:1</td>
<td>30.1.1.3</td>
<td>500</td>
<td>Up</td>
<td>30.1.1.3</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>20.1.1.2</td>
<td>30.1.1.3</td>
<td>None</td>
<td>Up</td>
<td>30.1.1.2</td>
<td>30.1.2.7</td>
<td>None</td>
<td>30.1.1.3</td>
<td>None</td>
<td></td>
<td></td>
</tr>
<tr>
<td>toce2_backup</td>
<td>50.1.2.3</td>
<td>502</td>
<td>Up</td>
<td>tunnel-1.private:3</td>
<td>30.1.1.3</td>
<td>502</td>
<td>Up</td>
<td>30.1.1.3</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>20.1.2.2</td>
<td>0.0.0.0</td>
<td>None</td>
<td>Up</td>
<td>30.1.1.2</td>
<td>30.1.2.7</td>
<td>None</td>
<td>30.1.1.3</td>
<td>None</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

GRE Tunnels: 2

A:Dut-A# show gre tunnel "toce2"

GRE Tunnel Configuration Detail

<table>
<thead>
<tr>
<th>Service Id</th>
<th>500</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sap Id</td>
<td>tunnel-1.private:1</td>
</tr>
<tr>
<td>Tunnel Name</td>
<td>toce2</td>
</tr>
<tr>
<td>Description</td>
<td>None</td>
</tr>
<tr>
<td>Target Address</td>
<td>20.1.1.2</td>
</tr>
<tr>
<td>Delivery Service</td>
<td>500</td>
</tr>
<tr>
<td>Admin State</td>
<td>Up</td>
</tr>
<tr>
<td>Oper State</td>
<td>Up</td>
</tr>
<tr>
<td>Source Address</td>
<td>50.1.1.7</td>
</tr>
<tr>
<td>Oper Remote Addr</td>
<td>30.1.1.3</td>
</tr>
<tr>
<td>Remote Address</td>
<td>30.1.1.3</td>
</tr>
<tr>
<td>Backup Address</td>
<td>30.1.2.7</td>
</tr>
<tr>
<td>DSCP</td>
<td>None</td>
</tr>
<tr>
<td>Oper Flags</td>
<td>None</td>
</tr>
</tbody>
</table>

GRE Tunnel Statistics: toce2

| Errors Rx | 0 |
| Pkts Rx   | 165342804 |
| Bytes Rx  | 84986201256 |
| Key Ignored Rx | 0 |
| Seq Ignored Rx | 0 |
| Vers Unsap. Rx | 0 |
| Invalid Chksum Rx | 0 |
| Too Big Tx | 0 |
```

**Label** | **Description**
--- | ---
Invalid Chksum Rx | Incremented every time a GRE packet is dropped because the checksum is invalid.
Loops Rx | Incremented every time a GRE packet is dropped because the destination IP address of the un-encapsulated packet would cause it be re-encapsulated into the same tunnel.

**Invalid Chksum Rx**
Incremented every time a GRE packet is dropped because the checksum is invalid.

**Loops Rx**
Incremented every time a GRE packet is dropped because the destination IP address of the un-encapsulated packet would cause it be re-encapsulated into the same tunnel.
A:Dut-A# show gre tunnel count
--------------------------------------------------------------------------------
GRE Tunnels: 2
--------------------------------------------------------------------------------
ike-policy
Syntax
ike-policy ike-policy-id
ike-policy
Context show>ipsec
Description This command displays
Parameters ike-policy-id — Specifies the ID of an IKE policy entry.
   Values 1 — 2048
Sample Output
*A:ALA-48# show ipsec ike-policy 10
===============================================================================
IPsec IKE policy Configuration Detail
===============================================================================
Policy Id : 10       IKE Mode : main
DH Group : Group2   Auth Method : psk
PFS : False       FFS DH Group : Group2
Auth Algorithm : Sha1   Encr Algorithm : Aes128
ISAKMP Lifetime : 86400 IPsec Lifetime : 3600
NAT Traversal : Disabled
NAT-T Keep Alive : 0  Behind NAT Only : True
DPD : Disabled
DPD Interval : 30    DPD Max Retries : 3
Description : (Not Specified)
===============================================================================
*A:ALA-48#
security-policy
Syntax
security-policy service-id [security-policy-id]
security-policy
Context show>ipsec
Description This command displays
Parameters service-id — Specifies the service-id of the tunnel delivery service.
   Values 1 — 214748364
tsvc-name: 64 char max
security-policy-id — Specifies the IPSec security policy entry that this tunnel will use.
   Values 1 — 8192
Sample Output

*A:ALA-48>show>ipsec# security-policy 1
========================================================================
Security Policy Param Entries
========================================================================
SvcId  Security  Policy  LocalIp  RemoteIp
      PlcyId  ParamId
------------------------------------------------------------------------
1      1         1       0.0.0.0/0  0.0.0.0/0
------------------------------------------------------------------------
No. of IPsec Security Policy Param Entries: 1
========================================================================
*A:ALA-48>show>ipsec#

static-sa

Syntax static-sa
static-sa name sa-name
static-sa spi spi

Context show>ipsec

Description This command displays IPSec static-SA information.

Parameters

sa-name — Specifies the SA name.

Values 32 chars max

spi — Specifies the spi.

Values 256..16383

transform

Syntax transform [transform-id]

Context show>ipsec

Description This command displays IPSec transforms.

Parameters transform-id — Specifies an IPSec transform entry.

Values 1 — 2048

Sample Output

*A:ALA-48>config>ipsec# show ipsec transform 1
=================================================================
IPsec Transforms
=================================================================
TransformId  EspAuthAlgorithm  EspEncryptionAlgorithm
---------------------------------------------------------------
1            Sha1              Aes128
No. of IPsec Transforms: 1

*A:ALA-48>config>ipsec#

tunnel

Syntax  tunnel  ipsec-tunnel-name
tunnel

Context  show>ipsec

Description  This command displays

Parameters  ipsec-tunnel-name — Specifies the name of the tunnel up to 32 characters in length.

tunnel-template

Syntax  tunnel-template  [ipsec template identifier]

Context  show>ipsec

Description  This command displays

Parameters  ipsec template identifier — Displays an existing IPSec tunnel template ID.

Values  1 — 2048

Sample Output

*A:ALA-48>config>ipsec# show ipsec tunnel-template 1

-----------------------------------------------------------------------------------------------
IPSec Tunnel Template
-----------------------------------------------------------------------------------------------
Id  Trnsfrm1  Trnsfrm2  Trnsfrm3  Trnsfrm4  ReverseRoute  ReplayWnd
-----------------------------------------------------------------------------------------------
1   1         none      none      none      useSecurityPolicy 128
-----------------------------------------------------------------------------------------------
Number of templates: 1
-----------------------------------------------------------------------------------------------
*A:ALA-48>config>ipsec#
In This Section

This section describes how to configure the hardware for video services and some basic video services configuration concepts in support of the IPTV video applications.

Topics include:

- Video Services on page 348
  - Video Groups on page 348
  - Video SAP on page 349
  - Video Interface on page 349
  - Multicast Information Policies on page 350
  - Duplicate Stream Protection on page 352
  - Duplicate Stream Selection on page 353
  - Video Quality Monitoring on page 357
- Retransmission and Fast Channel Change on page 365
  - RET and FCC Overview on page 365
  - Multi-Service ISA Support in the IOM-3 for Video Services on page 376
- Ad Insertion on page 380
  - Local/Zoned Ad Insertion on page 380
Video Services

Video Groups

When configured in the router, ISA-MS are logically grouped into video groups for video services. A video group allows more than one video ISA to be treated as a single logical entity for a given application where the system performs a load balancing function when assigning tasks to a member of the group. All video group members are “active” members, so there is no concept of a “standby” ISA as in other ISA groups in the 7750 SR and 7450 ESS.

Video groups provide a redundancy mechanism to guard against hardware failure within a group where the system will automatically rebalance tasks to the group excluding the failed ISA. Video groups also pool the processing capacity of all the group members and will increase the application throughput because of the increased packet processing capability of the group. The buffer usage is typically identical for all members of the video group, so increasing the number of members in a group will not increase the scaling numbers for parameters bounded by available buffering, but there will still be the increase in performance gained from the pooled packet processor capacity. A video service must be enabled at the video group level before that service can be used.

A maximum of four ISA-MSs can be supported in a single video group. Note that a given video application may restrict the number of members supported in a video group to a smaller number. Refer to specific sections in this guide for video application additional information.

A maximum of four video groups are supported in a router. There is a chassis limit of eight ISA-MSs per router which constrains the number and members of video groups.

Note: ISA-MS in a single video group cannot be on the same IOM. An IOM can accommodate two ISA-MS modules provided that the ISA-MS are members of different video groups.
**Video SAP**

The video group logically interfaces to a service instance with a video Service Access Point (SAP). Like a SAP for connectivity services, the video SAP allows the assignment of an ingress and egress filter policy and QoS policy.

Note: Ingress and egress directions for the filter and QoS policy are named based on the perspective of the router which is the opposite perspective of the ISA. An “egress” policy is one that applies to traffic egressing the router and ingressing the ISA. An “ingress” policy is one that applies to traffic ingressing the router and egressing the video. Although potentially confusing, the labeling of ingress and egress for the ISA policies was chosen so that existing policies for connectivity services can be reused on the ISA unchanged.

If no filter or QoS policy is configured, the default policies are used.

One of the key attributes of a video SAP is a video group association. The video SAP’s video group assignment is what determines which video group will service on that video SAP. The video groups configuration determines what video services are available.

---

**Video Interface**

A video interface is a logical IP interface associated with a video SAP and provide the IP addressing for a video SAP.

A video interface can have up to 16 IP addresses assigned in a Layer 3 service instance. A video interface can have only one IP address assigned in a Layer 2 service instance.
Multicast Information Policies

Multicast information policies on the 7750 SR and 7450 ESS serve multiple purposes. In the context of a service with video services, the multicast information policy assigned to the service provides configuration information for the multicast channels and defines video policy elements for a video interface.

Note: This section describes the base elements of a multicast information policy in support of a video service. Specific video service features will require additional configuration in the multicast information policy which are described in the sections dedicated to the video feature.

Multicast information policies are named hierarchically structured policies composed of channel bundles which contain channels which contain source-overrides.

- Bundles are assigned a name and contain a collection of channels. Attributes not defined for a named bundle are inherited from the special default bundle named “default”.

```
*A:ALA-48configmcast-mgmtmcast-info-plcy# info
----------------------------------------------
bundle "default" create
exit
----------------------------------------------
*A:ALA-48configmcast-mgmtmcast-info-plcy#
```

- Channels are ranges of IP multicast address identified by a start IP multicast address (G_{start}) and optional end IP multicast address (G_{end}), so the channels encompasses (*,G_{start}) through (*,G_{end}). A channel attribute is inherited from its bundle unless the attribute is explicitly assigned in which case the channel attribute takes precedence.

- A source-override within a channel are IP multicast addresses within the channel with a specific source IP address (S_{override}), so the source-override encompass (S_{override},G_{start}) through (S_{override},G_{end}). A source-override attribute is inherited from its channel unless the attribute is explicitly assigned in the source-override channel in which case the source-override channel attribute takes precedence.

For a given IP multicast channel (*,G) or (S,G), the most specific policy element in the hierarchy that matches applies to that channel.

A multicast information policy is assigned to a service instance. For video services, the multicast information policy assigned to the service determines the video group for a given IP multicast channel. When a channel is assigned to a video group, the channel is sent to the video group for buffering and/or processing as appropriate depending on the video services enabled on the video group. If no video group is assigned to a given channel, the channel will still be distributed within the service instance, but no video services will be available for that channel.
In addition to bundles, channels and source-overrides, multicast information policies also include video policies. Video policies define attributes for the video interfaces within the service instance.

Note: Video policy attributes are specific to the video feature and will be covered in detail in the applicable video feature section. Video policies are mentioned here because they are an element of the multicast information policy and provide the link to configuration for a video interface.
Duplicate Stream Protection

While H-RET can protect against minor amounts of packet loss, it is limited in the number of packets that can be recovered (currently 32). This can be from approximately 125ms of a 3Mbps stream to only 18ms for a 20Mbps stream. These times are short for a network reconvergence event which will typically be in the order of 300-1200ms. Further, retransmission will cause incremental bandwidth spikes in the network as the lost packets are sent to the client as quickly as possible.

Rather than invoke a retransmission event to protect against network interruption or reconvergence, it is often more efficient to protect the stream via an alternate transmission path. This can be a separate physical interface, transmission link, system or even technology.

Duplicate-stream protection allows an operator to split a single multicast stream (single S,G and common SSRC) into two different transmission paths that may have different transmission characteristics (latency/jitter). Rather than select one stream for retransmission to the client the Duplicate Stream protection feature evaluates each stream packet-by-packet, selecting the packet that first arrives (and is valid) for retransmission.

A circular buffer is used for duplicate-stream protection which incorporates both packet-by-packet selection (based on RTP sequence number/timestamp and SSRC) and a re-ordering function whereby any out-of-sequence packets will be placed into the buffer in order, thus creating a corrected, in-order stream.

Similar to the H-RET re-sequencing feature playout rate is a function in ingest rate, however because the two streams may be delayed between one-another a few assumptions are made:

- The first arriving packet is always put into the buffer, allowing for the backup medium to wander in terms of latency and jitter.
- Because the source is the same, the rate at which a packet is put into the buffer (from either stream) can be assumed to be the normal bitrate.

The output RTP stream is always maintained in-sequence and the playout speed is user-controlled. Either with constant-delay (i.e., packet ingress time + 500ms = packet egress time) or can be a moving window average to smooth jitter that may occur between packets or the two contributing streams. The operator can specify the size of this window where zero (0) is a constant-delay.

The buffer size is similarly configurable and is the higher of the inter-stream phase (i.e., one stream ahead of another) or the expected jitter.


Duplicate Stream Selection

Stream Identification

Stream selection is a simple selection algorithm that is applicable to any number of input streams. It is a prerequisite for stream selection that RTPv2 encapsulation be used in UDP.

Each service is identified by multicast source, group/destination address and current synchronization source (SSRC). Once this has been identified, the ISA monitors its ingress for:

- Traffic with a DA of the multicast group, or;
- Traffic with a DA of the ISA (unicast)

Traffic is further checked as having RTP-in-UDP payload, RTP version 2.

The SSRC of each incoming RTP packet is learned as unique sources. Only one SSRC is supported for each stream, however as SSRC may change during abnormal situations (such as encoder failover), it can be updated.

A SSRC can only be updated when a Loss of Transport (LoT) occurs, as other duplicate streams (with the original SSRC) may still be operational. When an LoT occurs the SSRC is deleted, the buffers are purged and the RTP sequence counters are reset. The SSRC will be extracted from the next valid RTP packet and the sequence will start over.

Note that individual streams are not tracked by the ISA. There may be one, two, or ten duplicate streams, the number is of no consequence to the selection algorithm (however bandwidth and/or video quality monitoring (VQM) may be impacted). Irrespective of the number of duplicate streams, one RTP packet is selected for insertion into the video ISA buffer. Once a packet is selected the RTP sequence counter is incremented and any further RTP packets received by the ISA with the previous sequence number are discarded.

In summary, duplicate stream selection is a FIFO algorithm for RTP packet selection, this is considered optimal because:

- All stream sources are identical, thus for any given sequence number the payload should also be identical.
- Most bit errors should be detected by the CRC-32 algorithm applied to Ethernet, SDH, ATM, etc. These devices will typically discard frames where bit errors occur with the net result being the video ISA will receive a bit error-free stream (though packet loss may/does occur).
- UDP checksum in verified by the video ISA (after input VQM) and any failures result in a silent discard of the packet.
Initial Sequence Identification

When a service is defined and is enabled (no shutdown), the video ISA will monitor for valid RTP packets and on first receipt of a valid RTP packet learn the following information:

- SSRC
- Sequence number
- Timestamp (as timestamp is profile-specific, MPEG2-TS are assumed)

The packet will be inserted into the video ISA playout buffer associated with that particular service and playout when directed (playout algorithm).

Packet Selection

For each valid RTP packet received for a given service will be inserted into the buffer if there is no existing RTP packet that matches the sequence number. Because sequence number and timestamp discontinuities may occur the video ISA makes a limited attempt at validating either as they are not required for MPEG. The video ISA code adopts a philosophy that for the most part sequence number and timestamp increment correctly, but should they prove to be non-contiguous, the packet selection algorithm adapts.

Duplicate packets are detected by sequence number (or timestamp unless M-bit reset it), so should a packet already exist in the buffer with the same sequence number as one received (or one recently played out) it will be discarded. For the purpose of determining recent playout if an incoming sequence number is within 6.25% (- 4096) the packet is considered late and is discarded.

In a multi programme transport stream (MPTS) timestamp is set uniquely for every RTP packet, this is because any RTP packet many contain a number of multiplexed elementary streams. As a result playout is based on the embedded timestamp in each RTP packet. In a single programme transport stream the inverse occurs, many RTP packets can share the same timestamp as it is referenced from the start of picture (and a picture can span many RTP packets). As a SPTS does not contain audio its application is limited to content production and so only MPTS are supported.

Timestamp discontinuities do occur and are normally represented with the Marker bit (M) being set.

Playout time is determined by an internal playout timestamp. The playout timestamp is set independently from the actual timestamp in the packet. The recovered clock is used to determine expected timestamp for every incoming RTP packet.

When a packet is received it is first compared to existing packets in the buffer based on sequence number (assuming here that a stream may be delay hundreds of milliseconds by a backup path yet still be valid); only if this packet is determined to be new RTP packet eligible for buffer insertion will jitter tolerance be evaluated. If jitter tolerance is exceeded then a timestamp discontinuity is
assumed and instead of setting playout timestamp based on the contained RTP timestamp, the actual received time (offset by playout-buffer) is set for the RTP packet playout timestamp.

In normal operation clock is recovered from the timestamp field in the RTP header, is offset by the playout buffer configuration parameter and used to schedule playout of the packet. The playout clock is synchronized with the sender by using an adaptive clock recovery algorithm to correct for wander.

Algorithm summary

- Is the service marked LoT — If a loss of transport occurred, purge the buffer and reset all counters/timers.
- If the service is UP, check the RTP packet sequence number. Compare to sequence numbers contained in the buffer. If no match then check last played sequence number. If the sequence number of this packet is between last played and last played + 4096 then consider this packet late and discard.
- Check the expected timestamp recovered clock value and compare to RTP timestamp: If the expected timestamp is (-ve)jitter tolerance<timestamp<(+ve)jitter tolerance then the packet is admitted to the buffer with a playout timestamp per the embedded RTP timestamp. If jitter tolerance is not maintained this marks a discontinuity event. Set playout timestamp to current clock + playout buffer and enqueue.

Clock Recovery

RFC 2250, *RTP Payload Format for MPEG1/MPEG2 Video*, defines the timestamp format for MPEG2 video streams (which may carry H.264 video): a 90kHz clock referenced to the PCR. Each ingest RTP packet has it’s timestamp inspected and it is used in an adaptive clock recovery algorithm. Importantly, these adjustments occur on ingress (not on playout). This serves as a long-term, stable, ingress stream recovered clock.

The 90kHz ingress stream recovered clock is adjusted for each service to account for the encoder’s reference clock/difference between the clock in the 7750 SR. This input timestamp is derived from the same RTP packet that is inserted into the buffer, and thus may be subjected to significant jitter. The clock adjustment algorithm must only adjust clock in extremely small increments (in the order of microseconds) over a very long sample period (not bitrate) of at least 30 minutes.
Playout

Playout is the process of regenerating the stream based on playout timestamp.

For each service the operator defines a fixed playout buffer. This serves as an exact offset to the ingress stream recovered clock and serves as playout time for the video ISA. Because timestamp is used for buffer playout, CBR, capped VBR and VBR streams are all supported without pre-configuration. The playout buffer mechanism effectively removes network-induced jitter and restores the output to the rate of the original encoder.

Loss of Transport

In the circumstance that the playout buffer is emptied an LoT is indicated. The video ISA will reset playout timestamp, clock, sequence number, etc., on this event and await the next valid RTP packet for this service.
Video Quality Monitoring

The following terminology is used in this section:

- **TNC**: Technically non-conformant
- **QoS**: Quality of Service
- **POA**: Program Off Air
- **Impairment event** — A trap/alarm that an impairment event is detected and is termed as tnc. An impaired event is said to have occurred if:
  - Continuity counter errors were detected.
  - If PAT/PMT/PCR pids were not present in the video stream for a time period equal to or greater than the configured tnc value in the respective alarm.
    - The default value of the impaired threshold in terms of milli second is:
      - PAT: 100ms
      - PCR: 100ms
      - PMT: 400ms
    - If unreferenced PID is seen in the video stream which has not been referred in the PMT table.
- **Impaired seconds** — The number of seconds an impaired event was detected.
- **Degraded event** — A trap/alarm that a degraded event is detected and is termed as QoS. A degraded event is said to have occurred if:
  - PAT/PMT Syntax error occurs in that second.
  - Absence of PAT/PMT/PCR pids in the video stream for a time period equal to or greater than the configured qos value in their respective alarms.
    - The default value of the degraded threshold in terms of milli second is:
      - PAT: 200ms
      - PCR: 200ms
      - PMT: 800ms
- **Degraded seconds** — The number of seconds an degraded event was detected.
- **Error event** — A trap/alarm that an error event is detected and is termed as POA.
• An errored event has occurred if:
  → If sync loss error has occurred for that particular second. A sync loss is said to have occurred if there are more than 1 consecutive sync byte errors are seen in the stream.
  → Absence of PAT/PMT/PCR PIDs in the video stream for a time period equal to or greater than the configured poa value.

The default value of the degraded threshold in terms of millisecond is:
  PAT : 500ms
  PCR : 500ms
  PMT : 2000ms

→ Traffic loss has occurred for that particular second.

→ Transport error indicator or TEI indicator is set in the transport stream packet header for that particular second in the video stream.

• Errored seconds — The number of seconds an errored event was detected.
• Good seconds — The number of seconds where we do not see any impaired, degraded or errored events.

Pid Stats :

• PID: Displays the value of the pid.
• Is PCR PID : Takes a value Yes/No. If yes, then it indicates that the pid is the PCR PID.
• TEI Err Sec : Counts the number of seconds TEI was set for that particular PID.
• Absent Err Secs: The number of seconds for which the PID was not seen for a particular interval of time which is decided by the alarms set for the Non-Vid PID Absent and Video PID Absent.
• PID bitrate: Is calculated by counting the number of times the pid occurred in the last second x 188 x 8.
  \[ 188 = \text{TS packet size} \]
  \[ 8 = \text{Number of bits in a byte} \]
• CC Err Secs: Number of seconds continuity counter errors were seen for that particular PID in the stream.
• PID Type: Specifies that the PID is either video, audio, PAT, PMT, or PCR.
• MPEG Stream Type: If the PID is of video or audio this field informs us about the way the video and audio is encoded.

For example:
  → For video : H.264 or Mpeg2 (Only the decimal equivalent defined by the MPEG standard is displayed and not the string)
  → For Audio : AC-3 or Mpeg-2 (Only the decimal equivalent defined by the MPEG standard is displayed and not the string)
Interval Stats

- Except the PID stats all other stats explained above have interval stats. Information can be obtained about stream status was in the last 1 minute, 5 minute and 15 minute.

MDI - Media Delivery Index (RFC 4445, *A Proposed Media Delivery Index (MDI)*)

- Delay Factor (RFC 4445) — The delay factor is a value which indicates the minimum amount of time a STB buffers to resolve network jitter (i.e., it is the minimum STB buffer depth in ms). RTP timestamp will be used as the definitive time indicator (the notional drain rate).
- Loss Rate (RFC 4445) — The Media Loss Rate is the number of media (Transport Stream) packets lost over a certain time interval. This is reported in TS/sec. Each RTP packet lost is assumed to have 7 TS packets lost.
- In absence of traffic MDI values will be reported as N/A . These stats are reported over current (current second), 1 minute, 5 minutes and 15 minutes intervals

In many instances IPTV operators are unable to identify the cause of visual impairments which are present in almost every video distribution network because the IPTV network has so many moving parts While head end transport-stream monitoring; full reference video analysis (comparing the source content to the encoded output), and; STB probes allow an operator to establish whether the contribution source, the encoder, or the network is the problem the network is a very complex thing.

Operators can use another measurement point in the network, just prior to the last mile such that network faults can be characterized as being between the head end and last mile (transport) or in the last-mile itself.

The multicast video quality monitoring solution provides an inspection point for the multicast video stream that is combined with other analysis methods to create a full view of video issues and help troubleshoot the part of the network causing the issue.

Video quality monitoring is one part of a video assurance program and is combined with:

- TS analysis on the encoder output (to detect encoder errors);
- Full-reference PSNR and PQR on the encoder output (to detect over-encoding, noise and other contribution or encoding artefacts)
- STB reporting (such as packet-loss, RET events, packet errors) from the entire STB population
- STB probes performing full-reference monitoring (against test streams)
- STB probes performing channel-change times, estimated PSNR, etc

Multicast video monitoring within the network can be positioned as complementary to STB reporting and head end analysis, and but should not attempt to perform either of these functions.
Because the network node is not capable of decrypting a MPEG transport stream is primarily used to identify correctable and un-correctable network errors, correlate them with network events (i.e., routing reconvergence, interface failure, etc) and provide summary reports and alarms.

For operators who do not have existing STB probes or reporting, a network-based VQM solution can provide insight into quality issues the network may be contributing to, possibly reducing the amount of STB probe investment that is needed. (i.e., both probes and the 7750 VQM reports many of the same issues in terms of picture quality, fewer probes are needed to test channel change delay, etc).

The metrics which VQM can report are based on the use of RTP streams which provide per-packet sequencing and an indication of picture type. These two parameters along with measured bitrate allow VQM to produce estimated MOSv scores for both stream ingress (uncorrected) and stream egress (corrected) outputs.

Reportable metrics include:

- Relevant SCTE-143 error counters
  - PAT
  - PMT
  - PCR
  - Transport errors, etc
- ETSI TR 101 290
  - PID
  - SI repetition
  - Degraded blocks/intervals, etc
- MDI (RFC 4445)
- RTP Measurements (RFC 3357, One-way Loss Pattern Sample Metrics)
- Forwarded and impaired I-/B-/P-frame counts
- GOP length
- Video/audio/stream bitrate

These metrics are collected per stream and have relevant parameters (such as profile and PIDs) pre-defined, these will be collected into a so-called stream ID. Reports (containing numeric metrics) and alarms (log, SNMP or syslog) can be generated.
For each group, reports contain:

- Stream ID (S,G / SSRC)
  - Stream A (ingress)
    - Statistics
  - Stream B (ingress)
    - Statistics
  - Output
    - Statistics

Reports are non-realtime and are compiled into an XML format for FTP extraction with a resolution of less than 5 minutes.

Event alarms are reported by log, syslog or SNMP (existing log interface).

VQM is an optional module available on the input side, or output side of the video ISA. On input, it is applied prior to ad-insertion, H-RET, and duplicate stream protection, conversely when on the output side it is applied only to multicast streams after ad-insertion, H-RET and duplicate stream protection.

Because of the large number of channels and the nature of measuring input and output sides, VQM is highly reliant on the use of RTP extensions to provide relevant transmission metrics to the VQM analysis module. In a typical head end a multicast stream will be scrambled to encrypt its video and/or audio. When this encryption occurs, it is typical for the entire payload of the transport stream (for the nominated PID) to be completely scrambled. The consequence of such is that the video and audio PES headers, which reveal much about the picture and timing information, are unavailable to the VQM program.

VQM utilizes intelligent RTP re-wrapping. RTP re-wrapping is a prerequisite for ad insertion and Fast Channel Change (FCC) and involves marking packets before encryption based on the picture type (most importantly, the start of the I frame of IDR frame in H.264).

The Alcatel-Lucent VSA as currently defined, re-multiplexes each transport stream into a new RTP packet. By doing so it allows the separation of different picture types into their own respective RTP packets, and the separation of audio packets from video packets to allow different synchronisation in events of FCC. In effect, it pulls the elementary streams back into their component forms while retaining the syntax and structure of the MPTS.

For information about Alcatel-Lucent VSAs, refer to the 7750 SR OS System Management Guide.

Meanwhile, additional information can be made available, prior to scrambling, of the picture information for quality analysis. The quality analysis performed by the VQM module emphasizes impairments caused by network issues and transport stream syntax given the relative proximity of the router to the customer.
When the video ISA is deployed alongside the ALU VSA re-wraper a custom RTP header extension is sent with each RTP packet.

<table>
<thead>
<tr>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>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</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| +---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+-------------
VoIP/Video/Teleconferencing Performance Measurements

The feature provides ability to measure and provide statistics to allow reporting on voice and video quality for VoIP and teleconferencing (A/V) applications. A sampled deployment is shown in the picture below (Figure 24). Although a distributed model is shown, a hub-and-spoke model, with AA-ISA deployed only on one side of the traffic flow, is also supported.

![Figure 24: Voice/Video Monitoring Deployment Example](image)

Because of network-based AA, the operator has an ability to monitor voice, video, teleconferencing applications for a given AA subscriber regardless of the type of that subscriber (a residential subscriber vs. a user of a business VPN service). AA-ISA monitors UDP/RTP/RTCP/SDP headers for each initiated call/application session (sampling may be provided – although, it is expected that a sampling rate will be smaller than that of TCP-applications due to the nature of the voice/video applications – longer lasting and smaller number of sessions/calls per subscriber). AA ISA gathers statistics and computes MOS-scores/R-factor results per each call/application session. At the end of a call (/application session closure), AA-ISA sends the statistics and computed scores to a Cflowd collector (the Cflowd infrastructure was introduced for TCP-performance but modified to carry voice/video specific data is used). The collector summarizes and presents the results to the operator/end user.
Mean Opinion Score (MOS) Performance Measurements Solution Architecture

AA-ISA integrates a third party MOS software stack to perform VoIP and video MOS measurements. This software provides:

- Call quality analysis using optimized ITU-T G.107
- Measurements of perceptual effects of burst packet loss and recency using ETSI TS 101 329-5 Annex E Extensions
- Measurements and analysis of RTCP XR (RFC3611) VoIP metrics payloads.

AA software monitors the associated SDP channel and passes codec information (when available) to the subsystem which monitors VoIP. The video bearer channels traffic generates a wide variety of A/V performance metrics such as:

- Call quality metrics
  - Listening and conversational quality MOS scores – MOS-LQ, MOS-CQ
  - Listening and conversational quality R-factors – R-LQ, R-CQ
  - Estimated PESQ scores – MOS-PQ
  - Separate R-factors for burst and gap conditions – R-Burst, R-Gap
  - Video MOS-V and Audio MOS-A
  - Video Transmission Quality - VSTQ
- Video stream metrics
  - Good and impaired I, B, P, SI, SP frame counts
  - Automatic detection of GoP structure and other key video stream attributes such as image size, bit rate, codec type
- Transport (IP/RTP) metrics
  - Packet loss rate, packet discard rate, burst/gap loss rates
  - Packet delay variation/ jitter
- Degradation factors
  - degradation due to loss, jitter, codec, delay, signal level, noise level, echo, recency

Once a flow terminates, AA software retrieve the flow MOS parameters from the subsystems, formats the info into a Cflowd record and forwards the record to a configured Cflowd collector (RAM).

RAM collects Cflowd records, summarizes these records using route of interest information (source/destinations). In addition, RAM provides the user with statistics (min/max/avg values) for the different performance parameters that are summarized.
Retransmission and Fast Channel Change

RET and FCC Overview

The following sections provide an overview of RET and FCC.

Retransmission

Retransmission (RET) for RTP (RFC 3550, *RTP: A Transport Protocol for Real-Time Applications*) is based on a client/server model where the client sends negative acknowledgments (NACKs) using Real-time Transport Control Protocol (RTCP) (RFC 4585, *Extended RTP Profile for Real-time Transport Control Protocol (RTCP)-Based Feedback (RTP/AVPF)*) to a RET server when the client detects missing sequence numbers in the RTP stream. The RET server which caches the RTP stream, for example in a circular buffer, detects missing sequence numbers in the replies to the NACKs by resending the missing RTP packets as illustrated in Figure 25.

![Figure 25: RET Server Retransmission of a Missing Frame](image)

The format of the reply must be agreed upon by the RET client and server and can be an exact copy (Payload Type 33 as defined in RFC 3551, *RTP Profile for Audio and Video Conferences*).
Retransmission and Fast Channel Change

with Minimal Control) or sent with a different Payload Type using an encapsulating RET header format (RFC 4588, RTP Retransmission Payload Format).

RET has been defined in standards organizations by the IETF in the above-noted RFCs and Digital Video Broadcasting (DVB) in “Digital Video Broadcasting (DVB); Transport of MPEG-2 TS Based DVB Services over IP Based Networks (DVB-IPTV Phase 1.4)” which describes the STB standards.

STBs that have a port of the Alcatel-Lucent RET/FCC Client SDK are an example of a standards-compliant RET Client implementation.

---

Fast Channel Change (FCC)

FCC is an Alcatel-Lucent method based on a client/server model for providing fast channel changes on multicast IPTV networks distributed over RTP. During a fast channel change, the FCC client initiates a unicast FCC session with the FCC server where the FCC server caches the video stream and sends the channel stream to the FCC client starting at the beginning of a Group of Pictures (GOP). Beginning at a GOP in the past minimizes the visual channel transition on the client/STB, but the FCC unicast stream must be sent at an accelerated rate in the time domain to allow the unicast stream to catch up to the main multicast stream, at which point, the FCC server signals to the client to join the main RTP stream.

Figure 26 illustrates the FCC client and server communication.
There are two techniques for compressing the FCC unicast stream in time to allow the unicast session to catch up to the multicast stream: bursting and denting. When bursting, the stream is sent at a rate faster than multicast stream, for example, the stream can be “bursted” at 130% (or 30% over the nominal) multicast rate. “Denting” is a technique where less important video frames are dropped by the FCC server and not sent to the FCC client. Hybrid mode combines bursting and denting.

Bursting is illustrated in Figure 27 and denting is illustrated in Figure 28.
Figure 27: FCC Bursting Sent Faster Than Nominal Rate

Figure 28: FCC Denting Removing Less Important Frames
When the unicast session has caught up to the multicast session, the FCC server signals to the FCC client to join the main multicast stream. The FCC server will then send the unicast session at a lower rate called the “handover” rate until the unicast session is terminated.

Note that the FCC server functionality requires the Alcatel-Lucent 5910 Video Services Appliance (VSA) Re-Wrapper which is used to encapsulate and condition the multicast channel streams into RTP, adding important information in the RTP extension header. Also, the ISA FCC server requires an STB FCC client based on the Alcatel-Lucent FCC/RET Client SDK.
Retransmission Client

The ISA RET client is used in hierarchical RET deployments and performs upstream corrections for missing packets in the RTP multicast stream to ensure that the RET server has all the packets for the stream.

The RET client is supported within a VPLS, IES or VPRN service context as applicable to the platform. The RET client source address is explicitly assigned. In a VPLS, the RET client IP appears to be an IP host within the service, and like a host, the RET client is also configured with a gateway IP address to provide a default route to reach the upstream RET server.

Whenever the RET client receives a retransmission from an upstream RET server, the replies are sent downstream as multicast in the multicast service using Payload Type 33 which is the Payload Type for an original stream.

Whether the RET client is active for a given multicast channel is defined in the multicast information policy where channels are defined. The channel configuration for the RET client within the policy is an explicit enable/disable of the RET client and the IP address and UDP port for the upstream RET server for the channel.

The ISA RET server supports the network model where there are separate service instances for unicast and multicast traffic that are cross-connected and multicast replicated downstream in the network, for example, where an access node provides the multicast service cross connect and replication at the last mile. If there are separate multicast and unicast service instances, the multicast service instance must be configured in the unicast service, and the unicast and multicast services must use the same multicast information policy.
Retransmission Server

The ISA RET server is supported within a VPLS, IES or VPRN service context as applicable to the platform.

Whether the RET server is active for a given multicast channel is defined in the multicast information policy where channels are defined. The channel configuration for the RET server within the policy is an explicit enable/disable of the local RET server (that is, whether the channel should be buffered), the RET buffer size for the channel in the ISA and a channel type (Picture-in-Picture (PIP), Standard Definition (SD) or High Definition (HD)). The RET buffer should be large enough to account for the round trip delay in the network; typically, a few hundred milliseconds is sufficient.

In a VPLS service, a single IP address is assigned to the RET server, and it acts like an IP host within the service.

In an IES or VPRN service, up to 16 IP addresses can be assigned to a video interface.

The video policy within the multicast information policy defines the characteristics for the how the RET server should respond to NACKs received on an IP address. The different characteristics defined in a RET server “profile” are for each channel type (PIP, SD and HD):

- Enable/disable for the RET server (that is, whether requests should be serviced or dropped).
- The RET rate (as a percentage of the nominal channel rate).

Typically, RET replies are sent below line rate because most dropped packets occur in the last mile and sending RET replies at a high rate may compound any last mile drop issues.

The IP address(es) of the RET server is(are) defined in the unicast service instance, whereas the UDP port for the RET server is defined in the “default” bundle in the multicast information policy. The same UDP port is used for all RET server IP addresses that use the particular multicast information policy.

The ISA RET server supports the network model where there are separate service instances for unicast and multicast traffic that are cross-connected and multicast replicated downstream in the network. If there are separate multicast and unicast service instances, the unicast and multicast services must use the same multicast information policy.
Fast Channel Change Server

The ISA FCC server is supported within a VPLS, IES or VPRN service context as applicable to the platform. VPRN services are not supported on the 7450 ESS.

Whether the FCC server is active for a given multicast channel is defined in the multicast information policy where channels are defined. The channel configuration for the FCC server within the policy is an explicit enable/disable of the local FCC server (that is, whether the channel should be buffered) and a channel type PIP, SD or HD. When FCC is enabled, three (3) GOPs are stored in the buffer. the channel also defines an optional fcc tuning parameter called the fcc Minimum Duration which is used by the FCC server to determine which GOP to start the FCC unicast session. If there are too few frames of the current GOP stored in the fcc server buffer (based on number of milliseconds of buffering), the FCC server will start the FCC session from the previous GOP.

In a VPLS service, a single IP address is assigned to the FCC server, and it acts like a IP host within the service.

In an IES or VPRN service, up to 16 IP addresses can be assigned to a video interface.

The Video Policy within the multicast information policy defines the characteristics for the how the FCC server should respond to FCC requests received on an IP address. The different characteristics defined in an FCC server “profile” are for each channel type (PIP, SD and HD):

- Enable/disable for the FCC server (for example, should the requests be serviced or dropped).
- The FCC mode: burst, dent or hybrid.
- The burst rate (as a percentage above the nominal channel rate) for PIP, SD and HD channel types.
- The multicast handover rate (as a percentage of the nominal channel rate) used by the server after it has signaled the client to join the main multicast channel.

Different FCC rates are allowed for each of the channel types because the channel types have different nominal bandwidths. For example, the last mile may only be able to reliably send a 25% burst (above nominal) for HD whereas the equivalent bit rate for SD is a 75% burst. The profiles are designed to provide flexibility.

The IP address of the FCC server is defined in the unicast service instance, whereas the UDP port for the FCC server is defined in the “default” bundle in the multicast information policy. The same UDP port is used for all FCC server IP addresses that use the particular multicast information policy.

The ISA FCC server supports the network model where there are separate service instances for unicast and multicast traffic that are cross-connected and multicast replicated downstream in the
network. If there are separate multicast and unicast service instances, the unicast and multicast services must use the same multicast information policy.

Logging and Accounting for RET and FCC

In previous releases, logging and statistics were maintained for active sessions (RET and FCC). This feature now provides more permanent logging, statistics and accounting for:

- RET Server sessions stats
- FCC session stats
- ADI events

RET Server Session Stats

For RET Server Stats, the RET session table entries will be sampled and periodically written to XML accounting records.

The basic framework is (requiring a CLI and perhaps some additional tuning) is:

- Session statistics will be written to a record in an XML file on a periodic basis with the sample period being 5 minutes or longer.
- Session statistics are written to a record when a) the session is removed from the session table, b) if the session is exists for more than two write periods.
- All statistics will be the total values (that is, not incremental values across sampling periods).
RET and FCC Server Concurrency

Even though the previous sections discussed the RET server and FCC server as separate entities, the ISA can support RET and FCC servers at the same service at the same time. As such, the configuration commands and operational commands for the services are intermingled. If both the RET server and FCC server are enabled for a given channel, a single buffer is used for caching of the channel.

A maximum bandwidth limit for all server requests can be defined for a given “subscriber” which is equated with the source IP address. Before an ISA server processes a request, the ISA calculates the bandwidth to the subscriber required, and will drop the request if the subscriber bandwidth limit will be exceeded.

The ISA services RET and FCC requests on a first in, first out (FIFO) basis. Before servicing any request, the ISA calculates whether its egress bandwidth can handle the request. If there is insufficient egress bandwidth to handle the service request, the request is dropped. Near the ISA’s egress limits, RET requests will generally continue to be serviced whereas FCC requests will be dropped because RET sessions are generally a fairly small percentage of the nominal rate and FCC sessions are slightly below to above the nominal channel rate.
Prerequisites and Restrictions

This section summarizes some key prerequisites and restrictions for the RET client, RET server and FCC server.

- Both RET and FCC require RTP as the transport stream protocol.
- FCC requires the Alcatel-Lucent 5910 VSA Re-Wrapper.
- FCC requires an implementation of the Alcatel-Lucent 5910 STB Client.
- The multicast information policies must be the same on multicast and unicast services which are cross connected downstream.
- Support for up to four ISA-MSs in a video group
- Only a single IP address and profile are supported within a VPLS service for RET or FCC, so only a single Profile can be supported in a VPLS service.
- Up to 16 IP addresses can be configured for a Layer 3 service video interface (IES or VPRN) with each supporting a distinct profile.
- There can be a maximum of 32 IP addresses across all Layer 3 service video interfaces per chassis.
Multi-Service ISA Support in the IOM-3 for Video Services

In previous releases, the Multi-Service ISA was supported in the iom-20g-b and the iom2-20g for video services. Now, this feature provides support for the Multi-Service ISA when installed in an iom3-xp card on both the 7450 ESS and the 7750 SR.

Prioritization Mechanism for RET vs. FCC

In previous releases, RET and FCC requests are processed with the same priority. Since RET generally has a more direct impact on a subscriber’s “quality of experience”, service providers are prioritizing RET as a feature over FCC, and for those that want to implement both, the preference is to have a mechanism to prioritize RET over FCC when there is contention for resources.

Now, this feature provides a mechanism to reserve an explicit amount of egress bandwidth for RET for all the ISAs within an video group. If the amount of egress bandwidth is less than the reserved amount, FCC requests are discarded and only RET requests processed. The bandwidth will need to be dynamically adjusted per ISA within the video group if ISAs become operational/non-operational within the group.
Alcatel-Lucent in Portugal has developed a network management application that does a statistical analysis of retransmissions to analyze the video quality. The following are existing MIB entries.

- TmnxVdoSessionEntry ::= SEQUENCE {
  - tmnxVdoSessionSourceAddrType InetAddressType,
  - tmnxVdoSessionSourceAddr InetAddress
  - tmnxVdoSessionSourcePort InetPortNumber,
  - tmnxVdoSessionSSRCId Counter32,
  - tmnxVdoSessionUpTime Unsigned32,
  - tmnxVdoSessionExpireTime Unsigned32,
  - tmnxVdoSessionCName TNamedItem,
  - tmnxVdoSessionDestAddrType InetAddressType,
  - tmnxVdoSessionDestAddr InetAddress,
  - tmnxVdoSessionRxFCCRequests Counter32,
  - tmnxVdoSessionTxFCCReplies Counter32,
  - tmnxVdoSessionTxFCCPackets Counter32,
  - tmnxVdoSessionTxFCCOctets Counter32,
  - tmnxVdoSessionRxRTRequests Counter32,
  - tmnxVdoSessionTxRTReplies Counter32,
  - tmnxVdoSessionTxRTPackets Counter32,
  - tmnxVdoSessionTxRTOctets Counter32
}

The following are new entries:

- Total number of sequences of 10 — total sequences of 2 to 10 lost packets
- Total number of sequences of 20 — total sequences of 11 to 20 lost packets
- Total number of sequences of 30 — total sequences of 21 to 30 lost packets
- Total number of sequences of 40 — total sequences of 31 to 40 lost packets
- Total number of sequences of more — total sequences of 41 or more lost packets
RETRANSMISSION AND FAST CHANNEL CHANGE

RET Server Multicast Tuning Parameters

Downstream RET requests are responded to using multicast when there are a number of identical RET requests with the assumption that there was a loss in the network that affected a number of clients. In this instance, the retransmitted frames will be sent as Payload Type 33 as original packets and not in the RFC 4588, *RTP Retransmission Payload Format*, retransmission format.

The `rt-mcast-reply` command can tune the RET server as to when to use multicast to reply to RET requests have the option to disable multicast responses.
FCC Features

FCC Hybrid Mode Support

There are three modes of operation supported for FCC:

- In burst mode, the unicast FCC traffic is sent faster than nominal rate (bursted above nominal).
- In dent mode, packets are dropped from the unicast FCC stream based on a defined threshold for markings added to the packet that indicate the importance of the packet to the audio/video stream added by the rewrapper.
- Hybrid mode combines both bursting and denting.
Ad Insertion

Local/Zoned Ad Insertion

Transport Stream Ad Splicing

Alcatel-Lucent’s Local/Zoned ADI feature allows a 7750 SR with the ISA-MS (the “splicer”) to perform ad splicing in an MSTV environment. The splicer is a post-A server transport stream (TS) splicer and can splice into encrypted or unencrypted transport streams. The splicer is positioned between the A-server and the D-server. Figure 29 shows an ad insertion model displaying components.

The ad insertion process is initiated when the splicer detects the SCTE 35 cue signal that identifies the upcoming start and end of the advertising time slot. The splicer communicates with the ad server using SCTE 30 standard messaging and will be instructed by the ad server:

- To take advantage of an ad insertion opportunity or avail and
- Determine the ad to be spliced into the main stream, if applicable.

The ad servers must be configured for ad content to match encoder configurations for video/audio streams. The ad server sends the ad stream to the ad splicer and the ad splicer will switch it into the main stream as dictated by the digital splice points (Figure 30). The ad splicer can splice multiple ads into multiple channels simultaneously.
Note that IPTV encryption and Digital Rights Management (DRM) can be applied to the transport stream payload but not to the transport stream (TS) header which allows a TS splicer to splice into encrypted streams, although the spliced ad content will in all cases be unencrypted. TS splicing does not put any requirements on the middleware platform as ad insertion will be outside the middleware’s knowledge and control.

The Figure 32 depicts a TS flow with various MUXed elementary streams (ES) identified by a unique Packet Identifier (PID). The Program Map Table (PMT) is used as the legend to map PID to elementary streams. The digital cue points are also identified by separate unique PID also defined in the PMT that is used by the TS splicer to know when to splice-in and splice-out of the stream. It is important to note that the only important thing that a TS splicer needs are the headers of the TS packets, and the underlying payload of each ES is not needed. This gives the splicer flexibility and makes it agnostic to the ES payload types.
Figure 32: Transport Stream Flow Example
Ad Zones

Within the splicer, zones are created by taking an ingress main channel multicast group, for example (*,G) or (S,G), and creating one or more egress “zone channels” on distinct source-specific multicast (SSM) groups (S1,G1), (S2,G2), etc. Up to 16 zones can be configured for each ingress multicast channel. The group multicast address for the zone channels need not be unique and can actually be the same as the ingress channel, but the SSM sources for the zone channels must be distinct.

Within SCTE 30, the main channel and zone channel are identified by an ASCII string name. These names must be unique and will be used when the splicer communicates with the ad server.

The input stream can be depicted through the following semantics diagram.

CHANNE1 \(\rightarrow\) CHANNEL1_North \((S1, G1)\)
(S, G) \(\rightarrow\) CHANNEL1_South \((S2, G2)\)
\(\rightarrow\) CHANNEL1_East \((S3, G3)\)
\(\rightarrow\) CHANNEL1_West \((S4, G4)\)
\(\rightarrow\) CHANNEL1_Central \((S5, G5)\)

where \((S,G)\) is the input main channel stream mapping into five \((5)\) \((Sx, Gx)\) which are zone channel streams.

\(S1..S16\) must be IP addresses in the video interface subnet but not the video interface address itself. This implies that traffic for the zones will be sourced from the ISA-MS.

To facilitate traffic from \((S,G)\) to go to the ISA-MS, a static IGMP \((S,G)\) must be configured on the video interface.
Local/Zoned ADI Prerequisites and Restrictions

This section describes prerequisites and restrictions for the local/zoned ADI feature:

- Network Time Protocol (NTP) is required to keep time synchronized between the ad server and the splicer. The time synchronization system helps keep the splicer and the server within +/-15 ms of each other.
- ADI is only supported within a Layer 3 IES or VPRN service.
- Splicing an SD advertisement into an HD main stream is supported, but splicing of an HD advertisement into an SD is not supported.
- The SCTE 30 connection between the ad server and the splicer must be maintained on separate IP addresses on the splicer within the video service.
- Up to 2 ad servers can be configured for redundancy.
- ADI only supports a single ISA-MS member in a video group.
- Up to 16 zone channels can be configured for a main channel.
- The audio re-ordering value in the multicast information policy must match the audio re-ordering configured on the A Server for reliable audio splicing.
- For best results, the ad should start/end with few frames of muted audio.
- The frequency of IDR frames in the network and ad streams must be less than one IDR frame every 1.3 seconds.
- Only the `splice_insert` command of SCTE-35 cue message is supported. The `splice_immediate` command is not supported.
Configuring Video Service Components with CLI

This section provides information to configure RET/FCC using the command line interface.

Topics in this section include:

- Video Services Overview on page 385
- Sample Configurations on page 391
- Configuring RET/FCC Video Features in the CLI on page 398
- Configuring ADI Components with CLI on page 411

Video Services Overview

There can be a maximum of eight ISA-MSs in a given system. The main entities of video configurations are:

- Video group
- Multicast information policy
  - A video policy to configure video interface properties
  - Multicast bundles and channels to associate bundles/channels with video groups
- Within a service, configuring a video interfaces and their associations with video groups.

Figure 33 shows various configuration elements and how they are associated by configuration.
Note that a video interface within a service can have multiple IP address, and their association with the video interfaces within the video policy are based on IP addresses. Support for multiple video interface IP addresses for a given video interface allows video characteristics (burst rate, retransmission format, etc.) for the channels associated with the video interface to be based on the IP address on which the request is received.

Both the bundle/channel configuration and the video interface configuration within the service are associated with a specific video group. If the request is received on a video interface for a channel not serviced by the video group associated with the video interface, the request is invalid and is dropped. **Figure 33** displays an example of this is a request for mc-range2 received on IP1, IP2 or IP3. A request for mc-range2 would only be valid on IP4.

As with other multicast information policies, the bundle name default is a special bundle and is reserved for setting of default values. If a video parameter is not explicitly set in a bundle/channel, the value set in the default bundle is used.
Configuring an ISA-MS Module

The ISA-MS hardware has an MDA form factor and is provisioned in the same manner as other MDAs in the config>card>mda>mda-type context.

Use the following commands to configure a ISA-MS module.

**CLI Syntax:**

```
config
  card slot-number
    mda slot-number
      mda-type isa-ms
```

The following output displays an ISA-MS configuration example:

```
*A:Dut-C>config>card# info
----------------------------------------------
card-type iom2-20g
    mda 1
      mda-type isa-ms
    exit
    mda 2
      mda-type isa-ms
    exit
----------------------------------------------
*A:Dut-C>config>card#
```
Configuring a Video Group

When used for video services, ISA-MSes are logically grouped into video groups that pool the ISA buffering and processing resources into a single logical entity.

Use the following commands to configure a video group.

**CLI Syntax:**
```
config
isa
  video-group video-group-id [create]
  description description-string
  primary mda-id
  [no] shutdown
```

The example shown below shows video-group 1 with a single ISA configured in slot 2/MDA 1.

```
*A: Dut-C> config> isa# info
===============================================================================
video-group 1 create
  description "Video Group 1"
  primary 7/2
  no shutdown
exit
===============================================================================
*A: Dut-C> config> isa#
```

Within the video group configuration, there are specific video application commands to enable features. These commands are described in the configuration examples for the application. Depending on the video application, more than one primary ISA-MS is allowed increasing the egress capacity of the video group.

Note: ISA-MS in a single video group cannot be on the same IOM. An IOM can accommodate two ISA-MS modules provided that the ISA-MS are members of different video groups.
Configuring a Video SAP and Video Interface in a Service

Video features in a VPLS service require the creation of a video SAP and a video interface. A video SAP is similar to other SAPs in the system in that QoS and filter policies can be associated with the SAP on ingress (traffic leaving the ISA and ingressing the system) and egress (traffic leaving system and entering the ISA).

Note that the video SAP is associated with a video group. Channels are also associated with a video group which is what establishes the link between what channels can be referenced through the video SAP. The multicast information policy associated with the service is where the channel to video group association is defined.

For unicast VPLS services that have an associated multicast service that is cross connected downstream of the router, the multicast service needs to be identified by the service ID in the unicast VPLS service.

The video commands for are identical in the IES and VPRN service contexts. The basic IES and VPRN commands are similar to the video commands in the VPLS context and follow the same logic of associating the video SAP with a video group and the multicast information policy defining the channel to video group association.

Another parameter defined for a channel in the multicast information policy that is important for video services is the administrative bandwidth defined for the channel. Many video applications use the bandwidth to determine if sufficient ISA egress bandwidth exists to service or drop a service request.

The following output displays an example video interface configuration.

```
A: IPTV-SR7> config> service> ies# info
----------------------------------------------
video-interface "video-100" create
    video-sap 4
    exit
    address 1.1.1.254/8
    address 100.100.0.254/8
    address 101.1.1.254/24
    adi
        channel 234.4.5.228 source 195.168.9.10 channel-name "228"
        scte35-action drop
        zone-channel 234.4.5.228 source 100.100.100.1 adi-channel-name "228-1"
    exit
    scte30
        ad-server 10.200.14.2
        local-address control 100.1.1.2 data 100.1.1.3
    exit
    exit
----------------------------------------------
A: IPTV-SR7> config> service> ies#
```
Basic Multicast Information Policy Configuration

Multicast information policies are used by the video applications to define multicast channel attributes and video policies which contains application-specific configuration for a video interface IP address.

Note that it is within the multicast information policy bundles, channels and source-overrides that a video group is assigned to a channel. The video group association is inherited from the more general construct unless it is explicitly disabled.

The administrative bandwidth for channels at the bundle, channel or source-override level is also defined in the multicast information policy. Video applications use the administrative bandwidth here when a channel rate estimate is needed.

A video policy is defined within the multicast information policy for a specific video interface IP address. The IP address for the video policy is the key value that associates it with a specific video interface IP address within a service associated with overall multicast information policy.

Refer to the 7x50 OS Triple Play Guide for CLI command descriptions and syntax usage information to configure multicast info policies.

The following output displays a policy example.

```
A:IPTV-SR7>config>mcast-mgmt># info
----------------------------------------------
multicast-info-policy "ies100" create
    bundle "5.6.140" create
        admin-bw 8000
        video
            video-group 1
            local-rt-server
            rt-buffer-size 3000
        exit
    channel "234.5.6.140" "234.5.6.140" create
    exit
exit
bundle "default" create
exit
bundle "5.6.241-5.6.243" create
    admin-bw 12000
    video
        video-group 1
        rt-buffer-size 4000
    exit
    channel "234.5.6.241" "234.5.6.243" create
    exit
exit
exit
----------------------------------------------
A:IPTV-SR7>config>router#
```
Sample Configurations

The following output displays configurations of VQM with packet selection.

*A:SR-7/Dut-C>config>mcast-mgmt># info
----------------------------------------------
multicast-info-policy "vqm" create
bundle "ixia" create
  channel "235.5.5.6" "235.5.5.7" create
  admin-bw 20000
  video
    video-group 4
    rt-buffer-size 1000
    analyzer
      alarms
        cc-error
        pat-repetition tnc 400 qos 600 poa 700
        pat-syntax
        pid-pmt-unref
        pmt-repetition tnc 2300 qos 2500 poa 2700
        pmt-syntax
        vid-pid-absent 5000
        non-vid-pid-absent 5000
        pcr-repetition tnc 400 qos 600 poa 700
        scte-35
        tei-set
        ts-sync-loss
      exit
    exit
  stream-selection source1 192.168.2.1 intf1 "ineo-ingress1"
  source2 192.168.2.1 intf2 "ineo-ingress2"
    exit
    source-override "192.168.2.1" create
  exit
  exit
bundle "default" create
  exit
----------------------------------------------
*A:SR-7/Dut-C>config>service# info
----------------------------------------------
customer 1 create
description "Default customer"
exit
ies 300 customer 1 vpn 300 create
description "Default Ies description for service id 300"
video-interface "video-300" create
  video-sap 4
  exit
address 20.20.255.254/16
channel 235.5.5.6 source 192.168.2.1 channel-name "Ineoquest-1"
  zone-channel 235.5.5.6 source 20.20.0.1 adi-channel-name "Ineoquest-1-1"
  exit
adi
  exit
  no shutdown
exit
    service-name "XYZ Ies 300"
    no shutdown
exit

*A:SR-7/Dut-C>config>service#

*A:SR-7/Dut-C>config>router# info
#--------------------------------------------------
#--------------------------------------------------
#--------------------------------------------------

#--------------------------------------------------

#--------------------------------------------------

#--------------------------------------------------

igmp
    interface "video-300-D"
    static
      group 235.5.5.6
      source 192.168.2.1
    exit
    exit
    interface "video-300-D2"
    static
      group 235.5.5.6
      source 192.168.2.1
    exit
    exit
    interface "ixia-egress"
    static
      group 235.5.5.6
      source 20.20.0.1
Video Services

```
exit
exit
exit
exit
#--------------------------------------------------
echo "PIM Configuration"
#--------------------------------------------------
pim
  rpf-table rtable-m
  interface "video-300"
  exit
  interface "ineo-ingress1"
    multicast-senders always
  exit
  interface "ineo-ingress2"
    multicast-senders always
  exit
  rp
    static
  exit
  bsr-candidate
    shutdown
  exit
  rp-candidate
    shutdown
  exit
exit
exit

--------------
*A:SR-7/Dut-C>config>router#
*A:SR-7/Dut-C>config>isa# info

-------------
video-group 4 create
  analyzer
  stream-selection
  primary 3/1
  no shutdown
exit

--------------
*A:SR-7/Dut-C>config>isa#
```
The following output displays configurations of VQM without packet selection.

```
customer 1 create
description "Default customer"
exit
ies 300 customer 1 vpn 300 create
description "Default Ies description for service id 300"
interface "linux-ingress" create
    address 10.10.33.228/24
    sap 3/2/17 create
description "sap-300-10.10.33.228"
exit
interface "linux-egress" create
    address 10.10.34.228/24
    sap 3/2/7 create
description "sap-300-10.10.34.228"
exit
video-interface "video-300" create
    video-sap 2
exit
    address 20.20.13.1/24
    channel 235.5.5.6 source 192.168.2.1 channel-name "A2-SP3"
    zone-channel 235.5.5.6 source 20.20.13.2 adi-channel-name "A2-SP3-1"
exit
adi
no shutdown
exit
service-name "XYZ Ies 300"
no shutdown
exit
```

```
*A:SR-7/Dut-C>config>service# /configure router
*A:SR-7/Dut-C>config>router# info
```

```
#--------------------------------------------------
echo "IP Configuration"
#--------------------------------------------------
interface "system"
    address 10.20.1.1/32
exit
multicast-info-policy "A-server"
#--------------------------------------------------
echo "Static Route Configuration"
#--------------------------------------------------
static-route 128.251.33.0/24 next-hop 10.10.33.229
static-route 192.168.2.0/24 next-hop 10.10.33.229
#--------------------------------------------------
echo "IGMP Configuration"
#--------------------------------------------------
igmp
    interface "video-300-D"
    static
```
group 235.5.5.6
    source 192.168.2.1
    exit
    exit
    exit
interface "linux-egress"
    static
    group 235.5.5.6
    source 20.20.13.2
    exit
    exit
    exit
    exit
#--------------------------------------------------
echo "PIM Configuration"
#--------------------------------------------------
pim
    interface "linux-ingress"
        hello-interval 0
        multicast-senders always
    exit
    interface "linux-egress"
        hello-interval 0
    exit
    apply-to all
    rp
        static
        exit
    bsr-candidate
        shutdown
        exit
    rp-candidate
        shutdown
        exit
    exit
    exit

*A:SR-7/Dut-C>config>router# /configure isa
*A:SR-7/Dut-C>config>isa# info
----------------------------------------------
video-group 2 create
    analyzer
    primary 2/1
    no shutdown
    exit
----------------------------------------------
*A:SR-7/Dut-C>config>isa# /configure mcast-management
*A:SR-7/Dut-C>config>mcast-mgmt># info
----------------------------------------------
multicast-info-policy "A-server" create
    bundle "LiveTv" create
    channel "234.5.6.243" "234.5.6.243" create
    admin-bw 3000
    video
        video-group 2
        rt-buffer-size 1000
        exit
    exit
    channel "235.5.5.6" "235.5.5.6" create
admin-bw 5000
video
  video-group 2
  rt-buffer-size 1000
analyzer
  alarms
    cc-error
    pat-repetition tnc 200 qos 400 poa 600
    pat-syntax
    pid-pmt-unref
    pmt-repetition
    pmt-syntax
    vid-pid-absent 1000
    non-vid-pid-absent 1000
    pcr-repetition tnc 200 qos 400 poa 600
    scte-35
    tei-set
    ts-sync-loss
    report-alarm severity tnc
exit
exit
exit
source-override "128.251.33.37" create
exit
exit
exit
bundle "default" create
exit
bundle "mp2ts-ads" create
  channel "234.4.5.1" "234.4.5.254" create
  admin-bw 5000
video
  video-group 2
  rt-buffer-size 1000
exit
exit
exit
exit
----------------------------------------------
*A:SR-7/Dut-C>config>mcast-mgmt>#
Configuring RET/FCC Video Components with CLI

This section provides information to configure RET/FCC using the command line interface.

Topics in this section include:

- Configuring RET/FCC Video Features in the CLI on page 398
  - Configuring the RET Client on page 398
  - Configuring the RET Server on page 402
  - Configuring the FCC Server on page 406
Configuring RET/FCC Video Components with CLI

Configuring RET/FCC Video Features in the CLI

The following sections provide configuration examples for the RET client, RET server and FCC server.

Configuring the RET Client

This section provides an example configuration for the RET client. The configuration example has the following assumptions:

- A single ISA-MS in slot 2/1 in video group 1
- A single channel 234.0.0.1 within multicast bundle “b1” with an administrative bandwidth of 2700 Kbps defined in `multicast-info-policy multicastinfopolicyname`.
- The upstream RET server for the channel is 4.4.4.4 on UDP port 4096
- A single video interface named “v1” in the service with IP address 3.3.3.3/24
- A RET client address of 3.3.3.4 for a VPLS and 3.3.3.3 for IES and VPRN case.

The first step in the configuration is to configure video group 1 and the ISA-MS hardware.

**CLI Syntax:**
```
config>isa
    video-group video-group-id [create]
            primary mda-id
            no shutdown

*A:ALA-48config>isa# info
-------------------------------------------------
    video-group 1 create
            primary 2/1
            no shutdown
    exit
-------------------------------------------------
*A:ALA-48config>isa#
```

**CLI Syntax:**
```
config# card slot-number
    mda mda-slot
            mda-type mda-type

*A:ALA-48config>card>mda# info
-------------------------------------------------
    mda-type isa-ms
-------------------------------------------------
*A:ALA-48config>card>mda#
```
The channel parameters for 234.0.0.1 are configured in **multicast-info-policy** 
*multicastinfopolicyname*. The channel configuration includes the administrative bandwidth, the 
channel’s association with video group 1 and the upstream RET server configuration for the 
channel (4.4.4.4 UDP port 4096). The following output displays the configuration. Refer to the 
CLI tree for a complete list of CLI commands.

```
*A:ALA-48config>mcast-mgmt>mcast-info-plcy# info
---------------------------------------------
bundle "b1" create
  admin-bw 2700
  video
    video-group 1
    rt-server 4.4.4.4 port 4096
  exit
  channel "234.0.0.1" "234.0.0.1" create
  exit
exit
bundle "default" create
exit
video-policy
  video-interface 3.3.3.3 create
  exit
exit
```

Note that the channel parameters are actually defined for the channel bundle “b1” and the channel 
inherits those values based on the multicast information policy inheritance rules.
For the RET client in a VPLS, the following commands within the service instance perform the following tasks to complete the RET client configuration:

- Associate the VPLS with **multicast-info-policy** `multicastinfopolicyname`.
- Create the video interface “vi”.
- Create video SAP and associate it with video group 1.
- Assigns a RET client address and gateway.
- Create a static IGMP join on SAP 3/2/13:21 for the channel 234.0.0.1.

Note that SAP 3/2/13:21 is a dummy SAP with the only purpose of attracting multicast traffic to the node to enable the caching. No subscribers are connected to it.

```
*A:ALA-48config>service>vpls# info
----------------------------------------------
  igmp-snooping
  no shutdown
  exit
  video-interface "vi" create
  video-sap 1
  exit
  address 3.3.3.3/24
  gateway-ip 3.3.3.253
  rt-client-src-address 3.3.3.4
  no shutdown
  exit
----------------------------------------------
*A:ALA-48config>service>vpls#
```

```
*A:ALA-48config>router# info
----------------------------------------------
...  
multicast-info-policy multicastinfopolicyname
  sap 3/2/13:21 create
  igmp-snooping
  static
  group 234.0.0.1
  starg
  exit
  exit
  exit
...  
----------------------------------------------
*A:ALA-48config>router#
```

Note that the RET client address is 3.3.3.4 which must be within the IP subnet assigned to the video interface (3.3.3.24).
For the RET client in an IES or VPRN, the following commands within the service instance perform these tasks to complete the RET client configuration:

- Associate the service with `multicast-info-policy multicastinfopolicyname`.
- Create the video interface “vi” and assign IP address 3.3.3.3.
- Create video SAP and associate it with video group 1.
- Creates a static IGMP join on the video interface for the channel 234.0.0.1. (7750 only)

```
*A:ALA-48config>service>ies# info
----------------------------------------------
 video-interface "vi" create
  video-sap 1
  exit
  address 3.3.3.3/32
  no shutdown
  exit

*----------------------------------------------
*A:ALA-48config>service>ies#

*A:ALA-48config>router# info
----------------------------------------------

*----------------------------------------------
*A:ALA-48config>router#

The RET client address is 3.3.3.3 which is the address assigned to the video interface in the video policy portion of the multicast information policy.
Configuring the RET Server

This section provides an example configuration for the RET server. The configuration example has the following assumptions:

- A single ISA-MS in slot 2/1 in video group 1
- A single channel 234.0.0.1 within multicast bundle “b1” with an administrative bandwidth of 2700 Kbps defined in `multicast-info-policy` `multicastinfopolicyname`.
- A retransmission buffer for the channel set to 300 milliseconds.
- The RET rate is 5% of nominal.
- Local RET server address is 3.3.3.3 with destination port is UDP 4096.

The first step in the configuration is to configure video group 1 enabling the RET server and the ISA-MS hardware.

**CLI Syntax:**
```
config>isa
  video-group video-group-id [create]
  local-rt-server
  no shutdown

*A:ALA-48config>isa# info
---------------------------------------------------------------------
  video-group 1 create
  local-rt-server
  primary 2/1
  no shutdown
  exit
---------------------------------------------------------------------
*A:ALA-48config>isa#

*A:ALA-48config>card 2/mda 1# info
----------------------------------------------
  mda-type isa-ms
----------------------------------------------
*A:ALA-48config>card>mda#
```

Note the **local-rt-server** command in the above output enables the local RET server on the video group.
The channel parameters for 234.0.0.1 are configured in `multicast-info-policy` `multicastinfopolicyname`. The channel configuration includes the administrative bandwidth and the channel’s association with video group 1.

```
*A:ALA-48config>mcast-mgmt>mcast-info-plcy# info
---------------------------------------------------------------------
bundle "default" create
  local-rt-port 4096
exit
bundle "b1" create
  admin-bw 2700
  video
    video-group 1
    local-rt-server
    rt-buffer-size 300
exit
channel "234.0.0.1" "234.0.0.1" create
exit
exit
video-policy
  video-interface 3.3.3.3 create
    rt-rate 5
    hd
      local-rt-server
exit
    sd
      local-rt-server
exit
    pip
      local-rt-server
exit
exit
---------------------------------------------------------------------

Note the `local-rt-port` command in the bundle “default” defines the destination UDP port used to reach the local RET server on the service where the multicast information policy is applied. The RET server port can only be defined in the bundle “default” and applies for all bundles in the policy. If no value is specified, the default is used.

In the bundle “b1” the `local-rt-server` command enables the RET server for all channels in the bundle, and the `rt-buffer-size` command sets the retransmission buffer for all channels in the bundle to 300 milliseconds.

In the video policy above, the `local-rt-server` commands for the video interface 3.3.3.3 enables the RET server on that interface for all channel types “hd” (High Definition), “sd” (Standard Definition) and “pip” (Picture-in-Picture). The `rt-rate` command indicates that the retransmission rate will be 5% of the nominal rate for all channel types; individual rates can be defined if desired.
For the RET server in a VPLS, these commands within the service instance perform the following tasks to complete the RET server configuration:

- Associate the VPLS with `multicast-info-policy multicastinfopolicyname`.
- Create the video interface “vi”.
- Create video SAP and associate it with video group 1.
- Assigns an IP address 3.3.3.3 to the video interface.
- Create a static IGMP join on SAP 3/2/13:21 for the channel 234.0.0.1.

Note that SAP 3/2/13:21 is a dummy SAP with the only purpose of attracting multicast traffic to the node to enable the caching. No subscribers are connected to it.

```
*A:ALA-48config>service>vpls# info
----------------------------------------------
  igmp-snooping
  no shutdown
  exit
  video-interface "vi" create
    video-sap 1
    exit
    address 3.3.3.3/32
    no shutdown
  exit
  multicast-info-policy multicastinfopolicyname
  sap 3/2/13:21 create
    igmp-snooping
    static
      group 234.0.0.1
      starg
      exit
    exit
  exit
----------------------------------------------
*A:ALA-48config>service>vpls#
```

The services available on the video interface address 3.3.3.3 are defined in the video policy in which the RET server was enabled.
For the RET server in an IES or VPRN, these commands within the service instance perform the following tasks to complete the RET server configuration:

- Associate the service with **multicast-info-policy multicastinfopolicyname**.
- Create the video interface “vi” and assign IP address 3.3.3.3.
- Create video SAP and associate it with video group 1.
- Creates a static IGMP join on video-interface “vi” for the channel 234.0.0.1.

```
*A:ALA-48config>service>ies# info
----------------------------------------------
video-interface "vi" create
  video-sap 1
  exit
  address 3.3.3.3/32
  no shutdown
  exit
multicast-info-policy multicastinfopolicyname
  pim
  interface "vi"
  exit
  exit
igmp
  interface "vi"
  static
  group 234.0.0.1
  starg
  exit
  exit
  exit
----------------------------------------------
*A:ALA-48config>service>ies#
```

The services available on the video interface address 3.3.3.3 are defined in the video policy in which the RET server was enabled.
Configuring the FCC Server

This section provides an example configuration for the FCC server. The configuration example has the following assumptions:

- A single ISA-MS in slot 2/1 in video group 1.
- A single channel 234.0.0.1 within multicast bundle “b1” with an administrative bandwidth of 8000 Kbps defined in `multicast-info-policy multicastinfopolicyname`.
- The FCC mode is burst with a rate 130% of nominal for HD, 200% for SD, and disabled for PIP.
- Local FCC server address is 3.3.3.3 with destination port is UDP 4098.

**CLI Syntax:**
```
config>isa
  video-group video-group-id [create]
    fcc-server
    no shutdown
```

The first step in the configuration is to configure video group 1 enabling the RET server and the ISA-MS hardware.

```
*A:ALA-48config>isa# info
-----------------------------------------------
  video-group 1 create
    fcc-server
      primary 2/1
        no shutdown
    exit
-----------------------------------------------
*A:ALA-48config>isa#
```

```
*A:ALA-48config>card>mda# info
-----------------------------------------------
  mda-type isa-ms
-----------------------------------------------
*A:ALA-48config>card>mda#
```

Note the `fcc-server` command in the above output enables the FCC server on the video group.
The channel parameters for 234.0.0.1 are configured in *multicast-info-policy* *multicastinfopolicyname*. The channel configuration includes the administrative bandwidth and the channel’s association with video group 1.

```
*A:ALA-48configmcast-mgmtmcast-info-picy# info
----------------------------------------------
bundle "default" create
   local-fcc-port 4098
exit
bundle "b1" create
   admin-bw 8000
   video
      video-group 1
      fcc-server
      fcc-channel-type hd
exit
channel "234.0.0.1" "234.0.0.1" create
exit
exit
video-policy
   video-interface 3.3.3.3 create
      rt-rate 5
      hd
         fcc-server mode burst
         fcc-burst 30
exit
      sd
         fcc-server mode burst
         fcc-burst 100
exit
      pip
         no fcc-server
exit
exit
----------------------------------------------
*A:ALA-48configmcast-mgmtmcast-info-picy#*
```

Note the **local-fcc-port** command in the bundle “default” defines the destination UDP port used to reach the FCC server on the service where the multicast information policy is applied. The FCC server port can only be defined in the bundle “default” and applies for all bundles in the policy. If no value is specified, the default is used.

In the bundle “b1”, the **fcc-server** command enables the FCC server for all channels in the bundle, and the **fcc-channel-type hd** command sets the channel type for all channels in the bundle to “hd” (High Definition).

In the video policy context above, the **fcc-server** commands for the video interface 3.3.3.3 enables the FCC server on that interface for all channel types “hd” (High Definition), “sd” (Standard Definition) whereas the **no fcc-server** command disables the FCC for “pip” (Picture-in-Picture) channels on the video interface. The **fcc-burst** command in the policy indicates that the burst rate over the nominal rate for the channel type; HD at 130% (30% over nominal) and SD at 200% (100% over nominal).
For the FCC server in a VPLS, the following commands within the service instance perform the following tasks to complete the FCC server configuration:

- Associate the VPLS with **multicast-info-policy** `multicastinfopolicyname`
- Create the video interface “vi”.
- Create video SAP and associate it with video group 1.
- Assigns an IP address 3.3.3.3 to the video interface.
- Create a static IGMP join on SAP 3/2/13:21 for the channel 234.0.0.1.

Note that SAP 3/2/13:21 is a dummy SAP with the only purpose of attracting multicast traffic to the node to enable the caching. No subscribers are connected to it.

```
*A:ALA-48configservicevpls# info
----------------------------------------------
igmp-snooping
   no shutdown
exit
video-interface "vi" create
   video-sap 1
   exit
   address 3.3.3.3/32
   no shutdown
exit
multicast-info-policy multicastinfopolicyname
   sap 3/2/13:21 create
   igmp-snooping
   static
      group 234.0.0.1
      starg
   exit
exit
exit
exit
----------------------------------------------
*A:ALA-48configservicevpls#
```

The services available on the video interface address 3.3.3 are defined in the video policy in which the FCC server was enabled.
For the FCC server in an IES or VPRN, the following commands within the service instance perform the following tasks to complete the FCC server configuration:

- Associate the service with `multicast-info-policy multicastinfopolicyname`.
- Create the video interface “vi” and assign IP address 3.3.3.3.
- Create video SAP and associate it with video group 1.
- Creates a static IGMP join on video-interface “vi” for the channel 234.0.0.1.

```
*A:ALA-49configserviceies# info
-----------------------------------------------
    video-interface "vi" create
    video-sap 1
    exit
    address 4.4.4.4/32
    no shutdown
    exit
-----------------------------------------------
*A:ALA-49configserviceies#

*A:ALA-48configrouter# info
-----------------------------------------------

    multicast-info-policy multicastinfopolicyname
    plm
        interface "vi"
        exit
    exit
    igmp
        interface "vi"
        static
            group 234.0.0.1
            starg
            exit
        exit
    exit
-----------------------------------------------
*A:ALA-48configrouter#
```

The services available on the video interface address 3.3.3.3 are defined in the video policy in which the FCC server was enabled.
Logging and Accounting Collection for Video Statistics

The following output displays a configuration example used in logging and accounting for video.

*A:SR-7/Dut-C>config>log# info
----------------------------------------------
file-id 1
  location cf3:
  exit
accounting-policy 1
  shutdown
  record video
  collection-interval 5
to file 1
  exit
... 
----------------------------------------------
*A:SR-7/Dut-C>config>log#

Use the following CLI to enable logging and accounting to a service to collect stats for that particular service.

Example:

*A:SR-7/Dut-C>config>service>ies# video-interface "vi" accounting-policy 1
*A:SR-7/Dut-C>config>service>ies# info
  video-interface "vi" create
    accounting-policy "1"
  exit

Start ing stats collection can be enabled by executing a no shutdown command on the accounting policy. This starts the recording of stats and the stats will be written in an act-collect directory and a shutdown command on the accounting policy will move the recorded file to act directory.
Configuring ADI Components with CLI

This section provides information to configure ADI using the command line interface.

Topics in this section include:

• Configuring the RET Client on page 412
• Configuring a Video Group on page 413
• Configuring NTP on page 414
• Configuring Channel Parameters on page 414
• Configuring Service Entities on page 415
Configuring ADI in CLI

Configuring the RET Client

This section provides an example configuration for the ADI splicer. The configuration example makes the following assumptions:

- A single ISA-MS is configured in slot 2/1 in video group 1.
- The NTP server for the router is 192.168.15.221.
- A single channel main 234.5.6.140 within multicast bundle “b1” is defined in the `multicast-info-policy multicastinfopolicyname` context.
- IES service 100 is a Layer 3 service in which ADI will be performed.
- The video interface in IES 100 is 100.100.0.254/8
- The ad server address is 10.200.14.2
- The splicer’s local addresses used to communicate with the ad server are 100.1.1.2 for control traffic and 100.1.1.3 for data traffic.
- For the SCTE 30 communication in the example, the main channel is named 228 with (S,G) = (195.168.9.10,234.4.5.228) and the zone channel is named 228-1 with (S,G) = (100.100.100.1,234.4.5.228).
- Must have an IGMP static entry for the network channel (S,G) on the video-interface to attract the network traffic to the video interface.
- Must have the video-interface enabled in PIM.
Configuring a Video Group

The first step in the configuration is to configure a video group \( \text{video-group-id} = 1 \) and enabling ad insertion and the ISA-MS hardware. Note the \texttt{ad-insert} command enables the ADI splicer on the video group.

A:ALA-49>config>isa# info
----------------------------------------------
...  
   video-group 1 create  
   description "Video Group 1"  
   ad-insert  
   primary 7/2  
   no shutdown  
   exit
...
----------------------------------------------
A:ALA-49>config>isa#

The following output shows the card and MDA configuration.

A:ALA-49>config>card# info
----------------------------------------------
   card-type iom2-20g  
   mda 1  
   shutdown  
   mda-type isa-ms  
   exit  
   mda 2  
   mda-type isa-ms  
   exit
----------------------------------------------
A:ALA-49>config>card#
Configuring NTP

NTP is required on the splicer to ensure that time is synchronized between it and the ad server.

```
A:ALA-49>config>system>time# info
----------------------------------------------
ntp
  no authentication-check
  ntp-server
  server 192.168.15.221
  no shutdown
  exit
...  
----------------------------------------------
A:ALA-49>config>system>time#
```

Configuring Channel Parameters

The channel parameters for 234.4.5.228 are configured in the `multicast-info-policy` context. For ADI, the channel configuration required is the channel’s association with video group 1.

```
*A:ALA-49>config>mcast-mgmt# info
-----------------------------------------------
... 
multicast-info-policy "multicastinfopolicyname" create
  bundle "b1" create
    video
      video-group 1
    exit
  channel "234.4.5.228" "234.4.5.228" create
  exit
  bundle "default" create
  exit
  exit
...  
-----------------------------------------------
*A:ALA-49>config>mcast-mgmt#
```
Configuring Service Entities

In addition to the commands needed to configure a service, the following commands within the service instance are used to perform the following ADI configuration steps. This example uses an IES service context.

- Associate IES 100 with `multicast-info-policy multicastinfopolicyname`.
- Create the video interface video-100.
- Create a video SAP and associate it with video group 1.
- Assigns an IP address 100.100.0.254 to the video interface and subnet 100.0.0.0/8.
- Name the main channel \((S,G) = (195.168.9.10,234.4.5.228)\) “228” and the zone channel \((S,G) = (100.100.100.1,234.4.5.228)\) “228-1”.
- Configure the ad server (address = 10.200.14.2) and create IP addresses within the video interface subnet for SCTE 30 control traffic (100.1.1.2) and data traffic (100.1.1.3).
- The control and data addresses must be in the video interface subnet.

```
*A:ALA-49>config>service>ies# info
----------------------------------------------
... video-interface "video-100" create
    video-sap 1
    exit
    address 100.100.0.254/8
    adi
        channel 234.4.5.228 source 195.168.9.10 channel-name "228"
        scte35-action drop
        zone-channel 234.4.5.228 source 100.100.100.1 adi-channel-name "228-1"
    exit
    scte30
    ad-server 10.200.14.2
    local-address control 100.1.1.2 data 100.1.1.3
    exit
    exit
    no shutdown
    no shutdown
----------------------------------------------
*A:ALA-49>config>service>ies#
```

Note that the source address (100.100.100.1) for the zone channel \((S,G)\) and the local addresses (100.1.1.2 and 100.1.1.3) used for SCTE 30 communication must all be within the video interface subnet (100.0.0.0/8).

Connections are accepted from multiple ad-servers. This can be used for ad server redundancy.
If the main channel were a (*,G), the source address of 0.0.0.0 would have been specified.

Additional zone channels with distinct names could be configured within the service instance. In a practical configuration, the G for the main channel (234.4.5.228) will be the same for G in the zone channel (S,G) because the STBs will join the (*,G) at the A-server and D-server.

Configuring ADI for a VPRN service instance uses the same commands within the VPRN service context.
Video Command Reference

This section provides a command reference for the CLI commands for IP-TV video applications.

Topics include:

- IP-TV Command Hierarchies on page 418
  - Hardware Commands on page 418
  - Video Group Commands on page 418
  - Video Policy Video Commands on page 418
  - Bundle and Channel Commands on page 420
  - Service Video Interface Commands on page 422
  - Show Commands on page 425
  - Clear Commands on page 425
  - Debug Commands on page 426

- Video Services Commands on page 427
IP-TV Command Hierarchies

Hardware Commands

config
  — [no] card slot-number
    — card-type card-type
    — no card-type
  — [no] mda mda-slot
    — mda-type mda-type
    — no mda-type

Video Group Commands

config
  — isa
    — ins-group ins-group-id [create]
    — no ins-group ins-group-id
      — description description-string
      — no description
      — mda mda-id [drain]
      — no mda mda-id
      — [no] shutdown
    — video-group video-group-id [create]
    — no video-group video-group-id
      — [no] ad-insert
      — [no] analyzer
      — description description-string
      — no description
      — [no] fcc-server
      — [no] local-rt-server
      — [no] primary mda-id
      — resv-ret resv-ret
      — [no] shutdown
      — [no] stream-selection

Video Policy Video Commands

config
  — mcast-management
    — multicast-info-policy policy-name [create]
    — no multicast-info-policy policy-name
      — video-policy
        — video-interface ip-address [create]
        — no video-interface ip-address
          — hd
            — dent-threshold threshold
            — no dent-threshold
            — fcc-burst burst-percentage
- no fcc-burst
- fcc-server [mode {burst | dent | hybrid}]
- no fcc-server
- local-rt-server
- no local-rt-server
- mc-handover percentage
- no mc-handover
- rt-rate rt-burst-percentage
- no rt-rate
- max-sessions sessions
- no max-sessions
- pip
  - dent-threshold threshold
  - no dent-threshold
  - fcc-burst burst-percentage
  - no fcc-burst
  - fcc-server [mode {burst | dent | hybrid}]
  - no fcc-server
  - local-rt-server
  - no local-rt-server
  - mc-handover percentage
  - no mc-handover
  - rt-rate rt-burst-percentage
  - no rt-rate
  - rt-mcast-reply [count count] [interval milliseconds] [hold-time milliseconds]
  - no rt-mcast-reply
  - rt-payload-type payload-type
  - no rt-payload-type
  - rt-rate rt-burst-percentage
  - no rt-rate
- sd
  - dent-threshold threshold
  - no dent-threshold
  - fcc-burst burst-percentage
  - no fcc-burst
  - fcc-server [mode {burst | dent | hybrid}]
  - no fcc-server
  - local-rt-server
  - no local-rt-server
  - mc-handover percentage
  - no mc-handover
  - rt-rate rt-burst-percentage
  - no rt-rate
  - subscriber-bw-limit bandwidth
  - no subscriber-bw-limit
Bundle and Channel Commands

config
  — mcast-management
    — multicast-info-policy policy-name [create]
    — no multicast-info-policy policy-name
      — bundle bundle-name [create]
      — no bundle bundle-name
        — admin-bw kbps
        — no admin-bw
        — bw-activity {use-admin-bw | dynamic [falling-delay seconds]} [black-hole-rate kbps]
        — no bw-activity
        — channel ip-address [ip-address] [create]
        — no channel ip-address [ip-address]
          — admin-bw kbps
          — no admin-bw
          — video
            — fcc-channel-type {hd | sd | pip}
            — no fcc-channel-type
            — fcc-min-duration time
            — no fcc-min-duration
            — fcc-server [disable]
            — no fcc-server
            — local-fcc-port port
            — no local-fcc-port
            — local-rt-port port
            — no local-rt-port
            — local-rt-server [disable]
            — no local-rt-server
            — reorder-audio time
            — no reorder-audio
            — rt-buffer-size rt-buffer-size
            — no rt-buffer-size
            — rt-server disable
            — no rt-server
            — rt-server ip-address port port-num
            — video-group video-group-id
            — video-group disable
            — no video-group
            — source-override ip-address [create]
            — no source-override ip-address
              — admin-bw kbps
              — no admin-bw
              — video
                — fcc-channel-type {hd | sd | pip}
                — no fcc-channel-type
                — fcc-min-duration time
                — no fcc-min-duration
                — fcc-server [disable]
                — no fcc-server
                — local-fcc-port port
                — no local-fcc-port
                — local-rt-port port
Service Video Interface Commands

VPLS Commands

```
config>service>vpls service-id
   — multicast-info-policy policy-name
   — no multicast-info-policy
   — video-interface ip-int-name [create]
   — no video-interface ip-int-name
      — [no] address ip-address/mask
      — cpu-protection policy-id
      — no cpu-protection
      — description description-string
      — no description
      — gateway-ip ip-address
      — no gateway-ip
      — multicast-service service-id
      — no multicast-service
      — rt-client-src-address ip-address
      — no rt-client-src-address
      — [no] shutdown
      — video-sap video-group-id
      — no video-sap
         — egress
            — filter ip ip-filter-id
            — no filter
            — qos egress-qos-policy-id
            — no qos
         — ingress
            — filter ip ip-filter-id
            — no filter
            — qos ingress-qos-policy-id
            — no qos
```
IES Commands

```plaintext
config>service>ies service-id
   — video-interface ip-int-name [create]
   — no video-interface ip-int-name
      — [no] address ip-address/mask
      — adi
         — channel mcast-address source ip-address [channel-name channel-name]
         — no channel mcast-address source ip-address
            — description description-string
            — no description
            — scte35-action {forward | drop}
            — zone-channel mcast-address source ip-address adi-channel-name channel-name
            — no zone-channel mcast-address source ip-address
   — scte30
      — [no] ad-server ip-address
      — local-address control ip-address data ip-address
      — no local-address
      — [no] shutdown
            — description description-string
            — no description
            — multicast-service service-id
            — no multicast-service
            — rt-client-src-address ip-address
            — no rt-client-src-address
            — [no] shutdown
            — video-sap video-group-id
            — no video-sap
               — egress
                  — filter ip ip-filter-id
                  — no filter
                  — qos egress-qos-policy-id
                  — no qos
               — ingress
                  — filter ip ip-filter-id
                  — no filter
                  — qos ingress-qos-policy-id
                  — no qos
```
VPRN Commands

Note that VPRN service commands are only applicable to the 7750 SR-Series platforms.

```
config>service>vprn service-id
   — video-interface ip-int-name [create]
   — no video-interface ip-int-name
      — [no] address ip-address/mask
      — adi
         — channel mcast-address source ip-address [channel-name channel-name]
         — no channel mcast-address source ip-address
            — description description-string
            — no description
            — scte35-action {forward | drop}
            — zone-channel mcast-address source ip-address adi-channel-name channel-name
            — no zone-channel mcast-address source ip-address
         — scte30
            — [no] ad-server ip-address
            — local-address control ip-address data ip-address
            — no local-address
            — [no] shutdown
            — description description-string
            — no description
            — multicast-service service-id
            — no multicast-service
            — rt-client-src-address ip-address
            — no rt-client-src-address
            — [no] shutdown
            — video-sap video-group-id
            — no video-sap
               — egress
                  — filter ip ip-filter-id
                  — no filter
                  — qos egress-qos-policy-id
                  — no qos
               — ingress
                  — filter ip ip-filter-id
                  — no filter
                  — qos ingress-qos-policy-id
                  — no qos
```
Show Commands

```plaintext
show
  — isa
    — video-group [video-group-id]

show
  — video
    — adi [service service-id] [interface ip-int-name] [address mcast-address] [source ip-address] [detail]
      — channel [service service-id] [interface ip-int-name] [address mcast-address] [source ip-address] [summary/detail] [pid|config] [analyzer[interval time-interval]]
      — session [service service-id] [interface ip-int-name] [address mcast-address] [source ip-address]
    — splice-status [service service-id] [interface ip-int-name] [address mcast-address] [source ip-address] [start-time start-time [interval time-interval]]
      — channel [service service-id] [interface ip-int-name] [address mcast-address] [source ip-address] [summary | detail]
      — interface [service service-id] [interface ip-int-name] [stats {rt-server|fcc-server}]
      — interface [service service-id] [interface ip-int-name] summary
      — rtp-session [service service-id] [source ip-address] [detail [stats {rt-server|fcc-server}]]
      — rtp-session [service service-id] summary
```

Clear Commands

```plaintext
clear
  — video
    — id service-id
      — session all
      — session client srcAddr
    — statistics
      — id service-id
        — adi-session
        — channel all [rt-client] [rt-server] [fcc-server] [ad-insert]
        — channel grp-address [source srcAddr] [rt-client] [rt-server] [fcc-server] [ad-insert]
        — interface ip-int-name [address ip-address] rt-client] [rt-server] [fcc-server] [ad-insert]
      — session all [rt-server] [fcc-server]
      — session client srcAddr [rt-server] [fcc-server]
    — isa video-group-id [mda-id]
```
Debug Commands

debug
   [no] service
      id service-id
         [no] video-interface video-ip-int-name
         adi [zone-channel-name]
         no adi
         adi-packet [zone-channel-name] [type {type-name [type-name] all}]
         no adi-packet
         fcc-server [client client-ip [source-port src-port]]
         no fcc-server
         packet-rx [client client-ip [source-port src-port]] [fcc-join] [fcc-leave] [ret-nack]
         no packet-rx
         packet-tx [group grp-addr [source src Addr]] [ret-nack]
         no packet-tx
         rt-client [group group-addr]
         no rt-client
         rt-server [client client-ip [source-port src-port]]
         no rt-server
         sg [group grp-addr [source src-addr]]
         no sg
**Video Services Commands**

- Generic Commands on page 427
- Hardware Commands on page 429
- ins-group ins-group-id [create] on page 432
- Multicast Info Policy Commands on page 436
- Video Policy Commands on page 443
- Bundle and Channel Commands on page 450
- Service Video Interface Commands on page 455
- Show Commands on page 463
- Clear Commands on page 479
- Debug Commands on page 482

---

**GENERIC COMMANDS**

**description**

**Syntax**

description description-string

no description

**Context**

config>isa>video-group
config>service>ies>video-interface
config>service>vpls>video-interface
config>service>vprn>video-interface
config>service>ies>video-interface>adi>channel
config>service>vpls>video-interface>adi>channel
config>service>vprn>video-interface>adi>channel

**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 context in the configuration file.

The `no` form of this command removes any description string from the context.

**Default**

No description is associated with the configuration context.

**Parameters**

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

Syntax
[no] shutdown

Context
config>isa>video-group
config>service>ies>video-interface
config>service>vpls>video-interface
config>service>vprn>video-interface
config>service>ies>video-interface>adi
config>service>vpls>video-interface>adi
config>service>vprn>video-interface>adi

Description
The shutdown command administratively disables the entity. When disabled, an entity does not change, reset, or remove any configuration settings or statistics. Many entities must be explicitly enabled using the no shutdown command.

The shutdown command administratively disables an entity. 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 can be deleted.

Unlike other commands and parameters where the default state is not indicated in the configuration file, shutdown and no shutdown are always indicated in system generated configuration files.

Default
no shutdown
**HARDWARE COMMANDS**

**card**

**Syntax**  
```
card slot-number
no card slot-number
```

**Context**  
config

**Description**  
This mandatory command enables access to the chassis card Input/Output Module (IOM), slot, and MDA CLI context.

The `no` form of this command removes the card from the configuration. All associated ports, services, and MDAs must be shutdown

**Default**  
No cards are configured.

**Parameters**  
`slot-number` — The slot number of the card in the chassis.

**Values**  
1 — 10 depending on chassis model.

- SR-1: `slot-number = 1`
- SR-7: `slot-number = 1 — 5`
- SR-12: `slot-number = 1 — 10`

- ESS-1: `slot-number = 1`
- ESS-6: `slot-number = 1 — 4`
- ESS-7: `slot-number = 1 — 5`
- ESS-12: `slot-number = 1 — 10`

**card-type**

**Syntax**  
```
card-type card-type
no card-type
```

**Context**  
config>card

**Description**  
This mandatory command adds an IOM to the device configuration for the slot. The card type can be preprovisioned, meaning that the card does not need to be installed in the chassis.

A card must be provisioned before an MDA or port can be configured.

A card can only be provisioned in a slot that is vacant, meaning no other card can be provisioned (configured) for that particular slot. To reconfigure a slot position, use the `no` form of this command to remove the current information.

A card can only be provisioned in a slot if the card type is allowed in the slot. An error message is generated if an attempt is made to provision a card type that is not allowed.

If a card is inserted that does not match the configured card type for the slot, then a medium severity alarm is raised. The alarm is cleared when the correct card type is installed or the configuration is modified.
A high severity alarm is raised if an administratively enabled card is removed from the chassis. The alarm is cleared when the correct card type is installed or the configuration is modified. A low severity trap is issued when a card is removed that is administratively disabled.

Because the IOM-3 integrated card does not have the capability to install separate MDAs, the configuration of the MDA is automatic. This configuration only includes the default parameters such as default buffer policies. Commands to manage the MDA such as `shutdown`, `named buffer pool` etc will remain in the MDA configuration context.

An appropriate alarm is raised if a partial or complete card failure is detected. The alarm is cleared when the error condition ceases.

The `no` form of this command removes the card from the configuration.

**Default**
No cards are preconfigured for any slots.

**Parameters**
- `card-type` — The type of card to be configured and installed in that slot.
  - **Values**
    - **7750 SR:** `iom-20g, iom2-20g, iom-20g-b, iom3-xp`
    - **7450 ESS:** `iom-20g, iom-20g-b, iom3-xp`

**mda**

**Syntax**
```
mda mda-slot
no mda mda-slot
```

**Context**
`config>card`

**Description**
This mandatory command enables access to a card’s MDA CLI context to configure MDAs.

**Default**
No MDA slots are configured by default.

**Parameters**
- `mda-slot` — The MDA slot number to be configured. Slots are numbered 1 and 2. On vertically oriented slots, the top MDA slot is number 1, and the bottom MDA slot is number 2. On horizontally oriented slots, the left MDA is number 1, and the right MDA slot is number 2.
  - **Values**
    - 1, 2

**mda-type**

**Syntax**
```
mda-type mda-type
no mda-type
```

**Context**
`config>card>mda`

**Description**
This mandatory command provisions a specific MDA type to the device configuration for the slot. The MDA can be preprovisioned but an MDA must be provisioned before ports can be configured. Ports can be configured once the MDA is properly provisioned.

A maximum of two MDAs can be provisioned on an IOM. Only one MDA can be provisioned per IOM MDA slot. To modify an MDA slot, shut down all port associations.
An MDA can only be provisioned in a slot if the MDA type is allowed in the MDA slot. An error message is generated when an MDA is provisioned in a slot where it is not allowed.

A medium severity alarm is generated if an MDA is inserted that does not match the MDA type configured for the slot. This alarm is cleared when the correct MDA is inserted or the configuration is modified.

A high severity alarm is raised when an administratively enabled MDA is removed from the chassis. This alarm is cleared if the either the correct MDA type is inserted or the configuration is modified. A low severity trap is issued if an MDA is removed that is administratively disabled.

An alarm is raised if partial or complete MDA failure is detected. The alarm is cleared when the error condition ceases.

All parameters in the MDA context remain and if non-default values are required then their configuration remains as it is on all existing MDAs.

The `no` form of this command deletes the MDA from the configuration. The MDA must be administratively shut down before it can be deleted from the configuration.

**Default**

No MD types are configured for any slots by default.

**Parameters**

`mda-type` — The type of MDA selected for the slot position.

**7750:** m60-10/100eth-tx, m10-1gb-sfp, m16-oc12/3-sfp, m8-oc12/3-sfp, m16-oc3-sfp, m8-oc3-sfp, m4-oc48-sfp, m1-oc192, m5-1gb-tx, m12-chds3, m1-choc12-sfp, m1-10gb, m4-choc3-sfp, m2-oc48-sfp, m20-100eth-sfp, m20-1gb-tx, m2-10gb-xfp, m4-atmoc12/3-sfp, m16-atmoc3-sfp, m20-1gb-sfp, m4-chds3, m1-10gb-xfp, vsm-cca, 5-1gb-sfp-b, m10-1gb-sfp-b, m4-choc3-as-sfp, m10-1gb+1-10gb, isa-ipsec, m1-choc12-as-sfp, m12-chds3-as, m4-chds3-as, m10-1gb-hs-sfp, m1-10gb-hs-xfp, m4-choc3-ces-sfp, m1-choc3-ces-sfp, m4-10gb-xp-xfp, m2-10gb-xp-xfp, m1-10gb-xp-xfp, m10-1gb-xp-sfp, m20-1gb-xp-sfp, m20-1gb-xp-tx, m1-choc12-ces-sfp, imm24-1gb-xp-xfp, imm4-10gb-xp-xfp, imm2-10gb-xp-xfp, isa-ms

**7450:** m60-10/100eth-tx, m10-1gb-sfp, m16-oc12/3-sfp, m8-oc12/3-sfp, m16-oc3-sfp, m4-oc48-sfp, m1-10gb, m2-oc48-sfp, m20-100eth-sfp, m20-1gb-tx, m2-10gb-xfp, m20-1gb-sfp, m1-10gb-xfp, vsm-cca, m5-1gb-sfp-b, m10-1gb-sfp-b, m10-1gb+1-10gb, m10-1gb-hs-sfp, m1-10gb-hs-xfp, m4-10gb-xp-xfp, m2-10gb-xp-xfp, m1-10gb-xp-xfp, m1-10gb-xp-sfp, m20-1gb-xp-sfp, m20-1gb-xp-tx, m1-choc12-ces-sfp, imm24-1gb-xp-xfp, imm4-10gb-xp-xfp, imm2-10gb-xp-xfp, isa-ms
**LNS GROUP COMMANDS**

**lns-group**

**Syntax**

`lns-group` **ins-group-id** [create]
`no lns-group` **ins-group-id**

**Context**

`config>isa`

**Description**

This command configures the ISA LNS group.

**Parameters**

`ins-group-id` — Specified the LNS group ID.

**Values**

1 — 4

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

**mda**

**Syntax**

`mda` **mda-id** [drain]
`no mda` **mda-id**

**Context**

`config>isa>lns-group`

**Description**

This command configures an ISA LNS group MDA.

**Parameters**

`mda-id` — Specifies the slot and MDA number for the primary video group ISA.

**Values**

<table>
<thead>
<tr>
<th>slot/mda</th>
</tr>
</thead>
<tbody>
<tr>
<td>slot 1 — 10</td>
</tr>
<tr>
<td>mda 1 — 2</td>
</tr>
</tbody>
</table>
VIDEO GROUP COMMANDS

video-group

Syntax  
video-group video-group-id [create]
no video-group video-group-id

Context  config>isa

Description  This command configures an ISA video group.

Parameters  
video-group-id — Specifies a video group ID.

Values  1 — 4

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

ad-insert

Syntax  
[no] ad-insert

Context  config>isa>video-group

Description  This command enables the ad insert server for the group. Ad insertion cannot be enabled if an FCC server or local RT server is enabled.

The no form of the command disables the server.

analyzer

Syntax  
[no] analyzer

Context  config>isa>video-group

Description  This command specifies whether or not the video analyzer is enabled for all streams on this video group.

The no form of the command disables the analyzer for the group.

Default  no analyzer

fcc-server

Syntax  
[no] fcc-server

Context  config>isa>video-group
Video Services Command Descriptions

**Description**

This command enables the FCC server capability for the ISA video group. FCC server cannot be enabled if ad insertion or the local RET server is enabled.

FCC Server parameters can be configured in a multicast information policy or a service, but the parameters will have no effect if the FCC server is disabled or if the video group is administratively disabled (shutdown).

The **no** form of the command disables the FCC server.

**Default**

no fcc-server

---

**local-rt-server**

**Syntax**

[no] local-rt-server

**Context**

config>isa>video-group

**Description**

This command enables the local RET server for the group. A local RET server cannot be enabled if an FCC server or ad insertion is enabled.

The **no** form of the command disables the server.

---

**primary**

**Syntax**

[no] primary mda-id

**Context**

config>isa>video-group

**Description**

This command configures the primary video group ISA. Only one primary can be configured per video group when ad insertion is enabled. The maximum number of primaries per video-group for FCC and RD is 4.

**Parameters**

*mda-id* — Specifies the slot and MDA number for the primary video group ISA.

**Values**

*slot/mda*  
slot | 1 — 10 (depending on the chassis model)  
mda | 1 — 2

---

**resv-ret**

**Syntax**

resv-ret resv-ret

**Context**

config>isa>video-group

**Description**

This command provides a mechanism to reserve an explicit amount of egress bandwidth for RET for all the ISAs within a video group. If the amount of egress bandwidth is less than the reserved amount, FCC requests are discarded and only RET requests processed. The bandwidth is dynamically adjusted per ISA within the video group if an ISA becomes operational/non-operational within the group.
stream-selection

Syntax      [no] stream-selection
Context     config>isa>video-group
Description  This command specifies whether or not stream selection is enabled on this video group.
             The no form of the command disables stream-selection for the group.
Default     no stream-selection
MULTICAST INFO POLICY COMMANDS

multicast-info-policy

Syntax

```
multicast-info-policy policy-name [create]
no multicast-info-policy policy-name
```

Context

```
cfg> mcast-management
```

Description

This command configures a multicast information policy. Multicast information policies are used to manage parameters associated with Layer 2 and Layer 3 multicast records. Multiple features use the configured information within the policy. The multicast ingress path manager uses the policy to decide the inactive and active state behavior for each multicast record using the ingress paths to the switch fabric. The egress multicast CAC function may use the policy information as a basis for allowing or disallowing downstream nodes to join multicast streams. The system’s multicast ECMP join decisions are influenced by the channel information contained within the policy.

Multicast Bundles:

A multicast information policy consists of one or multiple named bundles. Multicast streams are mapped to a bundle based on matching the destination address of the multicast stream to configured channel ranges defined within the bundles. Each policy has a bundle named ‘default’ that is used when a destination address does not fall within any of the configured channel ranges.

Each bundle has a set of default parameters used as the starting point for multicast channels matching the bundle. The default parameters may be overridden by optional exception parameters defined under each channel range. Further optional parameter overrides are possible under explicit source address contexts within each channel range.

Default Multicast Information Policy

A multicast information policy always exists with the name ‘default’ and cannot be edited or deleted. The following parameters are contained in the default multicast information policy:

- Policy Description: Default policy, cannot be edited or deleted.
- Bundle: default
- Bundle Description: Default Bundle, cannot be edited or deleted.
- Congestion-Priority-Threshold: 4
- ECMP-Optimization-Limit-Threshold: 7

Bundle Defaults:

- Administrative Bandwidth: 0 (undefined)
- Preference: 0
- CAC-Type: Optional
- Bandwidth Activity: Dynamic with no black-hole rate
- Explicit Ingress SF Path: None (undefined)
- Configured Channel Ranges: None

The default multicast information policy is applied to all VPLS and VPRN services and all routing contexts until an explicitly defined multicast information policy has been mapped.

Explicit Multicast Information Policy Associations

Each VPLS service and each routing context (including VPRN routing contexts) supports an explicit association with an pre-existing multicast information policy. The policy may need to be
unique per service or routing context due to the fact that each context has its own multicast address space. The same multicast channels may be and most likely will be used for completely different multicast streams and applications in each forwarding context.

Interaction with Ingress Multicast Path Management

When ingress multicast path management is enabled on an MDA, the system automatically creates a bandwidth manager context that manages the multicast path bandwidth into the switch fabric used by the ingress ports on the MDA. As routing or snooping protocols generate L2 or L3 multicast FIB records that will be populated on the MDA's forwarding plane, they are processed though the multicast information policy that is associated with the service or routing context associated with the record. The policy will return the following information for the record to be used by the ingress bandwidth manager:

- The records administrative bandwidth (‘0’ if undefined)
- Preference level (0 to 7 with 7 being highest)
- Bandwidth activity monitoring setting (use admin bw or dynamic monitoring)
  If admin bw is indicated, will also return active and inactive thresholds
- Initial switch fabric multicast path (primary, secondary or ancillary)
  If ancillary path is indicated, will also return an SF destination threshold
- Explicit switch fabric multicast path (primary, secondary, ancillary or none)

Interaction with Egress Multicast CAC

The egress multicast CAC feature has its own multicast CAC policy that is applied to egress IP interfaces or egress VPLS interfaces. The policy contains bundles, each with their own sets of channel ranges defined. When a multicast joint event occurs on the interface, the system searches the multicast CAC policy to determine how that join event should be processed. The information returned from the CAC lookup provides the bundles allowed bandwidth and the channels administrative bandwidth. Since the allowed bundle bandwidth may change between differing egress interfaces, multiple policies with the same channel information may be needed.

With the addition of the multicast information policy, managing the CAC feature is simplified. The CAC monitor for the egress interface first searches the multicast CAC policy to determine if the multicast join event matches a configured channel range. If a match is found, it simply uses the local policy information. If a match is not found, it then searches the multicast information policy associated with the service or routing context to which the join event is associated. The multicast information policy returns the following information to the interfaces CAC manager:

- Bundle name
- Administrative bandwidth (‘0’ if undefined)
- Congestion Priority Threshold (high or low)
- CAC Type (mandatory or optional)

The CAC manager evaluates the returned results according to the following rules:

- If the returned administrative bandwidth = ‘0’, all results are ignored
- If the returned bundle name is not found in the local multicast CAC policy, all results are ignored
- The administrative bandwidth is interpreted as channel ‘bw’
- A value of ‘high’ for congestion priority threshold is interpreted as ‘class high’
- A value of ‘low’ for congestion priority threshold is interpreted as ‘class low’
- A value of ‘mandatory’ for CAC type is interpreted as ‘type mandatory’
Using the multicast information policy to store the CAC information allows a single centralized managed policy for all channel information, allowing the multicast CAC policies to only have bundle defined with the appropriate bundle bandwidth. The multicast CAC policy still may be for channel information in exception cases.

Interaction with Multicast ECMP Optimization

The multicast information policy is used by the multicast ECMP optimization function to derive each channels administrative bandwidth. The ECMP function tallies all bandwidth information for channels joined and attempts to equalize the load between the various paths to the sender. The multicast information policy returns the following information to the ECMP path manager:

5. Administrative bandwidth (‘0’ if undefined)
6. Preference (0 to 7 with 7 the highest preference value)

Parameters

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>policy-name</td>
<td>Identifies the name of the policy to be either created or edited. Each multicast information policy must be uniquely named within the system. Names of up to 32 ASCII characters are supported with the normal character restrictions.</td>
</tr>
<tr>
<td>create</td>
<td>The create keyword is required if creating a new multicast information policy when the system is configured to require the explicit use of the keyword to prevent accidental object creation. Objects may be accidentally created when this protection is disabled and an object name is mistyped when attempting to edit the object. This keyword is not required when the protection is disabled. The keyword is ignored when the multicast information policy name already exists.</td>
</tr>
</tbody>
</table>

**multicast-info-policy**

**Syntax**

multicast-info-policy policy-name

no multicast-info-policy

**Context**

config>service>ies
config>service>vpls
config>service>vprn
config>router

**Description**

This command overrides the default multicast information policy on a service or routing context. When the policy association is changed, all multicast channels in the service or routing context must be reevaluated.

If a multicast information policy is not explicitly associated with the service or routing context, the default multicast information policy is used when ingress multicast path management is enabled.

While a multicast information policy is associated with a service or routing context, the policy cannot be deleted from the system.

The no form of the command removes an explicit multicast information policy from the service or routing context and restores the default multicast information policy.

**Parameters**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>policy-name</td>
<td>The policy-name parameter is required and specifies an existing multicast information policy that should be associated with the service or routing context.</td>
</tr>
</tbody>
</table>

**Default**

default
bundle

**Syntax**

```
bundle bundle-name [create]
no bundle bundle-name
```

**Context**

```
config>mcast-mgmt>mcast-info-plcy
```

**Description**

The `bundle` command is used to create or edit channel bundles within a multicast information policy. Bundles are used for two main purposes. First, bundles are used by the multicast CAC function to group multicast channels into a common bandwidth context. The CAC function limits the ability for downstream nodes to join multicast channels based on the egress interfaces ability to handle the multicast traffic. Bundling allows multicast channels with common preference or application to be managed into a certain percentage of the available bandwidth.

The second function of bundles is to provide a simple provisioning mechanism. Each bundle within a multicast information policy has a set of default channel parameters. If each channel provisioned in to the bundle is able to use the default parameters for the bundle, the provisioning and configuration storage requirements are minimized.

Up to 31 explicit bundles may be defined within a multicast information policy (32 including the default bundle).

Once a bundle is created, the default channel parameters should be configured and the individual channel ranges should be defined. Within each channel range, override parameters may be defined that override the default channel parameters. Further overrides are supported within the channel range based on explicit source overrides.

A bundle may be deleted at anytime (except for the default bundle). When a bundle is deleted, all configuration information within the bundle is removed including multicast channel ranges. Any multicast records using the bundle should be reevaluated. Multicast CAC and ECMP managers should also be updated.

**Default Bundle**

Each multicast information policy contains a bundle named `default`. The default bundle cannot be deleted. Any multicast channel that fails to match a channel range within an explicit bundle is automatically associated with the default bundle.

The `no` form of the command removes a bundle from the multicast information policy. The default bundle cannot be removed from the policy.

**Default**

```
default
```

`bundle-name` — Specifies bundle expressed as an ASCII string with up to 16 characters and must follow normal naming conventions. If `bundle-name` already exists, the system will enter the bundle context for editing purposes. If `bundle-name` does not exist, the system will create the defined bundle in the policy and enter the bundle context for editing purposes.

`create` — The create keyword is required if creating a new multicast information policy bundle when the system is configured to require the explicit use of the keyword to prevent accidental object creation. Objects may be accidentally created when this protection is disabled and an object name is mistyped when attempting to edit the object. This keyword is not required when the protection is disabled. The keyword is ignored when the bundle name already exists.
admin-bw

Syntax

admin-bw kbps
no admin-bw

Context

config>mcast-mgmt>mcast-info-plcy
config>mcast-mgmt>mcast-info-plcy>channel

Description

This command configures the administrative bandwidth.

Parameters

kbps — Specifies the administrative bandwidth in Kbps.

Values

1 — 40000000

bw-activity

Syntax

bw-activity {use-admin-bw | dynamic [falling-delay seconds]} [black-hole-rate kbps]

no bw-activity

Context

config>mcast-mgmt>mcast-info-plcy>bundle
config>mcast-mgmt>mcast-info-plcy>channel

Description

This command defines how the multicast ingress path manager determines the amount of bandwidth required by a multicast channel. The default setting is dynamic which causes the bandwidth manager to adjust the path bandwidth based on the current ingress multicast bandwidth. The alternative setting is use-admin-bw which causes the bandwidth manager to use the configured admin-bw associated with the channel. The use-admin-bw setting is enabled once the channels ingress bandwidth reaches the bandwidth-policy admin-bw-threshold value. The bandwidth manager uses the dynamic method until the threshold has been reached. If the ingress bandwidth falls below the threshold, the bandwidth manager reverts back to the dynamic method.

While operating in dynamic bandwidth mode, the bandwidth manager uses the falling-delay threshold to hold on to the previous highest bandwidth until the delay time has expired. This allows the bandwidth manager ignore momentary drops in channel bandwidth.

The bw-activity command in the bundle context defines how the current bandwidth is derived for all channels associated with the bundle unless the channel has an overriding bw-activity defined in the channel context. The channel context may also be overridden by the bw-activity command in the source-override context for a specific channel or channel range. The channel and source-override bw-activity settings default to ‘null’ (undefined) and have no effect unless explicitly set. The default-channel-info bw-activity default value is set to dynamic.

The use-admin-bw setting requires that the channel be configured with an admin-bw value that is not equal to ‘0’ in the same context as the bw-activity command using the setting. If use-admin-bw is defined in the default-channel-info context, then the default-channel-info admin-bw setting must not be set to ‘0’. A similar rule applies for channel and source-override bw-activity and admin-bw settings. Once a context has use-admin-bw configured, the context’s admin-bw value cannot be set to ‘0’ and the no admin-bw command will fail for that context.

The bw-activity command also supports an optional black-hole-rate kilobits-per-second keyword and parameter that defines at which current rate a channel should be placed in the black-hole state. This is intended to provide a protection mechanism against multicast channels that exceed a reasonable rate and cause outages in other channels.
The **no** form of the command reverts to the default parameters.

### channel

**Syntax**
```
channel ip-address [ip-address] [create]
noc channel ip-address [ip-address]
```

**Context**
```
config>mcast-mgmt>mcast-info-plcy>bundle
```

**Description**
This command defines explicit channels or channel ranges that are associated with the containing bundle. A channel or channel range is defined by their destination IP addresses. A channel may be defined using either IPv4 or IPv6 addresses. If a channel range is being defined, both the start and ending addresses must be the same type.

A specific channel may only be defined within a single channel or channel range within the multicast information policy. A defined channel range cannot overlap with an existing channel range.

If a channel range is to be shortened, extended, split or moved to another bundle, it must first be removed from its existing bundle.

Each specified channel range creates a containing context for any override parameters for the channel range. By default, no override parameters exist.

The **no** form of the command removes the specified multicast channel from the containing bundle.

**Parameters**

- **start-channel-ip-address**
  - The `start-channel-ip-address` parameter and optional `end-channel-ip-address` parameters define the starting and ending destination IP addresses for a channel range.

  - If only the `start-channel-ip-address` is given, the channel ranges comprises of a single multicast channel.

  - If both the starting and ending address are specified, all addresses within the range including the specified address are part of the channel range.

  - IPv4 or IPv6 addresses may be defined. All specified addresses must be valid multicast destination addresses. The starting IP address must be numerically lower then the ending IP address. [What do we do with 224.0.0.x addresses?]

  - **Values**
    - Any valid IP multicast destination address

  - **Default**
    - None

- **create**
  - The `create` keyword is required if creating a new multicast channel range when the system is configured to require the explicit use of the keyword to prevent accidental object creation.

  - Objects may be accidentally created when this protection is disabled and an object name is mistyped when attempting to edit the object. This keyword is not required when the protection is disabled. The keyword is ignored when the specified channel range already exists.
source-override

**Syntax**

source-override ip-address [create]
no source-override ip-address

**Context**

config>mcast-mgmt>mcast-info-plcy>bundle>channel

**Description**

This command defines a multicast channel parameter override context for a specific multicast sender within the channel range. The specified sender's IP address must be of the same type (IPv4 or IPv6) as the containing channel range.

The `no` form of the command removes the specified sender override context from the channel range.

**Default**

none

**Parameters**

*ip-address* — Specifies either an IPv4 or IPv6 address and it must be the same type as the containing channel range.

**Values**

ipv4-address a.b.c.d
ipv6-address x:x:x:x:x:x:x (eight 16-bit pieces)

create — The create keyword is required if creating a new source override when the system is configured to require the explicit use of the keyword to prevent accidental object creation. Objects may be accidentally created when this protection is disabled and an object name is mistyped when attempting to edit the object. This keyword is not required when the protection is disabled. The keyword is ignored when the specified source override IP address already exists.
**VIDEO POLICY COMMANDS**

### video-policy

**Syntax**

```plaintext
video-policy
```

**Context**

```plaintext
config>mcast-mgmt>mcast-info-plcy
```

**Description**

This command enables the context to configure video interfaces and video services.

### video-interface

**Syntax**

```plaintext
video-interface ip-address [create]  
no video-interface ip-address
```

**Context**

```plaintext
config>mcast-mgmt>mcast-info-plcy>video-policy
```

**Description**

This command creates a video interface policy context that correlates to the IP address assigned for a video interface. This interface is created in a subscriber service to which the multicast information policy is assigned. If the specified IP address does not correlate to a video interface ip address, the parameters defined within this context have no effect.

The `no` form of the command deletes the video interface policy context.

**Parameters**

- `ip-address` — The IP address of a video interface provisioned within the context of a service to which the Multicast Information Policy is assigned. If the IP address does not match the IP address assigned to a video interface, the parameters defined within this context have no effect.
- `create` — Mandatory keyword needed when creating a new video interface within the video policy.

### hd

**Syntax**

```plaintext
hd
```

**Context**

```plaintext
config>mcast-mgmt>mcast-info-plcy>video-policy>video-if
```

**Description**

This command configures properties relating to requests received by the video interface for High Definition (HD) channel requests.

**Default**

none

### dent-threshold

**Syntax**

```plaintext
dent-threshold threshold
no dent-threshold
```

**Context**

```plaintext
config>mcast-mgmt>mcast-info-plcy>video-policy>video-if>hd
```

---

OS Multi-Service ISA Guide
config>mcast-mgmt>mcast-info-plcy>video-policy>video-if>pip
config>mcast-mgmt>mcast-info-plcy>video-policy>video-if>sd

**Description**
This command sets the threshold value below which the FCC server will dent/drop unicast data sent to the FCC client during a fast channel change. Within the RTP extension header, the packet priority (PRI) (2 bits) and the fine-grained priority (FPRI) (3 bits) indicate the “importance” of the frame as to how essential it is to the video stream.

This parameter is only applicable if the FCC server mode is **dent**.

The **no** form of the command returns the parameter to the default value.

**Default**
16 (only B frames are dropped)

**Parameters**
- **threshold** — The threshold value is used by the FCC server to compare with the concatenation of the PRI and FPRI to determine whether to send the packet to the FCC client. If the PRI and FPRI expressed as a decimal integer is greater than or equal to the threshold value, the packet will be sent.

**Values**
1 — 31

---

### fcc-burst

**Syntax**
```plaintext
fcc-burst burst-percentage
no fcc-burst
```

**Context**
- config>mcast-mgmt>mcast-info-plcy>video-policy>video-if>hd
- config>mcast-mgmt>mcast-info-plcy>video-policy>video-if>pip
- config>mcast-mgmt>mcast-info-plcy>video-policy>video-if>sd

**Description**
This command sets the burst rate at which the Fast Channel Change (FCC) server will send unicast data to the FCC client above the received rate to allow the client to catchup to the multicast stream.

This parameter is only applicable if the FCC server mode is **burst**.

The **no** form of the command returns the parameter to the default value.

**Default**
25

**Parameters**
- **burst-percentage** — Specifies the percentage of nominal bandwidth used to catch up to the multicast stream.

**Values**
- HD: 0 — 100
- SD and PIP: 0 — 600

**Default**
25

---

### fcc-server

**Syntax**
```plaintext
fcc-server [mode {burst | dent | hybrid}]
no fcc-server
```

**Context**
- config>mcast-mgmt>mcast-info-plcy>video-policy>video-if>hd
- config>mcast-mgmt>mcast-info-plcy>video-policy>video-if>pip
config>mcast-mgmt>mcast-info-plcy>video-policy>video-if>sd

**Description**

This command enables the Fast Channel Change (FCC) server and sets the mode to send the FCC unicast stream.

The mode indicates how the FCC server will send information to the client. When **burst** is specified, the FCC server will send the channel at a nominally faster rate than the channel was received based on the applicable fcc-burst setting. When **dent** is specified, the FCC server will selectively discard frames from the original stream based on the applicable dent-threshold setting. If no mode is specified, burst is the default mode.

The **no** form of the command disables the FCC server at that context and subordinate contexts.

**Default**

no fcc-server

**Parameters**

mode burst — Sets the mode of the FCC server to burst when sending the channel to the FCC client.

mode dent — Sets the mode of the FCC server to dent when sending the channel to the FCC client.

mode hybrid — Combines the burst and dent modes.

---

**local-rt-server**

**Syntax**

[no] local-rt-server

**Context**

config>mcast-mgmt>mcast-info-plcy>video-policy>video-if>hd
config>mcast-mgmt>mcast-info-plcy>video-policy>video-if>pip
config>mcast-mgmt>mcast-info-plcy>video-policy>video-if>sd

**Description**

This command enables the local retransmission server function for requests directed to the IP address. The **no** form of the command disables the retransmission server.

**Default**

no local-rt-server

---

**mc-handover**

**Syntax**

mc-handover percentage

no mc-handover

**Context**

config>mcast-mgmt>mcast-info-plcy>video-policy>video-if>hd
config>mcast-mgmt>mcast-info-plcy>video-policy>video-if>pip
config>mcast-mgmt>mcast-info-plcy>video-policy>video-if>sd

**Description**

This command sets the rate at which the Fast Channel Change (FCC) server will send unicast data to the FCC client during the handover to the multicast stream. The **no** form of the command returns the parameter to the default value.

**Parameters**

percentage — Specifies the percentage of nominal bandwidth.

**Values**

- HD: 0 — 100
- SD and PIP: 0 — 600

**Default**

25
rt-mcast-reply

Syntax

```
rt-mcast-reply [count count] [interval milliseconds] [hold-time milliseconds]
no rt-mcast-reply
```

Context

```
config>mcast-mgmt>mcast-info-plcy>video-policy>video-if
```

Description

This command enables the use of multicast retransmission packets by the retransmission server in response to a number of identical retransmission requests.

By default, the retransmission server replies to all retransmission requests with a unicast stream directed to the client requesting retransmission. Enabling multicast retransmission on the retransmission server is an optimization where a number of identical retransmission requests received will trigger the retransmission server to service the retransmission request with a single multicast reply stream with packets of Payload Type 33. An example of where multiple clients will request retransmission for identical packets is if there is a packet loss in the Access Network which affects multiple clients.

For clients that received the original packets or requested retransmission and had the retransmission serviced in unicast, the multicast retransmission will look like duplicate packets and discard the multicast retransmitted packets. For other clients, the multicast retransmission will look like out-of-sequence multicast packets, so the client must support reception of out of sequence multicast for multicast retransmission to be used.

The threshold value for identical retransmission requested received by the retransmission server is configured when enabling multicast retransmission along with a sample interval and a hold time. The sample interval is the elapsed time over which the retransmission requests are counted. The hold time is a quiet period after a multicast retransmission is triggered on the retransmission server where an identical retransmission request will be ignored. After the hold time expires, a new sampling interval is started. Sampling intervals will be restarted until the packets for the multicast request are cleared from the retransmission buffer.

To illustrate the threshold count, sample interval and hold time, suppose the values are 5, 100 ms and 50 ms, respectively. The first retransmission request arrives at time = 0. In one scenario, assume the fifth identical retransmission request arrives at the server at time = 60 ms. In this case, the first four retransmission requests are serviced as unicast and the arrival of the fifth retransmission request triggers a multicast retransmission. All identical retransmission requests received between time = 60 and 110 ms are ignored. At time = 110 ms, a new sampling period is started and retransmission requests are serviced in unicast unless the threshold is passed again in the new sampling period. For a second scenario, assume the fifth identical retransmission request arrives at time = 25 ms. In this scenario, the behavior is the same except the new sampling period starts at time = 75 ms even though this is before the original sampling period was set to expire.

The no form of the command disables retransmissions using multicast, so all retransmissions will be sent as unicast.

Default

```
no rt-mcast-reply – Retransmission requests will only be serviced with unicast retransmission replies.
```

Parameters

```
count count — Specifies the number of identical retransmission requests received for a packet in a sampling interval after which a reply will be sent as multicast Payload Type 33.
```

Values

```
2 – 1024
```

Default

```
5
```

```
interval milliseconds — Specifies the number of milliseconds for a sampling interval.
```

```
Values
```

```
0 – 1024
```

Default

```
100
```

```
hold-time milliseconds — Specifies the number of milliseconds for a hold time.
```

```
Values
```

```
0 – 1024
```

Default

```
100
```
rt-payload-type

Syntax rt-payload-type payload-type
no rt-payload-type

Context config>mcast-mgmt>mcast-info-plcy>video-policy>video-if

Description This command describes the format to be used by Retransmission (RT) server to send retransmission packets. The RET server interface allows the payload type within the retransmission packets to be configured.

Default 99 — Indicates that the frames will be sent in the RFC 4588, RTP Retransmission Payload Format, format.

Parameters payload-type — Indicates the format expected for received retransmission packets. The value 33 indicates that the frames will be received as originally sent. A value between 96 and 127 indicates the dynamic payload type value (per RFC 3551) to be used for RFC 4588 formatted retransmission packets.

Values 33, 96 – 127

rt-rate

Syntax rt-rate rt-burst-percentage
no rt-rate

Context config>mcast-mgmt>mcast-info-plcy>video-policy>video-if>hd
config>mcast-mgmt>mcast-info-plcy>video-policy>video-if>pip
config>mcast-mgmt>mcast-info-plcy>video-policy>video-if
config>mcast-mgmt>mcast-info-plcy>video-policy>video-if>sd

Description This command sets the rate of nominal bandwidth at which retransmission packets are sent to the retransmission client for requests directed to the IP address.

The no form of the command returns the parameter to the default value.

Default 5

Parameters rt-burst-percentage — Specifies the percentage of nominal bandwidth to send retransmission packets.

Values 1— 100

Default 5
max-sessions

Syntax

max-sessions sessions
no max-sessions

Context
config>mcast-mgmt>mcast-info-plcy>video-policy>video-if

Description
This command configures the per-client maximum number of sessions. The no form of the command reverts to the default value.

Parameters

sessions — Specifies the per-client maximum number of sessions.

Values

1 — 65536

Default

256

pip

Syntax

pip

Context
config>mcast-mgmt>mcast-info-plcy>video-policy>video-if

Description
This command enables the context within a video interface policy to configure properties relating to requests received by the video interface for Picture-in-Picture (PIP) channel requests.

Default
none

sd

Syntax

sd

Context
config>mcast-mgmt>mcast-info-plcy>video-policy>video-if

Description
This command enables the context within a video interface policy to configure properties relating to requests received by the video interface for Standard Definition (SD) channel requests.

subscriber-bw-limit

Syntax

subscriber-bw-limit bandwidth
no subscriber-bw-limit

Default
config>mcast-mgmt>mcast-info-plcy>video-policy>video-if

Description
This command configures an egress per-subscriber bandwidth limit for the combined retransmission and Fast Channel Change (FCC) replies for requests received directed to the IP address. If the bandwidth for a request will exceed the bandwidth limit, the request is logged and dropped.

The no form of the command disables enforcement of an egress bandwidth limit.
<table>
<thead>
<tr>
<th>Default</th>
<th>4294967295</th>
</tr>
</thead>
</table>

**Parameters**

*bandwidth* — The per-subscriber egress bandwidth limit for retransmission and FCC packets in kilobits per second expressed as an integer indicates infinity or no limit.

**Values**

1 — 4294967295 kbps
**BUNDLE AND CHANNEL COMMANDS**

**video**

**Syntax**  
`video`

**Context**  
`config>mcast-mgmt>mcast-info-plcy>bundle`  
`config>mcast-mgmt>mcast-info-plcy>bundle>channel`  
`config>mcast-mgmt>mcast-info-plcy>bundle>channel>source-override`

**Description**  
This command enables the context to configure video parameters.

**fcc-channel-type**

**Syntax**
```
fcc-channel-type {hd | sd | pip}
```  
`no fcc-channel-type`

**Context**  
`config>mcast-mgmt>mcast-info-plcy>bundle>video`  
`config>mcast-mgmt>mcast-info-plcy>bundle>channel>video`  
`config>mcast-mgmt>mcast-info-plcy>bundle>channel>source-override>video`

**Description**  
This command configures the channel type for the bundle/channel. The channel type is used in the video policy to set various Fast Channel Change (FCC) parameters including the type of FCC and various FCC rates.

The no form of the command returns the parameter to the default value.

**Default**  
`no fcc-channel`

**Parameters**
- `hd` — The channel type is High-Definition (HD) (Default).
- `sd` — The channel type is Standard Definition (SD).
- `pip` — The channel type is Picture in Picture (PIP).

**fcc-min-duration**

**Syntax**
```
fcc-min-duration time
```  
`no fcc-min-duration`

**Context**  
`config>mcast-mgmt>mcast-info-plcy>bundle>video`  
`config>mcast-mgmt>mcast-info-plcy>bundle>channel>video`

**Description**  
This command configures the minimum time duration, in milliseconds, of the Fast Channel Change (FCC) burst. The value of this object determines the starting point of the FCC burst. If the current Group of Pictures (GOP) has less than the minimum duration worth of data, FCC burst begins from the previous GOP.

The no form of the command reverts to the default value.
Default 300

Parameters

\textit{time} — Specifies the FCC burst minimum duration, in milliseconds.

\begin{itemize}
  \item \textbf{Values} \hspace{1cm} 300 — 8000
\end{itemize}

\begin{description}

\item[local-fcc-port]

\begin{itemize}
  \item \textbf{Syntax} \hspace{1cm} \texttt{local-fcc-port \textit{port}}
  \item \texttt{no local-fcc-port}
\end{itemize}

\begin{itemize}
  \item \textbf{Context} \hspace{1cm} \texttt{config>mcast-mgmt>mcast-info-plcy>bundle>video}
  \hspace{1cm} \texttt{config>mcast-mgmt>mcast-info-plcy>bundle>channel>video}
  \hspace{1cm} \texttt{config>mcast-mgmt>mcast-info-plcy>bundle>channel>source-override>video}
\end{itemize}

\begin{itemize}
  \item \textbf{Description} \hspace{1cm} This command configures the local port on which Fast Channel Change (FCC) requests are received. The value of this object can only be set for the default bundle and will be used by all bundles and channels.
  \hspace{1cm} The local-fcc-port \textit{port} value is the only configuration parameter in the bundle “default” context.
  \hspace{1cm} The \texttt{no} form of the command removes the port from the video configuration.
\end{itemize}

\begin{itemize}
  \item \textbf{Parameters} \hspace{1cm} \textit{port} — Specifies a local port for FCC requests.
  \item \textbf{Values} \hspace{1cm} 1024 — 65535
\end{itemize}

\end{description}
local-rt-port

Syntax

- local-rt-port port
- no local-rt-port

Context

- config>mcast-mgmt>mcast-info-plcy>bundle>video
- config>mcast-mgmt>mcast-info-plcy>bundle>channel>video
- config>mcast-mgmt>mcast-info-plcy>bundle>channel>source-overide>video

Description

This command configures the local port on which retransmission (RET) requests are received. The value of this object can only be set for the default bundle and will be used by all channels.

The local-rt-port port value is the only configuration parameter in the bundle “default” context.

The no form of the command removes the port from the video configuration.

Parameters

- port — Specifies a local port for RT requests.
  
  Values
  
  1024 — 65535

local-rt-server

Syntax

- local-rt-server [disable]
- no local-rt-server

Context

- config>mcast-mgmt>mcast-info-plcy>bundle>video
- config>mcast-mgmt>mcast-info-plcy>bundle>channel>video
- config>mcast-mgmt>mcast-info-plcy>bundle>channel>source-overide>video

Description

This command enables the local retransmission server capability on the ISA video group.

RET server parameters can be configured in a multicast information policy or a service, but the parameters will have no effect if the RET server is disabled or if the video group is administratively disabled (shutdown).

The no form of the command returns the parameter to the default value where the RET server is disabled on the video group.

Default

- no local-rt-server

Parameters

- disable — Specifies to disable the RET server.

reorder-audio

Syntax

- reorder-audio time
- no reorder-audio

Context

- config>mcast-mgmt>mcast-info-plcy>bundle>video
- config>mcast-mgmt>mcast-info-plcy>bundle>channel>video

Description

This command configures the time, in milliseconds, by which the audio packets are reordered in the ad stream.
Configuring this parameter depends on what is configured on the A Server and the GOP sizes of the network stream. Typically, this configuration should match the A Server configuration.

The no form of the command removes the time value from the configuration.

**Default**

no reorder-audio

**Parameters**

time — Specifies the audio reorder time, in milliseconds.

**Values**

100 — 1000

---

**rt-buffer-size**

**Syntax**

rt-buffer-size rt-buffer-size

no rt-buffer-size

**Context**

config>mcast-mgmt>mcast-info-plcy>bundle>channel>video

config>mcast-mgmt>mcast-info-plcy>bundle>channel>source-override>video

**Description**

This command configures the retransmission buffer for channels within the bundle or channel range. The no form of the command returns the parameter to the default value.

**Default**

300

**Parameters**

rt-buffer-size — Specifies the buffer size, in milliseconds, to store channel packets.

**Values**

300 — 8000

---

**rt-server**

**Syntax**

rt-server disable

rt-server ip-address port port-num

no rt-server

**Context**

config>mcast-mgmt>mcast-info-plcy>bundle>video

config>mcast-mgmt>mcast-info-plcy>bundle>channel>video

config>mcast-mgmt>mcast-info-plcy>bundle>channel>source-override>video

**Description**

This command enables and configures the upstream retransmission server configuration parameters. The no form of the command removes the upstream retransmission server configuration and implies the configuration is inherited from a higher context or from the default policy.

**Default**

no rt-server – The upstream retransmission server settings are inherited.

**Parameters**

disable — This keyword explicitly disables the upstream retransmission server within the policy. For the default bundle within the default Multicast Information Policy, the no form of the command and the disable keyword have the same meaning and imply the server is disabled.

ip-address — The IP address of the upstream retransmission server.

port num — The UDP port to use to send RET requests to the upstream RET server.

**Values**

1024 — 65535
source-port

Syntax

source-port port-num
no source-port

Context
config>mcast-mgmt>mcast-info-plcy>bundle>video

Description
This command configures the source port for upstream RET requests.
The source-port port-num value is the only configuration parameter in the bundle “default” context.
The no form of the command removes the value from the configuration.

Parameters

port-num — Specifies the source port in the received RTP multicast stream.

Values
1024 — 65535

video-group

Syntax

video-group video-group-id
video-group disable
no video-group

Context
config>mcast-mgmt>mcast-info-plcy>bundle>video
config>mcast-mgmt>mcast-info-plcy>bundle>channel>video
config>mcast-mgmt>mcast-info-plcy>bundle>channel>source-override>video

Description
This command assigns a video group ID to the channel.

Parameters

video-group-id — Specifies the identifier for this video group. The video group must have been configured in the config>isa context.

Values
1 — 4

disable — Explicitly disables the video group within the policy.
SERVICE VIDEO INTERFACE COMMANDS

video-interface

Syntax

video-interface ip-int-name [create]
no video-interface ip-int-name

Context

config>service>ies
config>service>vpls
config>service>vprn

Description

This command creates a video interface within the service. The video interface and associated IP addresses are the addresses to which clients within the service will send requests.

The video interface must be associated with an ISA group using the video-sap command and have IP addresses for it to be functional.

The no form of the command deletes the video interface. The video interface must be administratively shut down before issuing the no video-interface command.

Default

none

Parameters

ip-int-name — Specifies the name of the video interface up to 32 characters in length. 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 within double quotes.

create — This keyword is mandatory when creating a video interface.

address

Syntax

[no] address ip-address/mask

Context

config>service>ies>video-interface
config>service>vpls>video-interface
config>service>vprn>video-interface

Description

This command assigns an IP address to the video interface within the service. Video interface IP addresses are used by video service clients to direct requests for video server services. Up to 16 IP address/subnets can be defined. Note that the addresses defined must all be distinct and cannot be contained within a previously defined address.

In the VPLS context, only one IP address can be defined for a video interface.

The no form of the command deletes the IP address/subnet from the video interface.

Default

none

Parameters

ip-address — The IP address/subnet of the video interface in dotted decimal notation.

mask — The subnet mask length for the IP address expressed as an integer.
Video Services Command Descriptions

adi

Syntax  
\texttt{adi}

Context  
\texttt{config>service>ies>video-interface}
\texttt{config>service>vprn>video-interface}

Description  
This command enables the context to configure ad insertion (ADI) for the video interface.

channel

Syntax  
\texttt{channel mcast-address source ip-address [channel-name channel-name]}
\texttt{no channel mcast-address source ip-address}

Context  
\texttt{config>service>ies>video-interface>adi}
\texttt{config>service>vprn>video-interface>adi}

Description  
This command configures channel parameters for ad insertion.

Parameters  
- \texttt{mcast-address} — Specifies the multicast address.
- \texttt{source ip-address} — Specifies the source IP address.
- \texttt{channel-name channel-name} — Specifies the channel name up to 32 characters in length.

cpu-protection

Syntax  
\texttt{cpu-protection policy-id}
\texttt{no cpu-protection}

Context  
\texttt{config>service>vpls>video-if}
\texttt{config>service>ies>video-if}
\texttt{config>service>vprn>video-if}

Description  
This command assigns an existing CPU protection policy to the associated service video interface. The CPU protection policies are configured in the \texttt{config>sys>security>cpu-protection>policy cpu-protection-policy-id} context. The number of RTCP messages per client will be limited to the number as configured under the policy.

Default  
none

Parameters  
- \texttt{policy-id} — Specifies a CPU protection policy.

Values  
- \texttt{1 — 255}

scte35-action

Syntax  
\texttt{scte35-action \{forward | drop\}}

Context  
\texttt{config>service>ies>video-interface>adi>channel}
config>service>vprn>video-interface>adi>channel

**Description**
This command specifies whether the Society of Cable Telecommunications Engineers 35 (SCTE 35) cue avails in the stream need to be forwarded or not. When specified to forward, SCTE 35 messages will be forwarded downstream. When specified to drop, SCTE 35 messages will not be forwarded downstream. They will be still be processed for local splicing decisions.

**Parameters**
- **forward** — Forwards SCTE 35 messages downstream.
- **drop** — Drops SCTE 35 messages.

---

**zone-channel**

**Syntax**
```bash
zone-channel mcast-address source ip-address adi-channel-name channel-name
```
```
no zone-channel mcast-address source ip-address
```

**Context**
config>service>ies>video-interface>adi>channel
config>service>vprn>video-interface>adi>channel

**Description**
This command configures zone-channel parameters or ad insertion. The channel configuration along with the zone-channel configuration associates a network channel to a zone-channel and builds the store and forward relationship.

**Parameters**
- **mcast-address** — Specifies the IP multicast group address for which this entry contains information.
- **source ip-address** — Specifies the type of address to be used for a source address/
- **adi-channel-name channel-name** — Specifies the name for this zone channel.

---

**scte30**

**Syntax**
```bash
scte30
```

**Context**
config>service>ies>video-interface>adi
config>service>vprn>video-interface>adi

**Description**
This command enables the context to configure SCTE 30 parameters.

---

**ad-server**

**Syntax**
```bash
[no] ad-server ip-address
```

**Context**
config>service>ies>video-interface>adi>scte30
config>service>vprn>video-interface>adi>scte30

**Description**
This command configures the ad server address. A TCP session will be accepted for SCTE 30 messaging only for IP addresses that appear in this configuration.

The **no** form of the command removes the address from the ad server configuration.

**Parameters**
- **ip-address** — Specifies the IP address of the ad server.
local-address

Syntax:  
local-address control ip-address data ip-address
no local-address

Context:  
config>service>ies>video-interface>adi>scte30
config>service>vprn>video-interface>adi>scte30

Description:  
SCTE 30 requires a TCP session per zone-channel between the ad server and splicer for control communication and it requires UDP sessions on which the video ad stream is sent. This command specifies the splicer’s control IP address to which the ad-server(s) should setup TCP connections and the data IP address to which the video ad streams should be sent.

The no form of the command removes the address information from the local address configuration.

Parameters:  
control ip-address — Specifies the local IP address to which ad servers send Society of Cable Telecommunications Engineers 30 (SCTE 30) ad control streams. This address should be in the same subnet as the ip address assigned to the video interface.

The values of control ip-address and the data ip-address specify the local IP address to which ad servers send SCTE 30 ad data streams, must be set together in the same SNMP request PDU or else the set request will fail with an inconsistent value error.

data ip-address — Specifies the local IP address to which ad servers send Society of Cable Telecommunications Engineers 30 (SCTE 30) ad data streams. This address should be in the same subnet as the ip address assigned to the video interface.

The values of the control ip-address and the data ip-address specify the local IP address to which ad servers send SCTE 30 ad control streams, must be set together in the same SNMP request PDU or else the set request will fail with an inconsistent value error.

multicast-service

Syntax:  
multicast-service service-id
no multicast-service

Context:  
config>service>ies>video-interface
config>service>vpls>video-interface
config>service>vprn>video-interface

Description:  
This command adds a multicast service association to the video interface. This parameter is not required on the video interface when the service carries both unicast and multicast traffic.

When multicast and unicast are carried in separate service instances, the operator can set this parameter on the unicast video interface to form an association with the multicast service when replies need to be sent in the multicast service instance.

When multicast and unicast are carried in separate services when a downstream device (such as a DSLAM) can perform a service cross connect between the services and performs multicast replication.

The no form of the command removes the multicast service association.

Default:  
none
Parameters

- **service-id** — The service ID of the associated multicast service.

Values

- **service-id**: 1 — 2147483647
- **svc-name**: 64 characters maximum

---

**rt-client-src-address**

**Syntax**

```
rt-client-src-address ip-address
no rt-client-src-address
```

**Context**

- `config>service>ies>video-interface`
- `config>service>vpls>video-interface`
- `config>service>vprn>video-interface`

**Description**

This command assigns the IP address for the retransmission client on the video interface within the service. The RET client IP address is the originating address used for communication with upstream RET servers. If no RET client address is assigned, the RT client is operationally down as the RET client configuration is incomplete.

For a VPLS service, the RET client address cannot be the same as an existing address for the video interface, but it must be an address within a video interface subnet.

For IES and VPRN, the RET client address can be the same as an existing address for the video interface or an address within a video interface subnet.

The `no` form of the command deletes the RT client address from the video interface.

**Default**

none

**Parameters**

- **ip-address** — Specifies the IP address for the retransmission client on the video interface within the service.

---

**video-sap**

**Syntax**

```
video-sap video-group-id
no video-sap
```

**Context**

- `config>service>ies>video-interface`
- `config>service>vpls>video-interface`
- `config>service>vprn>video-interface`

**Description**

This command configures a service video interface association with a video group.

The `no` form of the command removes the video group association.

**Parameters**

none

**Parameters**

- **video-group-id** — Specifies the video group ID number.

  **Values**

  - 1 — 4
egress

Syntax egress

Context config>service>ies>video-interface>video-sap
       config>service>vpls>video-interface>video-sap
       config>service>vprn>video-interface>video-sap

Description This command enables the context to configure egress parameters for the service’s video SAP.

ingress

Syntax ingress

Context config>service>ies>video-interface>video-sap
       config>service>vpls>video-interface>video-sap
       config>service>vprn>video-interface>video-sap

Description This command enables the context to configure ingress parameters for the service’s video SAP.

qos

Syntax qos policy-id
       no qos

Context config>service>ies>video-interface>video-sap>egress
       config>service>vpls>video-interface>video-sap>egress
       config>service>vprn>video-interface>video-sap>egress
       config>service>ies>video-interface>video-sap>ingress
       config>service>vpls>video-interface>video-sap>ingress
       config>service>vprn>video-interface>video-sap>ingress

Description This command associates an existing egress or ingress QoS policy to a video interface. If the policy-id does not exist, an error will be returned. Attempts to associate a QoS policy of the wrong type returns an error.

Only one QoS policy can be associated with a video interface at one time in the ingress and egress contexts. Attempts to associate a second QoS policy of a given type will return an error.

The no form of the command removes the QoS policy association from the video interface, and the QoS policy reverts to the default.

Default default QoS policy

Parameters policy-id — The sap-egress or sap-ingress policy ID to associate with the video interface on ingress/egress. The policy ID must already exist.

Values 1 — 65535
filter

Syntax  
filter ip ip-filter-id
no filter

Context  
config>service>ies>video-interface>video-sap>egress
config>service>vpls>video-interface>video-sap>egress
config>service>vprn>video-interface>video-sap>egress
config>service>ies>video-interface>video-sap>ingress
config>service>vprn>video-interface>video-sap>ingress

Description  
This command associates an existing IP filter policy with an ingress or egress video SAP. Filter policies control the forwarding and dropping of packets based on the matching criteria. 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.

Parameters  
ip ip-filter-id — Specifies the ID for the IP filter policy.
Values  
1 — 65535

gateway-ip

Syntax  
[n] gateway-ip ip-address

Context  
config>service>vpls>video-interface

Description  
This command assigns a gateway IP address for the video interface within the VPLS service. Because VPLS is a Layer 2 service and the video interface is modeled like a host within the service, the video interface needs a gateway IP to send requests to devices outside of the VPLS subnet.

Default  
none

Parameters  
ip-address — Specifies the gateway IP address of the VPLS video interface.
Show Commands

video-group

Syntax  
video-group [video-group-id]

Context  
show>isa

Description  
This command displays ISA IPSec group information

Parameters  
ipsec-aa-group-id — Specifies the ISA video group ID.

Sample Output

A:SR-7/Dut-C# show isa video-group
===============================================================================
ISA Video Group
===============================================================================

Video Group Id         : 1              Admin State            :  Up
Oper State             : Up             RT Server State        :  Enabled
FCC Server State       : Disabled       ADI State              :  Disabled
RT Resv Bandwidth(Mbps): 0              ADI State              :  Disabled
MDA                    : 2/1            Channels               :  2
Admin State            : Up             Oper State             :  Up
Used Cache (bytes)     : 586622         Available Cache (bytes): 186918616
Mem alloc failures     : 0              Droped pkts (dentrying) : 0
Failed Chnl Allocs : 0              Egress Bandwidth excee*:  0
Bandwidth in use(kbps) : 0              Peak Bandwidth(kbps) : 200
Egress stream resets : 0              Ingress stream resets : 53
Ad stream resets      : 0              Ad stream aborts : 0
SSRC collisions       : 0              Received data packets : 4521
Received data octets  : 6284714        Rx data packet errors : 0
Transmitted data packets: 1183         Transmitted data octets: 1646212
Tx data packet errors : 0              Tx lost data packets : 47
Active RTCP sessions : 1              Requested RTP Packets : 968
RTCP Parse Errors     : 0              RTCP Config Errors : 0
RTCP IPC Errors       : 0              RTCP SG Errors : 0
RTCP Subscriber Errors : 0              RTCP Interface Errors : 0
Total RET BW (Kbps)   : 0              Max. RET BW (Kbps) : 100
Total FCC BW (Kbps)   : 0              Drop Count for FCC : 0
Mcast RET Req for RTCP: 0              Mcast RET Req for RUDP : 0
Mcast RET Created     : 0              Mcast RET Req Quenched : 0
HighPkt pool limit hit : 0
Pkts Lost (2-10)      : 24             Pkts Lost (11-20) : 48
Pkts Lost (21-30)     : 0              Pkts Lost (31-40) : 0
Pkts Lost ( >40)      : 0

Video-groups : 1

* indicates that the corresponding row element may have been truncated.
A:SR-7/Dut-C#
Show Commands

adi

Syntax

adi [service service-id] [interface ip-int-name] [address mcast-address] [source ip-address] [detail]

Context

show>video

Description
This command displays ad insertion channel information.

Parameters

service service-id — Displays information pertaining to the specified service ID.

Values

1 — 2147483648

svc-name — a string up to 64 characters in length.

interface ip-int-name — Displays information pertaining to the specified interface.

address mcast-address — Displays information pertaining to the specified multicast channel address.

source ip-address — Displays information pertaining to the source IP address.

detail — The output displays detailed information.

channel

Syntax

channel [service service-id] [interface ip-int-name] [address mcast-address] [source ip-address] [summary|detail] [pid|config] [analyzer[interval time-interval]]

Context

show>video

show>video>adi

Description
This command displays video channel information.

Parameters

service service-id — Displays video channel information pertaining to the specified service ID.

Values

service-id: 1 — 2147483648

svc-name: A string up to 64 characters in length.

Default

Base

router-name: Base, management, vpls-management

interface ip-int-name — Displays video channel information pertaining to the specified interface.

address mcast-address — Displays video channel information pertaining to the specified multicast channel address.

source ip-address — Displays video channel information pertaining to the source IP address.

summary — The output displays summarized video channel information.

detail — The output displays detailed video channel information.

Sample Output

*A:SR-7/Dut-C# show video channel analyzer

===============================================================================
Video channel analyzer summary
### Channel number : 1

**Service Id** : 300  
**Interface Name** : video-300  
**Group Address** : 235.5.5.6  
**Source Address** : 20.20.13.2  
**MDI Delay Factor** : N/A  
**MDI Loss Rate** : N/A  
**Good Secs** : 1

### Channel number : 2

**Service Id** : 300  
**Interface Name** : video-300  
**Group Address** : 235.5.5.6  
**Source Address** : 192.168.2.1  
**MDI Delay Factor** : N/A  
**MDI Loss Rate** : N/A  
**Good Secs** : 2

Number of channels : 2

*A:*SR-7/Dut-C#  
*A:*SR-7/Dut-C# show video channel analyzer detail

---

### GOP Stats

<table>
<thead>
<tr>
<th>Min</th>
<th>Max</th>
<th>Avg</th>
</tr>
</thead>
<tbody>
<tr>
<td>GOP Length</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Frames/Sec</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

### Frame Stats

<table>
<thead>
<tr>
<th>I-Frame</th>
<th>P-Frame</th>
<th>B-Frame</th>
</tr>
</thead>
<tbody>
<tr>
<td>Good</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>Bad</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

### Error Stats

<table>
<thead>
<tr>
<th>Err Secs</th>
<th>Deg Secs</th>
<th>Imp Secs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overall</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>PAT Rep</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>PMT Rep</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>PCR Rep</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>PAT Syntax</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>PMT Syntax</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Sync Secs</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Sync Loss</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Unref PID</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Traffic Loss</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
### Channel number : 2

<table>
<thead>
<tr>
<th>Service Id</th>
<th>Interface Name</th>
<th>Group Address</th>
<th>Source Address</th>
<th>MDI Delay Factor</th>
<th>MDI Loss Rate</th>
<th>Good Secs</th>
</tr>
</thead>
<tbody>
<tr>
<td>300</td>
<td>video-300</td>
<td>235.5.5.6</td>
<td>192.168.2.1</td>
<td>3</td>
<td>0</td>
<td>17</td>
</tr>
</tbody>
</table>

**GOP Stats**

<table>
<thead>
<tr>
<th>Min</th>
<th>Max</th>
<th>Avg</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

**Frame Stats**

<table>
<thead>
<tr>
<th>I-Frame</th>
<th>P-Frame</th>
<th>B-Frame</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>3</td>
<td>439</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

**Error Stats**

<table>
<thead>
<tr>
<th>Err Secs</th>
<th>Deg Secs</th>
<th>Imp Secs</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Number of channels : 2

*A:* SR-7/Dut-C#

*A:* SR-7/Dut-C# show video channel analyzer address 235.5.5.6 source 20.20.13.2 interface video-300 detail

Video channel analyzer detail

<table>
<thead>
<tr>
<th>Channel number : 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Id</td>
</tr>
<tr>
<td>300</td>
</tr>
</tbody>
</table>

**GOP Stats**

<table>
<thead>
<tr>
<th>Min</th>
<th>Max</th>
<th>Avg</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
GOP Length          1                   1                   1
Frames/Sec          0                   0                   0
===============================================================================
Frame Stats
===============================================================================
<table>
<thead>
<tr>
<th></th>
<th>I-Frame</th>
<th>P-Frame</th>
<th>B-Frame</th>
</tr>
</thead>
<tbody>
<tr>
<td>Good</td>
<td>1</td>
<td>8</td>
<td>1155</td>
</tr>
<tr>
<td>Bad</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
===============================================================================
Error Stats
===============================================================================
<table>
<thead>
<tr>
<th></th>
<th>Err Secs</th>
<th>Deg Secs</th>
<th>Imp Secs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overall</td>
<td>0</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>PAT Rep</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>PMT Rep</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>PCR Rep</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>PAT Syntax</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PMT Syntax</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sync Secs</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sync Loss</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unref PID</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Traffic Loss</td>
<td>0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Number of channels : 1
*A:SR-7/Dut-C#
*A:SR-7/Dut-C# show video channel pid
Video Channel PID
===============================================================================
<table>
<thead>
<tr>
<th></th>
<th>Service Id</th>
<th>Interface Name</th>
<th>Group Address</th>
<th>Source Address</th>
<th>PID</th>
<th>PID Type</th>
<th>MPEG Stream Type</th>
<th>Is PCR PID</th>
<th>Cc Err Secs</th>
<th>TEI Err Secs</th>
<th>Absent Err Secs</th>
<th>PID Bitrate</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>300</td>
<td>video-300</td>
<td>235.5.5.6</td>
<td>20.20.13.2</td>
<td>0</td>
<td>pat</td>
<td>0</td>
<td>No</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td></td>
<td>300</td>
<td>video-300</td>
<td>235.5.5.6</td>
<td>20.20.13.2</td>
<td>110</td>
<td>pmt</td>
<td>0</td>
<td>No</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td></td>
<td>300</td>
<td>video-300</td>
<td>235.5.5.6</td>
<td>20.20.13.2</td>
<td>4096</td>
<td>video</td>
<td>2</td>
<td>Yes</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>18530784</td>
</tr>
</tbody>
</table>
Show Commands

---

**Group Address**: 235.5.5.6  **Source Address**: 20.20.13.2

**PID**: 4097  **PID Type**: audio

**MPEG Stream Type**: 129  **Is PCR PID**: No

**Cc Err Secs**: 0  **TEI Err Secs**: 0

**Absent Err Secs**: 0  **PID Bitrate**: 231616

---

**Service Id**: 300  **Interface Name**: video-300

**Group Address**: 235.5.5.6  **Source Address**: 192.168.2.1

**PID**: 0  **PID Type**: pat

**MPEG Stream Type**: 0  **Is PCR PID**: No

**Cc Err Secs**: 0  **TEI Err Secs**: 0

**Absent Err Secs**: 0  **PID Bitrate**: 0

---

**Service Id**: 300  **Interface Name**: video-300

**Group Address**: 235.5.5.6  **Source Address**: 192.168.2.1

**PID**: 110  **PID Type**: pmt

**MPEG Stream Type**: 0  **Is PCR PID**: No

**Cc Err Secs**: 0  **TEI Err Secs**: 0

**Absent Err Secs**: 0  **PID Bitrate**: 0

---

**Service Id**: 300  **Interface Name**: video-300

**Group Address**: 235.5.5.6  **Source Address**: 192.168.2.1

**PID**: 4096  **PID Type**: video

**MPEG Stream Type**: 2  **Is PCR PID**: Yes

**Cc Err Secs**: 2  **TEI Err Secs**: 0

**Absent Err Secs**: 0  **PID Bitrate**: 1853296

---

**Service Id**: 300  **Interface Name**: video-300

**Group Address**: 235.5.5.6  **Source Address**: 192.168.2.1

**PID**: 4097  **PID Type**: audio

**MPEG Stream Type**: 129  **Is PCR PID**: No

**Cc Err Secs**: 0  **TEI Err Secs**: 0

**Absent Err Secs**: 0  **PID Bitrate**: 231616

---

*A:SR-7/Dut-C#* show video channel config

---

**Service Id**: 300  **Interface Name**: video-300

**Group Address**: 235.5.5.6  **Source Address**: 20.20.13.2

**Analyzer State**: Enabled  **Cc Error**: Enabled

**PAT Rep Err**: Enabled  **TNC PAT Rep**: 200

**QOS PAT Rep**: 400  **POA PAT Rep**: 600

**PAT Syntax**: Enabled  **PCR Rep Err**: Enabled

**TNC PCR Rep**: 200  **QOS PCR Rep**: 400

**POA PCR Rep**: 600  **Vid PID Absent**: 1000

**PID PMT Unref**: Enabled  **PMT Rep Err Secs**: Enabled

**TNC PMT Rep**: 400  **QOS PMT Rep**: 800

**POA PMT Rep**: 2000  **PMT Syntax**: Enabled

**SCTE35 Err Secs**: Enabled  **TEI Err Secs**: Enabled

**TS Sync Loss**: Enabled  **Non-Vld Pid Abs**: 1000

---
Service Id : 300 Interface Name : video-300
Group Address : 235.5.5.6 Source Address : 20.20.0.1
Analyzer State : Enabled Cc Error : Enabled
PAT Rep Err : Enabled TNC PAT Rep : 200
QOS PAT Rep : 400 POA PAT Rep : 600
PAT Syntax : Enabled PCR Rep Err : Enabled
TNC PCR Rep : 200 QOS PCR Rep : 400
POA PCR Rep : 600 Vid PID Absent : 1000
PID PMT Unref : Enabled PMT Rep Err Secs : Enabled
TNC PMT Rep : 400 QOS PMT Rep : 800
POA PMT Rep : 2000 PMT Syntax : Enabled
SCTE35 Err Secs : Enabled TEI Err Secs : Enabled
TS Sync Loss : Enabled Non-Vid Pid Abse* : 1000

Number of channels : 3

* indicates that the corresponding row element may have been truncated.
*A:SR-7/Dut-C#

*A:SR-7/Dut-C# show video channel analyzer

Video channel analyzer summary

Channel number : 1

Service Id : 300 Interface Name : video-300
Group Address : 235.5.5.6 Source Address : 20.20.0.1
MDI Delay Factor : 1 MDI Loss Rate : 0
Good Secs : 68

Channel number : 2

Service Id : 300 Interface Name : video-300
Group Address : 235.5.5.6 Source Address : 192.168.2.1
MDI Delay Factor : 2 MDI Loss Rate : 0
Good Secs : 68

Channel number : 3

Service Id : 300 Interface Name : video-300-S
Group Address : 235.5.5.6 Source Address : 192.168.2.1
MDI Delay Factor : 3 MDI Loss Rate : 0
Good Secs : 69

Number of channels : 3

A:SR-7/Dut-C#

*A:SR-7/Dut-C# show video channel pid

Video Channel PID

Service Id : 300 Interface Name : video-300
Group Address : 235.5.5.6 Source Address : 20.20.0.1
PID : 0 PID Type : pat
MPEG Stream Type : 0                    Is PCR PID : No
Cc Err Secs : 8                    TEI Err Secs : 0
Absent Err Secs : 0                    PID Bitrate : 0

-------------------------------------------------------------------------------
Service Id : 300                  Interface Name : video-300
Group Address : 235.5.5.6            Source Address : 20.20.0.1
PID : 110                  PID Type : pmpt
MPEG Stream Type : 0                    Is PCR PID : No
Cc Err Secs : 0                    TEI Err Secs : 0
Absent Err Secs : 0                    PID Bitrate : 0

-------------------------------------------------------------------------------
Service Id : 300                  Interface Name : video-300
Group Address : 235.5.5.6            Source Address : 20.20.0.1
PID : 4096                 PID Type : video
MPEG Stream Type : 2                    Is PCR PID : Yes
Cc Err Secs : 0                    TEI Err Secs : 0
Absent Err Secs : 0                    PID Bitrate : 18538304

-------------------------------------------------------------------------------
Service Id : 300                  Interface Name : video-300
Group Address : 235.5.5.6            Source Address : 20.20.0.1
PID : 4097                 PID Type : video
MPEG Stream Type : 129                  Is PCR PID : No
Cc Err Secs : 0                    TEI Err Secs : 0
Absent Err Secs : 0                    PID Bitrate : 231616

-------------------------------------------------------------------------------
Service Id : 300                  Interface Name : video-300
Group Address : 235.5.5.6            Source Address : 20.20.0.1
PID : 4096                 PID Type : video
MPEG Stream Type : 2                    Is PCR PID : Yes
Cc Err Secs : 0                    TEI Err Secs : 0
Absent Err Secs : 0                    PID Bitrate : 18539808

-------------------------------------------------------------------------------
Service Id : 300                  Interface Name : video-300
Group Address : 235.5.5.6            Source Address : 20.20.0.1
PID : 4097                 PID Type : video
MPEG Stream Type : 129                  Is PCR PID : No
Cc Err Secs : 0                    TEI Err Secs : 0
Absent Err Secs : 0                    PID Bitrate : 231616
Show Commands

Service Id       : 300                  Interface Name   : video-300-S
Group Address    : 235.5.5.6            Source Address   : 192.168.2.1
PID              : 110                  PID Type         : pmt
MPEG Stream Type : 0                    Is PCR PID       : No
Cc Err Secs      : 0                    TEI Err Secs     : 0
Absent Err Secs  : 0                    PID Bitrate      : 0

Service Id       : 300                  Interface Name   : video-300-S
Group Address    : 235.5.5.6            Source Address   : 192.168.2.1
PID              : 4096                 PID Type         : video
MPEG Stream Type : 2                    Is PCR PID       : Yes
Cc Err Secs      : 0                    TEI Err Secs     : 0
Absent Err Secs  : 0                    PID Bitrate      : 18529280

Service Id       : 300                  Interface Name   : video-300-S
Group Address    : 235.5.5.6            Source Address   : 192.168.2.1
PID              : 4097                 PID Type         : audio
MPEG Stream Type : 129                  Is PCR PID       : No
Cc Err Secs      : 0                    TEI Err Secs     : 0
Absent Err Secs  : 0                    PID Bitrate      : 231616

A:SR-7/Dut-C# show video channel config interface "video-300-S"

Video channel config

Service Id       : 300                  Interface Name   : video-300-S
Group Address    : 235.5.5.6            Source Address   : 192.168.2.1
Analyzer State   : Enabled              Cc Error         : Enabled
PAT Rep Err      : Enabled              TNC PAT Rep      : 400
QOS PAT Rep      : 600                  POA PAT Rep      : 700
PAT Syntax       : Enabled              PCR Rep Err      : Enabled
TNC PCR Rep      : 400                  QOS PCR Rep      : 600
POA PCR Rep      : 700                  Vid PID Absent  : 5000
PID PMT Unref    : Enabled              PMT Rep Err Secs : Enabled
TNC PMT Rep      : 2300                 QOS PMT Rep      : 2500
POA PMT Rep      : 2700                 PMT Syntax       : Enabled
SCTE35 Err Secs  : Enabled              TEI Err Secs     : Enabled
TS Sync Loss     : Enabled              Non-Vid Pid Abse*: 5000

Number of channels : 1

* indicates that the corresponding row element may have been truncated.

A:SR-7/Dut-C# show video channel pid interface video-300-S address 235.5.5.6 source 192.168.2.1

Video Channel PID

Service Id       : 300                  Interface Name   : video-300-S
Group Address    : 235.5.5.6            Source Address   : 192.168.2.1
PID              : 0                    PID Type         : pat
### Show Commands

MPEG Stream Type : 0  Is PCR PID : No  
Cc Err Secs : 0  TEI Err Secs : 0  
Absent Err Secs : 0  PID Bitrate : 0

---

Service Id : 300  Interface Name : video-300-S  
Group Address : 235.5.5.6  Source Address : 192.168.2.1  
PID : 110  PID Type : pm  
MPEG Stream Type : 0  Is PCR PID : No  
Cc Err Secs : 0  TEI Err Secs : 0  
Absent Err Secs : 0  PID Bitrate : 0

---

Service Id : 300  Interface Name : video-300-S  
Group Address : 235.5.5.6  Source Address : 192.168.2.1  
PID : 4096  PID Type : video  
MPEG Stream Type : 2  Is PCR PID : Yes  
Cc Err Secs : 0  TEI Err Secs : 0  
Absent Err Secs : 84  PID Bitrate : 0

---

Service Id : 300  Interface Name : video-300-S  
Group Address : 235.5.5.6  Source Address : 192.168.2.1  
PID : 4097  PID Type : audio  
MPEG Stream Type : 129  Is PCR PID : No  
Cc Err Secs : 0  TEI Err Secs : 0  
Absent Err Secs : 84  PID Bitrate : 0

---

*A:* SR-7/Dut-C#

*B:* IPTV-SR7# show video adi channel

---

**Adi Channel Info**

---

SvcId  Interface Name  Group Address  Source Address  Channel Name

---

100  video-100  234.4.5.228  195.168.9.10  228
100  video-100  234.4.5.240  195.168.9.10  240
100  video-100  234.4.5.241  195.168.9.10  241
...

---

*B:* IPTV-SR7#

*A:* Dut-C# show video channel

---

**Video channel**

---

Service Id  Group Address  Stream  SSRCId  RxPackets  TxPackets  Interface  Source Address  GrId  Src/DstPr  RxBytes  TxBytes

---

1  234.0.0.1  Network  0  0  0  
vi  1.0.102.102  1  33333/40005  0  0
1  234.0.0.2  Network  0  0  0
vi  1.0.102.102  1  33333/40005  0  0
1  234.0.0.3  Network  0  0  0
vi  1.0.102.102  1  33333/40005  0  0
1  234.0.0.4  Network  0  0  0
vi  1.0.102.102  1  33333/40005  0  0
1  234.0.0.5  Network  0  0  0
vi  1.0.102.102  1  33333/40005  0  0
1  234.0.0.6  Network  0  0  0
vi  1.0.102.102  1  33333/40005  0  0
## Show Commands

<table>
<thead>
<tr>
<th></th>
<th>234.0.0.7</th>
<th>Network 0</th>
<th>0</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>vi</td>
<td>1.0.102.102</td>
<td>1</td>
<td>33333/40005</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>234.0.0.8</td>
<td>Network 0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>vi</td>
<td>1.0.102.102</td>
<td>1</td>
<td>33333/40005</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>234.0.0.249</td>
<td>Network 0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>vi</td>
<td>1.0.102.102</td>
<td>1</td>
<td>33333/40005</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>234.0.0.250</td>
<td>Network 0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>vi</td>
<td>1.0.102.102</td>
<td>1</td>
<td>33333/40005</td>
<td>0</td>
</tr>
</tbody>
</table>

Number of channels : 250

*A:Dut-C#*

*A:Dut-C# show video channel detail*

### Video channel detail

| Service Id | Interface Name | Group Address | Source Address | SSRC Id (hex) | Group Id | UDP Source Port | UDP Dest Port | Stream Type | Up Time | Admin Buffer | Oper Buffer | Received Bytes | Rx Invalid Pkts | Tx Bytes | Tx Packets | Tx Failed Pkts | RTClnt AdmState | RT Server Port | RT Server Address | Received Bytes | Received Pkts | Tx RT Req | Tx Repeat RTReq | Gaps detected | Failed RT Req | Local RT Server Admin State | RTP Pkts Req | Failed RT Req | Trans RT Replies | Transmittd Bytes | FCC Svr AdmState | FCC Svr Chl Type | Rx FCC Requests | Tx FCC Replies | Tx FCC Replies | Tx Packets |
|------------|----------------|---------------|---------------|---------------|-----------|----------------|--------------|-------------|---------|--------------|------------|----------------|---------------|------------|------------|--------------|----------------|---------------|------------------|----------------|-------------|-----------|--------------|-------------|-------------|----------------|-------------|--------------|--------------|--------------|-------------|-----------|
| 1          | vi             | 234.0.0.1     | 1.0.102.102   | ea000001      | 1         | 33333         | 40005        | Network    | 0d 00:01:54 | 1000         | 0             | 44107480      | 31732        | 0           | 0           | 0             | Up             | 4098           | 4.4.4.4        | 0            | 0          | 0         | 0            | 0            | 0            | Up             | 0             | 0           | 0         | 0          |

*A:Dut-C#*

### interface

**Syntax**

```
interface [service service-id] [interface ip-int-name] [stats {rt-server | fcc-server}]
```

**Context**

`show>video`

**Description**

This command displays video interface information.

**Parameters**

`service service-id` — Displays video interface information pertaining to the specified service ID.
Values  1 — 2147483648  
svc-name — a string up to 64 characters in length.

interface ip-int-name — Displays video interface information pertaining to the specified interface.
stats — Displays video interface statistics.

Values  rt-server — Displays video interface statistics for the RET server.
       fcc-server — Displays video interface statistics for the FCC server.

Sample Output

*A:Dut-C# show video interface
===============================================================================
| Video interface |
|-----------------|---------------------------------|
| Service Id      : 1                |
| Name            : vi               |
| Admin/Oper State: Up/Up            |
| Video Group Id  : 1                |
| Sessions        : 2000             |
| Address         : 3.3.3.3/32       |
| Tx Failed Pkts  : 0                |
| SCTE30 TCP sess : 0                |
| SD RT Srvr State: Enabled          |
| SD RT Requests  : 0                |
| SD RTP Pkts Req : 0                |
| Tx SD Bytes     : 0                |
| HD RT Srvr State: Enabled          |
| HD RT Requests  : 0                |
| HD RTP Pkts Req : 0                |
| Tx HD Bytes     : 0                |
| PIP RT Srvr State: Enabled         |
| PIP RT Requests : 0                |
| PIP RTP Pkts Req: 0                |
| Tx PIP Bytes    : 0                |
| SD FCC Srvr State: Enabled         |
| SD FCC Requests : 0                |
| Tx SD Bytes     : 0                |
| SD FCC Replies  : 0                |
| HD FCC Srvr State: Enabled         |
| HD FCC Requests : 448820            |
| TX HD Bytes     : 17150845788       |
| HD FCC Replies  : 448820            |
| PIP FCC Svr State: Enabled         |
| PIP FCC Requests: 0                |
| Tx PIP Bytes    : 0                |
| PIP FCC Replies : 0                |
| Interfaces : 1                      |
===============================================================================
*A:Dut-C#
Show Commands

**session**

**Syntax**

```
session [service service-id] [interface ip-int-name] [address mcast-address] [source ip-address]
```

**Context**

```
show>video>adi
```

**Description**

This command displays ADI video session information.

**Parameters**

- **service service-id** — Displays video session information pertaining to the specified service ID.
  - **Values**
    - 1 — 2147483648
    - svc-name — a string up to 64 characters in length.

- **interface ip-int-name** — Displays session information for the specified interface.

- **address mcast-address** — Displays session information for the specified multicast address.

- **source ip-address** — Displays session information for the specified IP address.

**Sample Output**

```
*B:IPTV-SR7# show video adi session
===============================================================================
Adi Session
===============================================================================
Service Id       : 100                  Interface Name   : video-100
Group Address    : 234.4.5.241          Source Address   : 100.100.100.1
Ad Server Addr   : 10.200.14.2          Up Time          : 0d 13:30:02
Init Requests    : 1                    Succ/Unsucc Resp : 1/0
Alive Requests   : 0                    Succ/Unsucc Resp : 0/0
Cue Requests     : 0                    Succ/Unsucc Resp : 0/0
Abort Requests   : 0                    Succ/Unsucc Resp : 0/0
Splice Requests  : 910                  Succ/Unsucc Resp : 906/4
Successful splice-in complete responses     : 902
Successful splice-out complete responses    : 894
Unsuccessful splice-out complete responses  : 11
Invalid SCTE30 R*: 0
-------------------------------------------------------------------------------
Number of adi sessions : 1
===============================================================================
*B:IPTV-SR7#
```

**splice-status**

**Syntax**

```
splice-status [service service-id] [interface ip-int-name] [address mcast-address] [source ip-address] [start-time start-time] [interval time-interval]
```

**Context**

```
show>video>adi
```

**Description**

This command displays ADI slice information.

- **service service-id** — Displays splice status information pertaining to the specified service ID.
  - **Values**
    - 1 — 2147483648
    - svc-name — a string up to 64 characters in length.
Show Commands

interface ip-int-name — Displays splice status information for the specified interface.

address mcast-address — Displays splice status information for the specified multicast address.

source ip-address — Displays splice status information for the specified IP address.

start-time start-time — Enter the start time.

Values 1 — 4294967295 minutes earlier

interval time-interval — Enter the interval time.

Values 1 — 4294967295 minutes

Sample Output

*B:IPTV-SR7# show video adi splice-status
===============================================================================
Adi Splice Status
===============================================================================
Service Id : 100  Interface Name : video-100
Group Address : 234.4.5.241  Source Address : 100.100.100.1
Status : Complete  Rate : 8936 kbps
Duration Req : 30 sec  Duration Played : 29 sec
Session Id : 1  Prior Session Id : 4294967295
SpliceIn SeqNum : 378  SpliceOut SeqNum : 29727
Abort Reason : None  Black Frames : 0
First black frame PTS : 1530
Max Ad Stream PTS : 0
Min Network Stream PTS : 0
------------------------------------------------------------------------------------------------- 
Service Id : 100  Interface Name : video-100
Group Address : 234.4.5.241  Source Address : 100.100.100.1
Status : Complete  Rate : 0 kbps
Duration Req : 30 sec  Duration Played : 0 sec
Session Id : 2  Prior Session Id : 1
SpliceIn SeqNum : 29727  SpliceOut SeqNum : 0
Abort Reason : Session incomplete  Black Frames : 0
First black frame PTS : 1530
Max Ad Stream PTS : 0
Min Network Stream PTS : 0
-------------------------------------------------------------------------------------------------
*B:IPTV-SR7#

rtp-session

Syntax rtp-session [service service-id] [source ip-address] [detail [stats {rt-server | fcc-server}]]
rtp-session [service service-id] summary

Context show>video

Description This command displays video session information.

Parameters service service-id — Displays video session information pertaining to the specified service ID.
Values

<table>
<thead>
<tr>
<th>Values</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 — 2147483648</td>
<td>Service ID range.</td>
</tr>
<tr>
<td>svc-name — a string up to 64 characters in length.</td>
<td>Session ID.</td>
</tr>
</tbody>
</table>

source ip-address — Displays session information for the specified IP address.

detail — The output displays detailed video session information.

stats — Displays video session statistics.

Values

<table>
<thead>
<tr>
<th>Values</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>rt-server</td>
<td>Displays video session statistics for the RT server.</td>
</tr>
<tr>
<td>fcc-server</td>
<td>Displays video session statistics for the FCC server.</td>
</tr>
</tbody>
</table>

summary — The output displays summarized video session information.

Sample Output

*A:Dut-C# show video rtp-session

```
<table>
<thead>
<tr>
<th>Service Id</th>
<th>Source address</th>
<th>SSRC Id (hex)</th>
<th>RT reqs</th>
<th>FCC reqs</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1.0.103.103</td>
<td>1</td>
<td>0</td>
<td>226</td>
</tr>
<tr>
<td>vi</td>
<td>1000</td>
<td>0d 00:03:24</td>
<td>0</td>
<td>225</td>
</tr>
<tr>
<td>1</td>
<td>1.0.103.103</td>
<td>1</td>
<td>0</td>
<td>226</td>
</tr>
<tr>
<td>vi</td>
<td>1001</td>
<td>0d 00:03:24</td>
<td>0</td>
<td>225</td>
</tr>
<tr>
<td>1</td>
<td>1.0.103.103</td>
<td>1</td>
<td>0</td>
<td>226</td>
</tr>
<tr>
<td>vi</td>
<td>1002</td>
<td>0d 00:03:24</td>
<td>0</td>
<td>225</td>
</tr>
<tr>
<td>1</td>
<td>1.0.103.103</td>
<td>1</td>
<td>0</td>
<td>226</td>
</tr>
<tr>
<td>vi</td>
<td>1003</td>
<td>0d 00:03:24</td>
<td>0</td>
<td>225</td>
</tr>
<tr>
<td>1</td>
<td>1.0.103.103</td>
<td>1</td>
<td>0</td>
<td>226</td>
</tr>
<tr>
<td>vi</td>
<td>1004</td>
<td>0d 00:03:24</td>
<td>0</td>
<td>225</td>
</tr>
<tr>
<td>1</td>
<td>1.0.103.103</td>
<td>1</td>
<td>0</td>
<td>226</td>
</tr>
<tr>
<td>vi</td>
<td>1005</td>
<td>0d 00:03:24</td>
<td>0</td>
<td>225</td>
</tr>
<tr>
<td>1</td>
<td>1.0.103.103</td>
<td>1</td>
<td>0</td>
<td>226</td>
</tr>
<tr>
<td>vi</td>
<td>1006</td>
<td>0d 00:03:24</td>
<td>0</td>
<td>225</td>
</tr>
<tr>
<td>1</td>
<td>1.0.103.103</td>
<td>1</td>
<td>0</td>
<td>226</td>
</tr>
<tr>
<td>vi</td>
<td>1007</td>
<td>0d 00:03:24</td>
<td>0</td>
<td>225</td>
</tr>
<tr>
<td>1</td>
<td>1.0.103.103</td>
<td>1</td>
<td>0</td>
<td>226</td>
</tr>
<tr>
<td>vi</td>
<td>1008</td>
<td>0d 00:03:24</td>
<td>0</td>
<td>225</td>
</tr>
<tr>
<td>1</td>
<td>1.0.103.103</td>
<td>1</td>
<td>0</td>
<td>226</td>
</tr>
<tr>
<td>vi</td>
<td>1009</td>
<td>0d 00:03:24</td>
<td>0</td>
<td>225</td>
</tr>
</tbody>
</table>
```

Number of RTP sessions : 10

*A:Dut-C# show video rtp-session summary

```
<table>
<thead>
<tr>
<th>Num Sessions</th>
<th>Rx RT Requests</th>
<th>Tx RT Packets</th>
<th>Rx RT Replies</th>
<th>Tx RT Octets</th>
</tr>
</thead>
<tbody>
<tr>
<td>2000</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Rx FCC Requests</td>
<td>371068</td>
<td>Tx FCC Packets</td>
<td>243011904</td>
<td></td>
</tr>
<tr>
<td>Tx FCC Replies</td>
<td>368259</td>
<td>Tx FCC Octets</td>
<td>14152149376</td>
<td></td>
</tr>
</tbody>
</table>
```

Interfaces : 1
### Video RTP session detail

<table>
<thead>
<tr>
<th>Service Id</th>
<th>: 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>vi</td>
</tr>
<tr>
<td>Source Address</td>
<td>1.0.103.103</td>
</tr>
<tr>
<td>Destination Addr</td>
<td>3.3.3.3</td>
</tr>
<tr>
<td>CName</td>
<td>ixiaPort</td>
</tr>
<tr>
<td>Up Time</td>
<td>0d 00:07:08</td>
</tr>
<tr>
<td>Num RT Requests</td>
<td>0</td>
</tr>
<tr>
<td>RT Packets Sent</td>
<td>0</td>
</tr>
<tr>
<td>RT Failed Pkts</td>
<td>0</td>
</tr>
<tr>
<td>Num FCC Requests</td>
<td>212</td>
</tr>
<tr>
<td>FCC Packets Sent</td>
<td>138582</td>
</tr>
<tr>
<td>FCC Failed Pkts</td>
<td>1</td>
</tr>
</tbody>
</table>

---

*A:Dut-C#*
Clear Commands

id

Syntax: id service-id

Context: clear>video

Description: This command clears video information pertaining to the specified service ID.

Parameters:

- service service-id — Specifies the service ID to clear.
  
  Values: 1 — 2147483648
  
  svc-name — a string up to 64 characters in length.

session

Syntax: session all

session client srcAddr

Context: clear>videoid

Description: This command clears session information.

Parameters:

- all — Clears all sessions.
  
- client srcAddr — Clears information for the client source address.

statistics

Syntax: statistics

Context: clear>video

Description: This command clears video related statistics.

id

Syntax: id service-id

Context: clear>video>statistics

Description: This command clears video statistics for a particular service.

Parameters:

- service service-id — Specifies the service ID to clear statistics.
  
  Values: 1 — 2147483648
  
  svc-name — a string up to 64 characters in length.
Clear Commands

adi-session

Syntax  
adi-session

Context  
clear>video>statistics>id

Description  
This command clears video statistics for an ADI session.

channel

Syntax  
channel all [rt-client] [rt-server] [fcc-server] [ad-insert]

channel grp-address [source srcAddr] [rt-client] [rt-server] [fcc-server] [ad-insert]

Context  
clear>video>statistics>id

Description  
This command clears video statistics for a particular channel.

Parameters  

- all — Clears statistics for all channels.
- rt-client — Clears all RET client related statistics.
- rt-server — Clears all RET server related statistics.
- fcc-server — Clears all FCC server related statistics.
- ad-insert — Clears all ad insert related statistics.

grp-address — Clears statistics for the specified channel group address.

source srcAddr — Clears statistics for the specified source address.

interface

Syntax  
interface ip-int-name [address ip-address] rt-client] [rt-server] [fcc-server] [ad-insert]

Context  
clear>video>statistics>id

Description  
This command clears video statistics for a particular channel.

Parameters  

- ip-int-name — Clears statistics for the specified interface.
- address ip-address — Clears statistics for the specified IP address.
- rt-client — Clears all RET client related statistics.
- rt-server — Clears all RET server related statistics.
- fcc-server — Clears all FCC server related statistics.
- ad-insert — Clears all ad insert related statistics.

grp-address — Clears statistics for the specified channel group address.

source srcAddr — Clears statistics for the specified source address.
Clear Commands

**session**

**Syntax**
```
session all [rt-server] [fcc-server]
session client srcAddr [rt-server] [fcc-server]
```

**Context**
clear>video>statistics>id

**Description**
This command clears video statistics for a particular channel.

**Parameters**
- `all` — Clears statistics for all sessions.
- `rt-server` — Clears all RET server related statistics.
- `fcc-server` — Clears all FCC server related statistics.
- `client srcAddr` — Clears statistics for the specified source address.

**isa**

**Syntax**
```
isa video-group-id [mda-id]
```

**Context**
clear>video>statistics

**Description**
This command clears statistics for a particular ISA video group.

**Parameters**
- `video-group-id` — statistics for a particular ISA video group a video group ID.
- `mda-id` — Specifies the card/slot identifying a provisioned ISA.

**Values**
- `video-group-id`: 1 — 4
- `mda-id`: slot/mda
  - `slot`: 1 — 10 (depending on the chassis model)
  - `mda`: 1 — 2
Debug Commands

video-interface

Syntax  
[no] video-interface video-ip-int-name

Context  
debug>service>id

Description  
This command enables debugging for video interfaces.
The no form of the command disables the video interface debugging.

Parameters  
video-ip-int-name — Specifies the video interface name.

adi

Syntax  
adi [zone-channel-name]
no adi

Context  
debug>service>id>video-interface

Description  
This command enables debugging for the ad insert server.

Parameters  
zone-channel-name — Specifies the channel name up to 32 characters in length.

adi-packet

Syntax  
adi-packet [zone-channel-name] [type {type-name [type-name]|all}]
no adi-packet

Context  
debug>service>id>video-interface

Description  
This command enables debugging for ADI packets exchanged between the splicer and the ad-server over scte30 session(s)

Parameters  
zone-channel-name — Specifies the channel name up to 32 characters in length.
type type-name — Specifies the ADI packet type.
Values alive, abort, init, splice, cue, all

Sample Output

A:IPTV-SR7# debug service id 100 video-interface video-100 adi-packet 240-1 type init
A:IPTV-SR7# show debug
debug
  service id 100
    video-interface video-100
      adi-packet 240-1 type init
Debug Commands

exit
exit
exit
A:IPTV-SR7# debug service id 100 video-interface video-100 adi-packet 240-1 type alive
A:IPTV-SR7# show debug
debu
service id 100
video-interface video-100
adi-packet 240-1 type alive
exit
exit
exit

fcc-server

Syntax  fcc-server [client client-ip [source-port src-port]]
no fcc-server

Context  debug>service>id>video-interface

Description  This command enables debugging the FCC server.

Parameters  client client-ip — Specifies the client IP address.
source-port src-port — Specifies the source port’s IP address.

packet-rx

Syntax  packet-rx [client client-ip [source-port src-port]] [fcc-join] [fcc-leave] [ret-nack]
no packet-rx

Context  debug>service>id>video-interface

Description  This command enables debugging of received RTCP messages. The options for this command allow
the user to filter only certain types of messages to appear in the debug traces.

Parameters  client client-ip — Specifies the client IP address.
source-port src-port — Specifies the source port’s IP address.
fcc-join — Enables debugging for FCC joins.
fcc-leave — Enables debugging for FCC leaves.
ret-nack — Enables debugging for retransmission nack packets.

packet-tx

Syntax  packet-tx [group grp-addr [source srcAddr]] [ret-nack]
no packet-tx

Context  debug>service>id>video-interface
Debug Commands

**Description**
This command enables debugging transmitted RTCP packets.

**Parameters**
- **client**  
  `client client-ip` — Specifies the client IP address.
- **source**  
  `source src-srcAddr` — Specifies the source port.
  
  **Values**
  1 — 65535

**rt-client**

**Syntax**
```
rt-client [group group-addr]
```
```
o rt-client
```

**Context**
```
debug>service>id>video-interface
```

**Description**
This command enables debugging the RET client.

**Parameters**
- **group**  
  `group group-addr` — Specifies the multicast group address.

**rt-server**

**Syntax**
```
rt-server [client client-ip [source-port src-port]]
```
```
o rt-server
```

**Context**
```
debug>service>id>video-interface
```

**Description**
This command enables debugging for the RET server.

**Parameters**
- **client**  
  `client client-ip` — Specifies the client IP address.
- **source**  
  `source src-srcAddr` — Specifies the source port.
  
  **Values**
  1 — 65535

**sg**

**Syntax**
```
sg [group grp-addr [source src-addr]]
```
```
o sg
```

**Context**
```
debug>service>id>video-interface
```

**Description**
This command enables channel debugging.

**Parameters**
- **group**  
  `group grp-addr` — Specifies the multicast channel address.
- **source**  
  `source src-addr` — Specifies the source address.
Configuring NAT

This section provides information to configure NAT using the command line interface.

Topics in this section include:

- ISA Redundancy on page 485
- NAT Layer 2-Aware Configurations on page 488
- Large Scale NAT Configuration on page 490

ISA Redundancy

The 7750 SR supports ISA redundancy to provide reliable NAT even when an MDA fails. The active-mda-limit allows an operator to specify how many MDAs will be active in a given NAT group. Any number of MDAs configured above the active-mda-limit will be spare MDAs; they take over the NAT function if one of the current active MDAs fail.

A sample configuration is as follows:

```
Configure isa
  nat-group 1 create
  active-mda-limit 1
  mda 1/2
  mda 2/2
  no shutdown
  exit
exit
```

Show commands are available to display the actual state of a nat-group and its corresponding MDAs:

```
show isa nat-group 1
```

<table>
<thead>
<tr>
<th>Group Member</th>
<th>State</th>
<th>Mda</th>
<th>Addresses</th>
<th>Blocks</th>
<th>Se-%</th>
<th>Hi Se-Prio</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>active</td>
<td>1/2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>N</td>
</tr>
</tbody>
</table>

No. of members: 1
A maximum of four nat-groups can be configured. This gives the operator the ability to differentiate between different traffic types. Normal traffic could be routed to nat-group one, where a limited number of MDA without spare MDAs are available, while high priority traffic could make use of nat-group two, where several active MDAs and a spare MDA are configured. A maximum of six MDAs per nat-group can be configured.

A nat-group cannot become active (no shutdown) if the number of configured MDAs is lower that the active-mda-limit.

A given MDA can be configured in several nat-groups but it can only be active in a single nat-group at any moment in time. Spare MDAs can be shared in several nat-groups, but a spare can only become active in one nat-group at a time. Changing the active-mda-limit, adding or removing MDAs can only be done when the nat-group is shutdown.

Nat-groups that share spare MDAs must be configured with the same list of MDAs. It is possible to remove/add spare MDAs to a nat-group while the nat-group is admin enabled.

```plaintext
Configure
  isa
    nat-group 1 create
    active-mda-limit 1
    mda 1/2
    mda 2/2
    mda 3/1
    no shutdown
  exit
  nat-group 2 create
    active-mda-limit 1
    mda 1/2
    mda 2/2
    mda 3/1
    no shutdown
  exit
  exit
exit
```

Through show commands, it is possible to display an overview of all the nat-groups and MDAs.

```plaintext
show isa nat-group
===============================================================================
ISA NAT Group Summary
===============================================================================
Mda Group 1 Group 2
-------------------------------------------------------------------------------
1/1 active busy
2/2 busy active
3/1 standby standby
===============================================================================
```

If an MDA fails, the spare (if available) will take over. All active sessions will be lost, but new incoming sessions will make use of the spare MDA.

In case of an MDA failure in a nat-group without any spare MDA, all traffic towards that MDA will be black-holed.
For L2-aware NAT, the operator has the possibility to clear all the subscribers on the affected MDA (clear nat isa), terminating all the subscriber leases. New incoming subscribers will make use of the MDAs that are still available in the nat-group.
NAT Layer 2-Aware Configurations

The following sections provide NAT Layer 2-Aware configurations.

#--------------------------------------------------
echo "Card Configuration"
#--------------------------------------------------
card 1
   card-type iom3-xp
   mda 1
      mda-type m60-10/100eth-tx
      exit
   mda 2
      mda-type isa-bb
      exit
   exit
card 2
   card-type iom3-xp
   mda 1
      mda-type m60-10/100eth-tx
      exit
   mda 2
      mda-type isa-bb
      exit
   exit

#--------------------------------------------------
echo "ISA Configuration"
#--------------------------------------------------
isa
   nat-group 1 create
dataction "1 active + 1 spare"
   active-mda-limit 1
   mda 1/2
   mda 2/2
   no shutdown
   exit
   exit

#--------------------------------------------------
echo "Router (Network Side) Configuration"
#--------------------------------------------------
router...

#--------------------------------------------------
echo "NAT (Network Side) Configuration"
#--------------------------------------------------
nat
   outside
      pool "pool1" nat-group 1 type l2-aware create
      address-range 81.81.0.0 81.81.0.200 create
      exit
      no shutdown
      exit
   exit
   exit

#--------------------------------------------------
echo "Service Configuration"
#--------------------------------------------------
service
   customer 1 create
description "Default customer"
exit
...
vprn 100 customer 1 create
...
nat
outside
  pool "pool2" nat-group 1 type l2-aware create
  address-range 82.0.0.0 82.0.0.200 create
  exit
  no shutdown
  exit
  exit
  exit
exit

vprn 101 customer 1 create
...
nat
inside
  l2-aware
    # Hosts in this service with IP addresses in these ranges
    # will be subject to l2-aware NAT.
    address 10.0.0.1/29
    address 10.1.0.1/29
    exit
    exit
    exit
exit
exit
...
nat
  nat-policy "l2-aware-nat-policy1" create
  pool "pool1" router Base
  exit
  nat-policy "l2-aware-nat-policy2" create
  pool "pool2" router 100
  exit
  exit
  ...
exit
#--------------------------------------------------
# Subscriber-mgmt Configuration
#--------------------------------------------------
subscriber-mgmt
  # Subscribers using these sub-profiles will be subject to l2-aware NAT.
  # The configured nat-policies will determine which IP pool will be used.
  sub-profile "l2-aware-profile1" create
    nat-policy "l2-aware-nat-policy1"
  exit
  sub-profile "l2-aware-profile2" create
    nat-policy "l2-aware-nat-policy2"
  exit
  ...
exit
Large Scale NAT Configuration

The following sections provide Large Scale NAT configuration examples.

```plaintext
configure
#--------------------------------------------------
echo "Card Configuration"
#--------------------------------------------------
card 3
    card-type iom3-xp
    mda 1
        mda-type isa-bb
    exit
    mda 2
        mda-type isa-bb
    exit
exit
#--------------------------------------------------
echo "ISA Configuration"
#--------------------------------------------------
isa
    nat-group 1 create
    active-mda-limit 2
    mda 3/1
    mda 3/2
    no shutdown
    exit
exit
#--------------------------------------------------
echo "Filter Configuration"
#--------------------------------------------------
filter
    ip-filter 123 create
    entry 10 create
        match
            src-ip 13.0.0.1/8
        exit
    action nat
    exit
exit
#--------------------------------------------------
echo "NAT (Declarations) Configuration"
#--------------------------------------------------
service
    nat
        nat-policy "ls-outPolicy" create
    exit
exit
#--------------------------------------------------
echo "Service Configuration"
#--------------------------------------------------
service
    customer 1 create
        description "Default customer"
    exit
    vprn 500 customer 1 create
        interface "ip-113.0.0.1" create
    exit
```
nat
outside
  pool "nat1-pool" nat-group 1 type large-scale create
    port-reservation ports 200
    address-range 81.81.0.0 81.81.6.0 create
  exit
  no shutdown
  exit
exit
exit
exit
exit
exit
vprn 550 customer 1 create
  interface "ip-13.0.0.1" create
  exit
exit
nat
  nat-policy "ls-outPolicy" create
    pool "nat1-pool" router 500
    timeouts
      udp hrs 5
      udp-initial min 4
    exit
  exit
exit
vprn 500 customer 1 create
  router-id 10.21.1.2
  route-distinguisher 500:10
  vrf-target export target:500:1 import target:500:1
  interface "ip-113.0.0.1" create
    address 113.0.0.1/24
    static-arp 113.0.0.5 14:99:01:01:00:01
    sap 1/1/1:200 create
    exit
  exit
  no shutdown
  exit
vprn 550 customer 1 create
  router-id 10.21.1.2
  route-distinguisher 550:10
  vrf-target export target:550:1 import target:550:1
  interface "ip-13.0.0.1" create
    address 13.0.0.1/8
    sap 1/2/1:900 create
    ingress
      filter ip 123
    exit
  exit
exit
nat
  inside
    nat-policy "ls-outPolicy"
  exit
exit
no shutdown
exit
exit
exit all
NAT Command Reference

Command Hierarchies

- NAT ISA Configuration Commands on page 493
- NAT Service Configuration Commands on page 493
- NAT Subscriber Management Commands on page 496
- NAT Router Configuration Commands on page 496
- NAT Show Commands on page 497
- NAT Filter Commands on page 498

NAT ISA Configuration Commands

```command
config
    isa
        nat-group nat-group-id [create]
        no nat-group
        active-mda-limit number
        no active-mda-limit
        description description-string
        no description
        [no] mda mda-id
        session-limits
            reserved num-sessions
            no reserved
            watermarks high percentage low percentage
            no watermarks
        [no] shutdown
```

NAT Service Configuration Commands

```command
configure
    service
        nat
            nat-policy nat-policy-name [create]
            no nat-policy nat-policy-name
            alg
                [no] ftp
                [no] rtsp
                [no] sip
            block-limit [1..40]
            no block-limit
            description description-string
            no description
```
— filtering filtering-mode
— no filtering
— pool nat-pool-name service-name service-name
— pool nat-pool-name router router-instance
— no pool
— port-limits
  — reserved num-ports
  — no reserved
  — watermarks high percentage-high low percentage-low
  — no watermarks
— [no] priority-sessions
  — [no] fc fc-name
— session-limits
  — max num-sessions
  — no max
  — reserved num-sessions
  — no reserved
  — watermarks high percentage-high low percentage-low
  — no watermarks
— [no] timeouts
  — icmp-query [min minutes] [sec<seconds]
  — no icmp-query
  — sip min minutes [sec<seconds]
  — no sip
  — tcp-established [hrs hours] [min minutes] [sec seconds]
  — no tcp-established
  — tcp-syn [hrs hours] [min minutes] [sec seconds]
  — no tcp-syn
  — tcp-time-wait [min minutes] [sec seconds]
  — no tcp-time-wait
  — tcp-transitory [hrs hours] [min minutes] [sec seconds]
  — no tcp-transitory
  — udp [hrs hours] [min minutes] [sec seconds]
  — no udp
  — udp-dns [hrs hours] [min minutes] [sec seconds]
  — no udp-dns
  — udp-initial [min minutes] [sec seconds]
  — no udp-initial
VPRN Commands

```
config
  service
    vprn service-id customer cust-id create
      nat
        inside
          destination-prefix ip-prefix/length
          12-aware
            address ip-address/mask
          nat-policy nat-policy-name
          no nat-policy
        outside
          pool nat-pool-name [nat-group nat-group-id type pool-type create]
          no pool nat-pool-name
            address-range start-ip-address end-ip-address
              [create]
          no address-range start-ip-address end-ip-address
            description description-string
          no description
            drain
          description description-string
          no description
          port-reservation blocks num-blocks
          port-reservation ports num-ports
          no port-reservation
          shutdown
          no subscriber-limit
          subscriber-limit [1..65535]
          no subscriber-limit
          watermarks high percentage-high low percentage-low
          no watermarks
```
NAT Subscriber Management Commands

configure
  — subscriber-mgmt
    — sub-profile
      — nat-policy policy-name
      — no nat-policy

NAT Router Configuration Commands

config
  — router
    — nat
      — inside
        — [no] destination-prefix ip-prefix/length
        — nat-policy nat-policy-name
        — no nat-policy
      — outside
        — pool nat-pool-name [nat-group nat-group-id type pool-type create]
        — no pool nat-pool-name
          — address-range start-ip-address end-ip-address [create]
          — no address-range start-ip-address end-ip-address
            — description description-string
            — no description
            — [no] drain
          — description description-string
          — no description
          — port-reservation blocks num-blocks
          — port-reservation ports num-ports
          — no port-reservation
          — [no] shutdown
          — watermarks high percentage-high low percentage-low
          — no watermarks
NAT Show Commands

show
   — isa
     — nat-group
     — nat-group nat-group-id [associations]
     — nat-group nat-group-id member [1..255] [statistics]
     — nat-group [nat-group-id] members
   — service
     — nat
       — l2-aware-hosts [outside-router router-instance] [outside-ip outside-ip-address]
         [inside-ip-prefix ip-prefix/mask]
       — l2-aware-subscribers [nat-policy nat-policy-name] [nat-group nat-group-id]
         [member [1..255]] [outside-router router-instance] [outside-ip outside-ip-address]
       — l2-aware-subscribers subscriber sub-ident
       — nat-policy nat-policy-name associations
       — nat-policy nat-policy-name statistics
       — nat-policy nat-policy-name
       — nat-policy

show
   — router
     — nat
       — l2-aware-blocks [outside-ip-prefix ip-prefix/length] [outside-port [1..65535]]
         [pool pool-name]
       — lsn-blocks [inside-router router-instance] [inside-ip ip-address] [outside-ip-prefix ip-prefix/length]
         [outside-port [1..65535]] [pool pool-name]
       — lsn-hosts host ip-address
       — lsn-hosts [outside-router router-instance] [outside-ip ip-address]
         [inside-ip-prefix ip-prefix/mask]
       — pool pool-name
       — pool
       — summary

Clear Commands

clear
   — nat
     — isa
       — nat-group nat-group-id member [1..255] l2-aware-subscribers
       — nat-group nat-group-id member [1..255] statistics

Tools Commands

tools
   — dump
     — nat
       — isa
NAT Command Reference

- **resources** mda mda-id
- **sessions** [nat-group nat-group-id] [mda mda-id] [protocol [icmp|tcp|udp]] [inside-ip ip-address] [inside-router router-instance] [inside-port port-number] [outside-ip ip-address] [outside-port port-number] [foreign-ip ip-address] [foreign-port port-number]

NAT Filter Commands

```
configure
  - filter
    - ip-filter filter-id
      - entry entry-id
        - action nat
        - no action
```
LNS and NAT Group Commands

```
config
  isa
    - ins-group ins-group-id [create]
    - no ins-group ins-group-id
      - description description-string
      - no description
      - mda mda-id [drain]
      - no mda mda-id
      - [no] shutdown
    - nat-group nat-group-id [create]
    - no nat-group nat-group-id
      - active-mda-limit number
      - no active-mda-limit
      - description description-string
      - no description
      - [no] mda mda-id
      - session-limits
        - reserved num-sessions
        - no reserved
        - watermarks high percentage low percentage
        - no watermarks
      - [no] shutdown
```
Network Address Translation Configuration Commands

NAT Router Configuration Commands

nat

**Syntax**  
[no] nat

**Context**  
config>service>vprn  
config>router

**Description**  
This command configures, creates or deletes a NAT instance.

inside

**Syntax**  
inside

**Context**  
config>service>vprn>nat  
config>router>nat

**Description**  
This command enters the “inside” context to configure the inside NAT instance.

outside

**Syntax**  
outside

**Context**  
config>service>vprn>nat  
config>router>nat

**Description**  
This command enters the “outside” context to configure the outside NAT instance.

destination-prefix

**Syntax**  
[no] destination-prefix ip-prefix/length

**Context**  
config>service>vprn>nat>inside  
config>router>nat>inside

**Description**  
This command configures a destination prefix. An (internal) static route will be created for this prefix. All traffic that hits this route will be subject to NAT. The system will not allow a destination-prefix to be configured if the configured nat-policy refers to an IP pool that resides in the same service (as this would result in a routing loop).
Parameters

- **ip-prefix** — Specifies the IP prefix; host bits must be zero (0).
  
  **Values**
  
  a.b.c.d

- **length** — Specifies the prefix length.
  
  **Values**
  
  0 — 32

l2-aware

**Syntax**

`l2-aware`

**Context**

`config>services>vprn>nat>inside`

**Description**

This command enters the “l2-aware” context for configuration specific to Layer 2-aware NAT.

address

**Syntax**

`[no] address ip-address/mask`

**Context**

`config>services>vprn>nat>inside>l2-aware`

**Description**

This command configures a Layer 2-aware NAT address. This address will act as a local address of the system. Hosts connected to the inside service will be able to ARP for this address. To verify connectivity, a host can also ping the address. This address is typically used as next hop of the default route of a Layer 2-aware host. The given mask defines a Layer 2-aware subnet. The (inside) IP address used by an Layer 2-aware host must match one of the subnets defined here or it will be rejected.

**Parameters**

- **ip-address** — Specifies the IP address in a.b.c.d format.
  
  **Values**
  
  16 — 32

- **mask** — Specifies the mask.
  
  **Values**
  
  16 — 32

nat-policy

**Syntax**

`nat-policy nat-policy-name`

`no nat-policy`

**Context**

`config>services>vprn>nat>inside`

`config>router>nat>inside`

**Description**

This command configures the NAT policy that will be used for large-scale NAT in this service.

**Parameters**

- **nat-policy-name** — Specifies the NAT policy name.
  
  **Values**
  
  32 chars max
pool

Syntax

pool nat-pool-name [nat-group nat-group-id type pool-type create]
no pool nat-pool-name

Context

config>service>vprn>nat>outside
config>router>nat>outside

Description

This command configures a NAT pool.

Parameters

nat-pool-name — Specifies the NAT pool name.

Values

32 chars max

nat-group-id — Specifies the NAT group ID.

Values

1 — 4

create — This parameter must be specified to create the instance.

pool-type — Species the pool type, either large-scale or L2-aware.

address-range

Syntax

address-range start-ip-address end-ip-address [create]
no address-range start-ip-address end-ip-address

Context

config>service>vprn>nat>outside>pool
config>router>nat>outside>pool

Description

This command configures a NAT address range.

Parameters

start-ip-address — Specifies the beginning IP address in a.b.c.d form.

end-ip-address — Specifies the ending IP address in a.b.c.d form.

create — This parameter must be specified to create the instance.

description

Syntax

description description-string
no description

Context

config>service>vprn>nat>outside>pool>address-range
config>service>vprn>nat>outside>pool
config>router>nat>outside>pool>address-range
config>router>nat>outside>pool

Description

This command configures the description for the NAT address range.

Parameters

description-string — Specifies the NAT address range description.

Values

80 chars max
Network Address Translation Configuration Commands

**drain**

**Syntax**

```
[no] drain
```

**Context**

```
config>service>vprn>nat>outside>pool>address-range
config>router>nat>outside>pool>address-range
```

**Description**

This command starts or stops draining this NAT address range. When an address-range is being drained, it will not be used to serve new hosts. Existing hosts, however, will still be able to use the address that was assigned to them even if it is being drained. An address-range can only be deleted if the parent pool is shut down or if the range itself is effectively drained (no hosts are using the addresses anymore).

**port-reservation**

**Syntax**

```
port-reservation blocks num-blocks
port-reservation ports num-ports
no port-reservation
```

**Context**

```
config>service>vprn>nat>outside>pool
config>router>nat>outside>pool
```

**Description**

This command configures the size of the port-block that will be assigned to a host that is served by this pool. The number of ports configured here will be available to UDP, TCP and ICMP (as identifiers).

**Parameters**

- **num-blocks** — Specifies the number of port-blocks per IP address. Setting num-blocks to one (1) for large scale NAT will enable 1:1 NAT for IP addresses in this pool.
  
  **Values**
  
  1 — 64512

- **num-ports** — Specifies the number of ports per block.
  
  **Values**
  
  1 — 32256

**shutdown**

**Syntax**

```
[no] shutdown
```

**Context**

```
config>service>vprn>nat>outside>pool
```

**Description**

This command administratively enables or disables the NAT pool.
subscriber-limit

Syntax:   subscriber-limit [1..65535]
          no subscriber-limit

Context:  config>service>vprn>nat>outside

Description: This command configures the maximum number of subscribers per outside IP address. In case multiple port blocks per subscriber are used, the block size is typically small; all blocks assigned to a given subscriber belong to the same IP address; the subscriber limit guarantees that any subscriber can get a minimum number of ports.

Default:  65535

Parameters:  limit — Specify the maximum number of subscribers per IP address.
             Values:  1..65535

watermarks

Syntax:   watermarks high percentage-high low percentage-low
          no watermarks

Context:  config>service>vprn>nat>outside>pool
          config>router>nat>outside>pool

Description: This command configures the watermarks for this NAT pool.

Parameters:  percentage-high — Specifies the high percentage.
             Values:  2 — 100

   percentage-low — Specifies the low percentage.
             Values:  1 — 99

filtering

Syntax:   filtering filtering-mode
          no filtering

Context:  config>service>nat>nat-policy

Description: This command configures the filtering of the NAT policy.

Parameters:  filtering-mode — Specifies the way that inbound traffic is filtered.
             Values:  address-and-port-dependent | endpoint-independent
pool

Syntax

pool nat-pool-name service-name service-name
pool nat-pool-name router router-instance
no pool

Context
config>service>nat>nat-policy

Description
This command configures the NAT pool of this policy.

Parameters

nat-pool-name — Specifies the name of the NAT pool.

Values
32 chars max

router-instance — Specifies the router instance the pool belongs to, either by router name or service ID.

Values
router-name: “Base” | “management”

Default
Base

Values
1 — 2147483648

svc-name — a string up to 64 characters in length.

service-name — Specifies the name of the service.

Values
64 chars max

port-limits

Syntax
port-limits

Context
config>service>nat>nat-policy

Description
This command configures the port limits of this policy.

reserved

Syntax
reserved num-ports
no reserved

Context
config>service>nat>nat-policy>port-limits

Description
This command configures the number of ports per block that will be reserved for prioritized sessions.

Parameters
num-ports — Specifies the number of ports to reserve for prioritized sessions.

Values
1 — 65534
watermarks

Syntax

```
watermarks high percentage-high low percentage-low
no watermarks
```

Context

```
config>service>nat>nat-policy port-limits
```

Description

This command configures the port usage watermarks for the NAT policy.

Parameters

- `percentage-high` — Specifies the high percentage.
  - Values: 1 — 100
- `percentage-low` — Specifies the low percentage.
  - Values: 0 — 99

priority-sessions

Syntax

```
[nop]
```

Context

```
config>service>nat>nat-policy
```

Description

This command configures the prioritized sessions of this NAT policy.

fc

Syntax

```
[nop] fc fc-name
```

Context

```
config>service>nat>nat-policy>priority-sessions
```

Description

This command configures the forwarding classes that have their sessions prioritized.

Parameters

- `fc-name` — Specifies the forwarding class.
  - Values: be | l2 | af | l1 | h2 | ef | h1 | nc

max

Syntax

```
max num-sessions
no max
```

Context

```
config>service>nat>nat-policy>session-limits
```

Description

This command configures the session limit of this policy. The session limit is the maximum number of sessions allowed for a subscriber associated with this policy.

Parameters

- `num-sessions` — Specifies the session limit.
  - Values: 1 — 65535
**timeouts**

Syntax: `[no] timeouts

Context: `config>service>nat>nat-policy`

Description: This command configures session idle timeouts for this policy.

**icmp-query**

Syntax: `icmp-query [min minutes] [sec seconds]

no icmp-query`

Context: `config>service>nat>nat-policy>timeouts`

Description: This command configures the timeout applied to an ICMP query session.

Parameters:
- `min minutes` — Specifies the timeout, in minutes, applied to an ICMP query session
  - Values: 1 — 4
  - Default: 1
- `sec seconds` — Specifies the timeout, in seconds, applied to an ICMP query session
  - Values: 1 — 59

**sip**

Syntax: `sip min minutes] [sec seconds]

no sip`

Context: `config>service>nat>nat-policy>timeouts`

Description: This command configures the SIP inactive media timeout.

Parameters:
- `min minutes` — Specifies the SIP inactive media timeout, in minutes.
  - Values: 1 — 4
  - Default: 1
- `sec seconds` — Specifies the SIP inactive media timeout, in seconds.
  - Values: 1 — 59
icmp-query

Syntax: `icmp-query [min minutes] [sec seconds]
no icmp`

Context: `config>service>nat>nat-policy>timeouts`

Description: This command configures the timeout applied to an ICMP query session.

Parameters:
- `minutes` — Specifies the timeout in minutes.
  - Values: 1 — 4
- `seconds` — Specifies the timeout in seconds.
  - Values: 1 — 59

tcp-established

Syntax: `tcp-established [hrs hours] [min minutes] [sec seconds]
no tcp-established`

Context: `config>service>nat>nat-policy>timeouts`

Description: This command configures the idle timeout applied to a TCP session in the established state.

Parameters:
- `hours` — Specifies the timeout hours field.
  - Values: 1 — 24
- `minutes` — Specifies the timeout minutes field.
  - Values: 1 — 59
- `seconds` — Specifies the timeout seconds field.
  - Values: 1 — 59

tcp-syn

Syntax: `tcp-syn [hrs hours] [min minutes] [sec seconds]
no tcp-syn`

Context: `config>service>nat>nat-policy>timeouts`

Description: This command configures the timeout applied to a TCP session in the SYN state.

Parameters:
- `hours` — Specifies the timeout hours field.
  - Values: 1 — 24
- `minutes` — Specifies the timeout minutes field.
  - Values: 1 — 59
Network Address Translation Configuration Commands

seconds — Specifies the timeout seconds field.

Values 1 — 59

tcp-time-wait

Syntax tcp-time-wait [min minutes] [sec seconds]
no tcp-time-wait

Context config>service>nat>nat-policy>timeouts

Description This command configures the timeout applied to a TCP session in a time-wait state.

Parameters minutes — Specifies the timeout minutes field.

Values 1 — 4

seconds — Specifies the timeout seconds field.

Values 1 — 59

tcp-transitory

Syntax tcp-transitory [hrs hours] [min minutes] [sec seconds]
no tcp-transitory

Context config>service>nat>nat-policy>timeouts

Description This command configures the idle timeout applied to a TCP session in a transitory state.

Parameters hours — Specifies the timeout hours field.

Values 1 — 24

minutes — Specifies the timeout minutes field.

Values 1 — 59

seconds — Specifies the timeout seconds field.

Values 1 — 59

udp

Syntax udp [hrs hours] [min minutes] [sec seconds]
no udp

Context config>service>nat>nat-policy>timeouts

Description This command configures the UDP mapping timeout.

Parameters hours — Specifies the timeout hours field.
Values | 1 — 24
--- | ---

*minutes* — Specifies the timeout minutes field.

Values | 1 — 59
--- | ---

*seconds* — Specifies the timeout seconds field.

Values | 1 — 59
--- | ---

**udp-dns**

Syntax: `udp-dns [hrs hours] [min minutes] [sec seconds]`

```
no udp-dns
```

Context: `config>service>nat>nat-policy>timeouts`

Description: This command configures the timeout applied to a UDP session with destination port 53.

Parameters:

*hours* — Specifies the timeout hours field.

Values | 1 — 24
--- | ---

*minutes* — Specifies the timeout minutes field.

Values | 1 — 59
--- | ---

*seconds* — Specifies the timeout seconds field.

Values | 1 — 59
--- | ---

**udp-initial**

Syntax: `udp-initial [min minutes] [sec seconds]`

```
no udp-initial
```

Context: `config>service>nat>nat-policy>timeouts`

Description: This command configures the UDP mapping timeout applied to new sessions.

Parameters:

*minutes* — Specifies the timeout minutes field.

Values | 1 — 4
--- | ---

*seconds* — Specifies the timeout seconds field.

Values | 1 — 59
--- | ---
NAT Service Configuration Commands

alg

Syntax: alg
Context: config>service>nat
Description: This command enables the context to configure Application Level Gateway parameters of this policy.

ftp

Syntax: [no] ftp
Context: config>service>nat>alg
Description: This command enables FTP ALG.
The no form of the command disables FTP ALG.
Default: ftp

rtsp

Syntax: [no] rtsp
Context: config>service>nat>alg
Description: This command enables RTSP ALG.
The no form of the command disables RTSP ALG.
Default: no rtsp

sip

Syntax: [no] sip
Context: config>service>nat>alg
Description: This command enables SIP ALG.
The no form of the command disables SIP ALG.
Default: no sip
block-limit

Syntax

block-limit [1..40]
no block-limit

Context

config>service>nat>alg

Description

This command configures the maximum number of port blocks per subscriber.

The no form of the command reverts to the default.

Default

1

nat-policy

Syntax

nat-policy nat-policy-name [create]
no nat-policy nat-policy-name

Context

config>service>nat

Description

This command configures a NAT policy.

Parameters

nat-policy-name — Specifies the NAT policy name.

Values

32 chars max
**NAT Subscriber Management Commands**

**nat-policy**

| Syntax      | nat-policy policy-name  
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>no nat-policy</td>
</tr>
</tbody>
</table>

**Context** config>subscriber-mgmt>sub-profile

**Description** This command configures the NAT policy to be used for subscribers associated with this subscriber profile.

**Parameters**  

- *policy-name* — Specifies the policy name.  
  - **Values** 32 chars max
NAT ISA Configuration Commands

nat-group

Syntax  

   nat-group  nat-group-id  [create]
   no  nat-group  nat-group-id

Context  
config>isa

Description  
This command configures an ISA NAT group.

active-mda-limit

Syntax  

   active-mda-limit  number
   no  active-mda-limit

Context  
config>isa>nat-group

Description  
This command configures the number of MDAs in this NAT ISA group that are intended for active use.

Parameters  

   number  —  Specifies the active MDA limit.

mda

Syntax  

   [no]  mda  mda-id

Context  
config>isa>nat-group

Description  
This command configures an ISA NAT group MDA.

Parameters  

   mda-id  —  Specifies the MDA ID in the slot/mda format.

   Values

      slot: 1 — 10
      mda: 1 — 2

session-limits

Syntax  

   session-limits

Context  
config>isa>nat-group

Description  
This command configures the ISA NAT group session limits.
reserved

Syntax reserved num-sessions
no reserved

Context config>isa>nat-group>session-limits

Description This command configures the number of sessions per block that will be reserved for prioritized sessions.

Parameters num-sessions — Specifies the number of sessions reserved for prioritized sessions.

Values 0 — 4194303

watermarks

Syntax watermarks high percentage low percentage
no watermarks

Context config>isa>nat-group>session-limits

Description This command configures the ISA NAT group watermarks.

high percentage — Specifies the high watermark of the number of sessions for each MDA in this NAT ISA group.

Values 2 — 100

low percentage — Specifies the low watermark of the number of sessions for each MDA in this NAT ISA group.

Values 1 — 99
NAT Show Commands

**nat-group**

Syntax:
- `nat-group nat-group-id [associations]`
- `nat-group nat-group-id member [1..255] [statistics]`
- `nat-group [nat-group-id] members`

**Context**
- `show>isa`

**Description**
This command displays ISA NAT group information.

**Parameters**
- `nat-group-id` — Specifies the NAT group ID.
  - **Values**: 1 — 4
- `statistics` — Keyword; displays NAT group statistics.

**Sample Output**

```
show isa nat-group
===============================================================================
ISA NAT Group Summary
===============================================================================
Mda Group 1 Group 2 Group 3
===============================================================================
3/1 active - -
3/2 - active busy
4/1 - busy active
4/2 - standby standby
===============================================================================
```

```
show isa nat-group 1
===============================================================================
ISA NAT Group 1
===============================================================================
Admin state : inService Operational state : inService
Active MDA limit : 1 Reserved sessions : 0
High Watermark (%) : (Not Specified) Low Watermark (%) : (Not Specified)
Last Mgmt Change : 02/04/2010 16:24:33
===============================================================================
ISA NAT Group 1 members
===============================================================================
Group Member State Mda Addresses Blocks Se-% Hi Se-Prio
===============================================================================
1 1 active 3/1 2 3 0 N 0
No. of members: 1
```
show isa nat-group members
===============================================================================
ISA NAT group members
===============================================================================
Group Member State Mda Addresses Blocks Se-% Hi Se-Prio
-------------------------------------------------------------------------------
1 1 active 3/1 2 3 0 N 0
2 1 active 3/2 0 0 0 N 0
3 1 active 4/1 0 0 0 N 0
-------------------------------------------------------------------------------
No. of members: 3
===============================================================================

show isa nat-group 1 members
===============================================================================
ISA NAT Group 1 members
===============================================================================
Group Member State Mda Addresses Blocks Se-% Hi Se-Prio
-------------------------------------------------------------------------------
1 1 active 3/1 2 3 0 N 0
-------------------------------------------------------------------------------
No. of members: 1
===============================================================================

show isa nat-group 1 member 1 statistics
===============================================================================
ISA NAT Group 1 Member 1
===============================================================================
no resource : 0
pkt rx on wrong port : 0
unsupported protocol : 0
no host : 0
no ip or port : 0
no matching flow : 0
max flow exceeded : 0
TCP no flow for RST : 0
TCP no flow for FIN : 0
TCP no flow : 0
addr. dep. filtering : 0
unsupported ICMP : 0
unsupported local ICMP : 0
ICMP checksum error : 0
ICMP embedded checksum error : 0
ICMP unsupported L4 : 0
pkt length error : 0
ICMP length error : 0
FTP ALG host refused : 0
FTP ALG no resource : 0
Pkt not ip : 7
Pkt rcv error : 0
Pkt ip exception : 8
Pkt fragmented : 0
Pkt not TCP or UDP : 0
Pkt error : 0
Pkt send error : 0
no policy : 0
locked by mgmt core : 0
l2-aware-hosts

Syntax  l2-aware-hosts [outside-router router-instance] [outside-ip outside-ip-address] [inside-ip-prefix ip-prefix/mask]

Context  show>service>nat

Description  This command displays layer-2 aware NAT hosts.

Parameters  

- **nat-policy-name** — Specifies the NAT policy name.
  
  **Values**  32 chars max

- **nat-group-id** — Specifies the NAT group ID.
  
  **Values**  1 — 4

- **router-instance** — Specifies the router instance.
  
  **Values**  
  router-name: Base , management
  service-id: 1 — 2147483647
  svc-name: A string up to 64 characters in length.

- **outside-ip-address** — Specifies the outside IP address.
  
  **Values**  a.b.c.d

- **sub-ident** — Specifies the identifier.
  
  **Values**  32 chars max
Sample Output

```
show service nat l2-aware-hosts
```

Layer-2-Aware NAT hosts

```
Inside IP Out-Router Outside IP Subscriber
13.0.0.100 Base 81.81.0.0 Sub001
13.0.0.102 Base 81.81.0.0 Sub001
13.0.0.101 Base 81.81.0.203 Sub002
13.0.0.103 Base 81.81.0.0 Sub003
```

No. of hosts: 4

---

L2-aware-subscribers

**Syntax**

```
l2-aware-subscribers [nat-policy nat-policy-name] [nat-group nat-group-id] [member [1..255]] [outside-router router-instance] [outside-ip outside-ip-address]
l2-aware-subscribers subscriber sub-ident
```

**Context**

```
show>service>nat
```

**Description**

This command displays layer-2 aware NAT subscribers.

**Parameters**

- **nat-policy-name** — Specifies the NAT policy name.
  
  **Values**
  32 chars max

- **nat-group-id** — Specifies the NAT group ID.
  
  **Values**
  1 — 4

- **router-instance** — Specifies the router instance.
  
  **Values**
  router-name: Base, management
  service-id: 1 — 2147483647
  svc-name: A string up to 64 characters in length.

- **outside-ip-address** — Specifies the outside IP address.
  
  **Values**
  a.b.c.d

- **sub-ident** — Specifies the identifier.
  
  **Values**
  32 chars max

**Sample Output**

```
show service nat l2-aware-subscribers
```

Layer-2-Aware NAT subscribers

```
Subscriber Policy Group/Member
Outside IP Router Ports
```
Sub001 outPolicy 1/1
81.81.0.0 Base 32-33
Sub002 outPolicy 2 1/1
81.81.0.203 Base 32-41
Sub003 outPolicy 1/1
81.81.0.0 Base 34-35

No. of subscribers: 3

show service nat l2-aware-subscribers subscriber "Sub881"

Layer-2-Aware NAT subscriber Sub001

Policy : outPolicy
ISA NAT group : 1
ISA NAT group member : 1
Outside router : Base
Outside IP : 81.81.0.0
ICMP Port usage (%) : < 1
ICMP Port usage high : false
UDP Port usage (%) : < 1
UDP Port usage high : false
TCP Port usage (%) : < 1
TCP Port usage high : false
Session usage (%) : < 1
Session usage high : false
Number of sessions : 0
Number of reserved sessions : 0
Ports : 32-33

nat-policy

Syntax

nat-policy

nat-policy-name associations
nat-policy

nat-policy-name

nat-policy

nat-policy-name statistics

Context

show>service>nat

Description

This command displays NAT policy information.

Parameters

nat-policy-name — Specifies the NAT Policy name.

Values

32 chars max

associations — Keyword; displays the router instances and/or subscriber profiles associated with the
NAT policy.

statistics — Keyword; displays statistics of the specified NAT policy.
Sample Output

show service nat nat-policy
===============================================================================
NAT policies
===============================================================================
Policy Description
-------------------------------------------------------------------------------
outPolicy
outPolicy2
outPolicy3
-------------------------------------------------------------------------------
No. of NAT policies: 3
===============================================================================

show service nat nat-policy "outPolicy2"
===============================================================================
NAT Policy outPolicy2
===============================================================================
Pool : MyPool2
Router : Base
Filtering : endpointIndependent
Reserved ports : 0
Port usage High Watermark (%) : (Not Specified)
Port usage Low Watermark (%) : (Not Specified)
Session limit : 65535
Reserved sessions : 0
Session usage High Watermark (%) : (Not Specified)
Session usage Low Watermark (%) : (Not Specified)
Prioritized forwarding classes : (Not Specified)
Timeout TCP established (s) : 7440
Timeout TCP transitory (s) : 240
Timeout TCP SYN (s) : 15
Timeout TCP TIME-WAIT (s) : 0
Timeout UDP mapping (s) : 300
Timeout UDP initial (s) : 15
Timeout UDP DNS (s) : 15
Timeout ICMP Query (s) : 60
Last Mgmt Change : 02/04/2010 15:33:05
===============================================================================

show service nat nat-policy "outPolicy2" associations
===============================================================================
NAT Policy outPolicy2 Subscriber Profile Associations
===============================================================================
sub_prof_B_3
-------------------------------------------------------------------------------
No. of subscriber profiles: 1
===============================================================================

show service nat nat-policy "outPolicy2" statistics
===============================================================================
NAT Policy outPolicy2 Statistics
===============================================================================
mda 3/1
-------------------------------------------------------------------------------
hostsActive : 1
Interface Configuration

hostsPeak : 1
sessionsTcpCreated : 0
sessionsTcpDestroyed : 0
sessionsUdpCreated : 0
sessionsUdpDestroyed : 0
sessionsIcmpQueryCreated : 0
sessionsIcmpQueryDestroyed : 0

---

### l2-aware-blocks

**Syntax**

```plaintext
l2-aware-blocks [outside-ip-prefix ip-prefix/length] [outside-port [1..65535]] [pool pool-name]
```

**Context**

```plaintext
show>router>nat
```

**Description**

This command displays Layer 2 aware NAT blocks.

**Parameters**

- `ip-prefix` — Specifies the IP prefix.
  - **Values**
    - a.b.c.d (host bits must be 0)

- `length` — Specifies the IP prefix length.
  - **Values**
    - 1 — 32

- `pool-name` — Specifies the pool name.
  - **Values**
    - 32 chars max

**Sample Output**

```plaintext
show router nat l2-aware-blocks
```

```plaintext
Layer-2-Aware NAT blocks for Base
```

```plaintext
81.81.0.0 [32..33]
Pool : MyPool
Policy : outPolicy
Started : 2010/02/04 16:24:55
Subscriber ID : Sub001
81.81.0.0 [34..35]
Pool : MyPool
Policy : outPolicy
Started : 2010/02/04 16:25:24
Subscriber ID : Sub002
81.81.0.203 [32..41]
Pool : MyPool2
Policy : outPolicy2
Started : 2010/02/04 16:25:21
Subscriber ID : Sub003
```

**Number of blocks:** 3
Isn-blocks

Syntax

```
lsn-blocks [inside-router router-instance] [inside-ip ip-address] [outside-ip-prefix ip-prefix/length] [outside-port [1..65535]] [pool pool-name]
```

Context

```
show>router>nat
```

Description

This command displays large scale NAT blocks.

Parameters

- **router-instance** — Specifies the router instance name and service ID.
  - **Values**
    - router-name: Base, management
    - service-id: 1 — 2147483647
    - svc-name: A string up to 64 characters in length.

- **ip-address** — Specifies the IP address in a.b.c.d format.
  - **Values**
    - a.b.c.d (host bits must be 0)

- **ip-prefix** — Specifies the IP prefix.
  - **Values**
    - a.b.c.d (host bits must be 0)

- **length** — Specifies the IP prefix length.
  - **Values**
    - 1 — 32

- **pool-name** — Specifies the pool name.
  - **Values**
    - 32 chars max

Sample Output

```
show router 588 nat isn-blocks
===============================================================================
Large-Scale NAT blocks for vprn500
===============================================================================
81.81.0.0 [1232..1431]
  Pool : nat1-pool
  Policy : ls-outPolicy
  Started : 2010/02/04 19:43:01
  Inside router : vprn550
  Inside IP address : 13.0.0.7
81.81.0.0 [1432..1631]
  Pool : nat1-pool
  Policy : ls-outPolicy
  Started : 2010/02/04 19:43:00
  Inside router : vprn550
  Inside IP address : 13.0.0.5
  ..
Number of blocks: 6
===============================================================================
```
lsn-hosts

**Syntax**

```
lsn-hosts host ip-address
lsn-hosts [outside-router router-instance] [outside-ip ip-address] [inside-ip-prefix ip-prefix/mask]
```

**Context**

```
show>router
```

**Description**

This command displays large scale NAT hosts.

**Parameters**

- `router-instance` — Specifies the router instance name and service ID.
  - **Values**
    - `router-name`: Base, management
    - `service-id`: 1 — 2147483647
    - `svc-name`: A string up to 64 characters in length.

- `ip-address` — Specifies the IP address in a.b.c.d format.

- `ip-prefix` — Specifies the IP prefix.
  - **Values**
    - a.b.c.d (host bits must be 0)

- `length` — Specifies the IP prefix length.
  - **Values**
    - 1 — 32

- `pool-name` — Specifies the pool name.
  - **Values**
    - 32 chars max

**Sample Output**

```
show router 558 nat lsn-hosts
===============================================================================
Large-Scale NAT hosts for router 550
===============================================================================
Inside IP Out-Router Outside IP
-------------------------------------------------------------------------------
13.0.0.5 500 81.81.0.0
13.0.0.6 500 81.81.3.1
13.0.0.7 500 81.81.0.0
13.0.0.8 500 81.81.0.0
13.0.0.9 500 81.81.3.1
13.0.0.10 500 81.81.0.0
-------------------------------------------------------------------------------
No. of hosts: 6
===============================================================================
show router 558 nat lsn-hosts host 13.8.8.5
===============================================================================
Large-Scale NAT host details
===============================================================================
Policy : ls-outPolicy
ISA NAT group : 1
ISA NAT group member : 1
Outside router : vprn500
Outside IP : 81.81.0.0
ICMP Port usage (%) : < 1
```
ICMP Port usage high : false
UDP Port usage (%) : 2
UDP Port usage high : false
TCP Port usage (%) : < 1
TCP Port usage high : false
Session usage (%) : < 1
Session usage high : false
Number of sessions : 5
Number of reserved sessions : 0
Ports : 1432-1631

pool

**Syntax**

```
pool pool-name
```

**Context**

```
show>router>nat
```

**Description**

This command displays NAT pool information.

**Parameters**

`pool-name` — Specifies the pool name.

**Values**

32 chars max

**Sample Output**

```
show router nat pool
===============================================================================
NAT pools
===============================================================================
Pool NAT-group Type Admin-state
-------------------------------------------------------------------------------
MyPool 1 l2Aware inService
MyPool2 1 l2Aware inService
-------------------------------------------------------------------------------
No. of pools: 2
===============================================================================
show router nat pool "MyPool"
===============================================================================
NAT Pool MyPool
===============================================================================
ISA NAT Group : 1
Pool type : l2Aware
Admin state : inService
Port reservation : 2 ports
Block usage High Watermark (%) : (Not Specified)
Block usage Low Watermark (%) : (Not Specified)
Block usage (%) : < 1
Last Mgmt Change : 02/04/2010 16:24:33
===============================================================================
NAT address ranges of pool MyPool
===============================================================================
```
Range Drain Num-blk

81.81.0.0 - 81.81.0.200 2

No. of ranges: 1

summary

Syntax     summary
Context    show>router>nat
Description This command displays the NAT information summary.

Sample Output

show router nat summary

NAT Layer-2-Aware addresses
Layer-2-Aware address subnet
13.0.0.1/16

No. of subnets: 1

NAT pools
Pool NAT-group Type Admin-state
MyPool 1 l2Aware inService
MyPool2 1 l2Aware inService

No. of pools: 2
NAT Tools Commands

nat-group

**Syntax**

```
nat-group nat-group-id member [1..255] l2-aware-subscribers
nat-group nat-group-id member [1..255] statistics
```

**Context**
clear>nat>isa

**Description**
This command clears ISA nat-group commands related statistics or removes all the subscribers that are associated with a specific nat-group member.

**Parameters**

- `nat-group-id` — Specifies the NAT group ID to clear.
  
  **Values**
  
  1 — 4

- `statistics` — Specifies to clear the NAT group ID’s statistics.

- `l2-aware-subscribers` — Specifies to clear the NAT group ID’s l2-aware subscribers.
NAT Tools Commands

nat

Syntax      nat
Context     tools>dump
Description This command enables the dump tools for NAT.

isa

Syntax      isa
Context     tools>dump>nat
Description This command enables the dump tools for NAT ISA.

resources

Syntax      resources mda mda-id
Context     tools>dump>nat>isa
Description This command enables dump ISA resources for an MDA.

sessions

Syntax      sessions [nat-group nat-group-id] [mda mda-id] [protocol {icmp|tcp|udp}] [inside-ip ip-address] [inside-router router-instance] [inside-port port-number] [outside-ip ip-address] [outside-port port-number] [foreign-ip ip-address] [foreign-port port-number]
Context     tools>dump>nat
Description This command dumps ISA sessions.

Sample Output

*A:Dut-C# tools dump nat sessions
===============================================================================
Matched 3 sessions on Slot #3 MDA #2
===============================================================================
Owner          : LSN-Host@11.11.12.12
Router         : 10
<table>
<thead>
<tr>
<th>Flow Type</th>
<th>TCP</th>
<th>Timeout (sec)</th>
<th>11</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inside IP Addr</td>
<td>11.11.12.12</td>
<td>Inside Port</td>
<td>99</td>
</tr>
<tr>
<td>Outside IP Addr</td>
<td>101.0.0.1</td>
<td>Outside Port</td>
<td>1537</td>
</tr>
<tr>
<td>Foreign IP Addr</td>
<td>10.10.10.10</td>
<td>Foreign Port</td>
<td>5678</td>
</tr>
<tr>
<td>Owner</td>
<td>LSN-Host@11.11.12</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Router</td>
<td>10</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Flow Type</td>
<td>ICMP</td>
<td>Timeout (sec)</td>
<td>59</td>
</tr>
<tr>
<td>Inside IP Addr</td>
<td>11.11.12.12</td>
<td>Inside Identifier</td>
<td>12345</td>
</tr>
<tr>
<td>Outside IP Addr</td>
<td>101.0.0.1</td>
<td>Outside Identifier</td>
<td>1535</td>
</tr>
<tr>
<td>Foreign IP Addr</td>
<td>10.10.10.10</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Owner</td>
<td>LSN-Host@11.11.12</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Router</td>
<td>10</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Flow Type</td>
<td>UDP</td>
<td>Timeout (sec)</td>
<td>109</td>
</tr>
<tr>
<td>Inside IP Addr</td>
<td>11.11.12.12</td>
<td>Inside Port</td>
<td>99</td>
</tr>
<tr>
<td>Outside IP Addr</td>
<td>101.0.0.1</td>
<td>Outside Port</td>
<td>1533</td>
</tr>
<tr>
<td>Foreign IP Addr</td>
<td>10.10.10.10</td>
<td>Foreign Port</td>
<td>5678</td>
</tr>
</tbody>
</table>

*A:Dut-C# tools*
NAT Filter Commands

action

Syntax  action nat
         no action

Context  config>filter>ip-filter>entry

Description  This command specifies packets matching the entry criteria will be subject to large-scale NAT.
Appendix A: 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 534
## 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><code>slot/mda/port[.channel]</code></td>
<td>1/1/5</td>
</tr>
<tr>
<td>qinq</td>
<td>`[port-id</td>
<td>bpgrp-id</td>
</tr>
<tr>
<td>frame-relay</td>
<td>`[port-id</td>
<td>aps-id ]:dlci</td>
</tr>
<tr>
<td>cisco-hdlc</td>
<td><code>slot/mda/port.channel</code></td>
<td>port-id: 1/1/3.1</td>
</tr>
</tbody>
</table>
**Appendix A: Common CLI Command Descriptions**

7750 SR:

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>sap-id</td>
<td><code>null</code> [port-id</td>
<td>bundle-id</td>
</tr>
<tr>
<td>dot1q</td>
<td>[port-id</td>
<td>bundle-id</td>
</tr>
<tr>
<td>qinq</td>
<td>[port-id</td>
<td>bundle-id</td>
</tr>
<tr>
<td>atm</td>
<td>[port-id</td>
<td>aps-id]</td>
</tr>
<tr>
<td>frame</td>
<td>[port-id</td>
<td>aps-id]</td>
</tr>
<tr>
<td>cisco-hdlc</td>
<td><code>slot/mda/port.channel</code> (default)</td>
<td></td>
</tr>
<tr>
<td>cem</td>
<td><code>slot/mda/port.channel</code> (default)</td>
<td></td>
</tr>
<tr>
<td>ima-grp</td>
<td>[bundle-id]</td>
<td><code>vpi1.vpi2</code> (default)</td>
</tr>
<tr>
<td>port-id</td>
<td><code>slot/mda/port[.channel]</code> (default)</td>
<td></td>
</tr>
<tr>
<td>bundle-id</td>
<td>bundle-type-sol/mda.bundle-num</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>bundle</code> keyword</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>type</code> ima, fr, ppp</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>bundle-num</code> 1 — 336</td>
<td></td>
</tr>
<tr>
<td>bpgrp-id</td>
<td>bpgrp-type-bpgrp-num</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>bpgrp</code> keyword</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>type</code> ima, ppp</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>bpgrp-num</code> 1 — 2000</td>
<td></td>
</tr>
<tr>
<td>aps-id</td>
<td>aps-group-id[.channel]</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>aps</code> keyword</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>group-id</code> 1 — 64</td>
<td></td>
</tr>
<tr>
<td>ccag-id</td>
<td>ccag-id.path-id[cc-type]:cc-id</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>ccag</code> keyword</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>id</code> 1 — 8</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>path-id</code> a, b</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>cc-type</code> .sap-net, .net-sap</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>cc-id</code> 0 — 4094</td>
<td></td>
</tr>
<tr>
<td>eth-tunnel</td>
<td>eth-tunnel-id[eth-tun-sap-id]</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>id</code> 1 — 1024</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>eth-tun-sap-id</code> 0 — 4094</td>
<td></td>
</tr>
<tr>
<td>lag-id</td>
<td>lag-id</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>lag</code> keyword</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>id</code> 1 — 200</td>
<td></td>
</tr>
<tr>
<td>qtag1</td>
<td>0 — 4094</td>
<td></td>
</tr>
<tr>
<td>qtag2</td>
<td>*, 0 — 4094</td>
<td></td>
</tr>
<tr>
<td>vpi</td>
<td>NNI: 0 — 4095</td>
<td></td>
</tr>
<tr>
<td></td>
<td>UNI: 0 — 255</td>
<td></td>
</tr>
<tr>
<td>vci</td>
<td>1, 2, 5 — 65535</td>
<td></td>
</tr>
<tr>
<td>dci</td>
<td>16 — 1022</td>
<td></td>
</tr>
<tr>
<td>ipsec-id</td>
<td>ipsec-id[private</td>
<td>public]:tag</td>
</tr>
<tr>
<td></td>
<td><code>id</code> 1 — 4</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>tag</code> 0 — 4094</td>
<td></td>
</tr>
</tbody>
</table>
7450 ESS:

<table>
<thead>
<tr>
<th>Variables</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sap-id</td>
<td>Values: sap-id null</td>
</tr>
<tr>
<td></td>
<td>[port-id</td>
</tr>
<tr>
<td>dot1q</td>
<td>[port-id</td>
</tr>
<tr>
<td>qinq</td>
<td>[port-id</td>
</tr>
<tr>
<td>atm</td>
<td>[port-id</td>
</tr>
<tr>
<td>frame</td>
<td>[port-id</td>
</tr>
<tr>
<td>cisco-hdlc</td>
<td>slot/mda/port.channel</td>
</tr>
<tr>
<td>ima-grp</td>
<td>[bundle-id]:vpi/vci[vpi1.vpi2]</td>
</tr>
<tr>
<td>port-id</td>
<td>slot/mda/port[.channel]</td>
</tr>
<tr>
<td>bundle-id</td>
<td>bundle-type-slot/mda.bundle-num</td>
</tr>
<tr>
<td></td>
<td>bundle keyword</td>
</tr>
<tr>
<td></td>
<td>type ima, fr, ppp</td>
</tr>
<tr>
<td></td>
<td>bundle-num 1 — 336</td>
</tr>
<tr>
<td>bpggrp-id</td>
<td>bpggrp-type-bpggrp-num</td>
</tr>
<tr>
<td></td>
<td>bpggrp keyword</td>
</tr>
<tr>
<td></td>
<td>type ima, ppp</td>
</tr>
<tr>
<td></td>
<td>bpggrp-num 1 — 2000</td>
</tr>
<tr>
<td>aps-id</td>
<td>aps-group-id[.channel]</td>
</tr>
<tr>
<td></td>
<td>aps keyword</td>
</tr>
<tr>
<td></td>
<td>group-id 1 — 64</td>
</tr>
<tr>
<td>ccag-id</td>
<td>ccag-id,path-id[cc-type]:cc-id</td>
</tr>
<tr>
<td></td>
<td>ccag keyword</td>
</tr>
<tr>
<td></td>
<td>id 1 — 8</td>
</tr>
<tr>
<td></td>
<td>path-id a, b</td>
</tr>
<tr>
<td></td>
<td>cc-type .sap-net, .net-sap</td>
</tr>
<tr>
<td></td>
<td>cc-id 0 — 4094</td>
</tr>
<tr>
<td>eth-tunnel</td>
<td>eth-tunnel-id[eth-tun-sap-id]</td>
</tr>
<tr>
<td></td>
<td>id 1 — 1024</td>
</tr>
<tr>
<td></td>
<td>eth-tun-sap-id 0 — 4094</td>
</tr>
<tr>
<td>lag-id</td>
<td>lag-id</td>
</tr>
<tr>
<td></td>
<td>lag keyword</td>
</tr>
<tr>
<td></td>
<td>id 1 — 200</td>
</tr>
<tr>
<td>qtag1</td>
<td>0 — 4094</td>
</tr>
<tr>
<td>qtag2</td>
<td>*, 0 — 4094</td>
</tr>
<tr>
<td>vpi</td>
<td>NNI: 0 — 4095</td>
</tr>
<tr>
<td></td>
<td>UNI: 0 — 255</td>
</tr>
<tr>
<td>vci</td>
<td>1, 2, 5 — 65535</td>
</tr>
<tr>
<td>dlc1</td>
<td>16 — 1022</td>
</tr>
</tbody>
</table>

**Common Service Commands**

**OS Multi-Service ISA Guide**
The following terms and acronyms describe the operation and maintenance of RET/FCC and ad insertion configurations are presented for reference purposes.

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AA-ISA</td>
<td>Application Aware Integrated Service Adapter</td>
</tr>
<tr>
<td>AA-Sub</td>
<td>The AA-ISA view of the AA context. Supported AA-subs types include ESM and SAPs, which mapped directly to divert contexts, spoke-SDP as AA-sub divert context, transit AA-sub type within a parent AA-sub divert context.</td>
</tr>
<tr>
<td>Parent AA-Sub</td>
<td>A SAP/SDP diverted to AA containing transit AA subs.</td>
</tr>
<tr>
<td>Transit AA Sub</td>
<td>An ISA local AA sub contained within a parent AA sub. There will be two types of transit AA subs:</td>
</tr>
<tr>
<td></td>
<td>• Transit IP AA-subs— Defined by transit IP policy as one or more /32 IP addresses per sub.</td>
</tr>
<tr>
<td>ADI</td>
<td>Ad Insertion</td>
</tr>
<tr>
<td>ADI-LZ</td>
<td>Ad Insertion Local and Zoned</td>
</tr>
<tr>
<td>Avail</td>
<td>An “available” part of the program stream where an authorized operator is allowed to replace the stream. A time space offered to cable operators by cable programming services during a program for use by the CATV operator; the time can be sold to local advertisers or used for channel self promotion.</td>
</tr>
<tr>
<td>BTV</td>
<td>Broadcast Television</td>
</tr>
<tr>
<td>DPI</td>
<td>Digital Program Insertion</td>
</tr>
<tr>
<td>Duplicate stream</td>
<td>Two or more streams where the SSRC and group are identical.</td>
</tr>
<tr>
<td>DRM</td>
<td>Digital Rights Management</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>--------</td>
<td>------------------------------------------------</td>
</tr>
<tr>
<td>DSLAM</td>
<td>Digital Subscriber Line Access Multiplexer</td>
</tr>
<tr>
<td>ES</td>
<td>Elementary Stream</td>
</tr>
<tr>
<td>ESM</td>
<td>Enhanced Subscriber Management</td>
</tr>
<tr>
<td>FCC</td>
<td>Fast Channel Change</td>
</tr>
<tr>
<td>GOP</td>
<td>Group of Pictures</td>
</tr>
<tr>
<td>HD</td>
<td>High Definition</td>
</tr>
<tr>
<td>HGW</td>
<td>Home Gateway</td>
</tr>
<tr>
<td>IPTV</td>
<td>Internet Protocol Television</td>
</tr>
<tr>
<td>ISA</td>
<td>Integrated Services Adapter</td>
</tr>
<tr>
<td>LoT</td>
<td>Loss of Transmission</td>
</tr>
<tr>
<td>MSTV</td>
<td>Microsoft Television</td>
</tr>
<tr>
<td>NTP</td>
<td>Network Time Protocol</td>
</tr>
<tr>
<td>PID</td>
<td>Packet Identifier</td>
</tr>
<tr>
<td>PMT</td>
<td>Program Map Table</td>
</tr>
<tr>
<td>PON</td>
<td>Passive Optical Network</td>
</tr>
<tr>
<td>RAM</td>
<td>Reporting and analysis manager</td>
</tr>
<tr>
<td>RG</td>
<td>Routed Gateway</td>
</tr>
<tr>
<td>RET</td>
<td>Retransmission</td>
</tr>
<tr>
<td>RTCP</td>
<td>RTP Control Protocol</td>
</tr>
<tr>
<td>RTP</td>
<td>Real-Time Transport Protocol</td>
</tr>
<tr>
<td>SAP</td>
<td>Subscriber or service access point</td>
</tr>
</tbody>
</table>

**Service Selection**

One service may have many component streams (which undergo selection).

**SSRC**

Synchronization source

**Stream Source**

A sequence of packets which comprise a service. A stream can have different sources.
| **STB** | Set Top Box |
| **TS** | Transport Stream |
| **VoD** | Video-on-Demand |
| **VQM** | Video Quality Monitoring |
Index

A
AA accounting files 75
AA-ISA groups 33
  bypass modes 36
  redundancy 37
accounting
  special study 73
  statistics and accounting 73
ad zones 383
adi
  local/zoned 380
  splicing 380
application assurance
  overview 22
application filters 72
application groups 71
application profiles 50
application QoS policies 91
application service options 52
applications 71
AQP 85
ASO 85

B
bursting 368
business VPN services 27

C
Card, MDA, Port
configuring
  command reference
    card commands 418
command reference
  application assurance 121, 124
    admin 122
    hardware 121
  ISA 122
  LNS and NAT group 499
  show 130
  tools 131
application assurance clear 131
application assurance debug 131
clear commands 479
debug commands 482
IPSec 267
IPSec commands
  configuration 267
  hardware 267
  show 275
IPSec configuration commands 267
NAT 493
show commands 463
video 417
  bundle and channel 420
  clear 425
  debug 426
  service interface 422
  show 425
configuration tasks
configuring
  accounting and billing statistics 114
  application filters 103
  application groups 104
  application profile 108
  application QoS policies 111
  application service options 113
  policers 109
policies
  aborting 102
  beginning and committing 102
  profile policies 102
  watermark 101
configuring 385, 397
  channel parameters 414
  FCC server 406
  NTP 414
  RET client 398, 412
  RET server 402
  service entities 389, 415
  video group 388, 413
video ISA module 387
video policy 390

D
denting 368
duplicate stream protection 352
duplicate stream selection 353

F
FCC 366
FCC server 372

G
glossary 537
group of pictures (GOP) 366

H
hardware
  IOM support 18
  MDA support 17
hardware features 17

I
IPSec 240

M
multicast information policies 350
multicast video quality monitoring 357

O
overview
  RET and FCC 365
  video ISA 16

P
policers 86
profile policies
  abort 102
  begin 102
  commit 102

protocol signatures 68

R
retransmission 365
  client 370
  server 371

S
server concurrency 374
software features
  application ID 64
  application QoS policies 91
  CLI batch commands 94
  identification components 66

T
ToD adjustments 93

V
video
  groups 348
  interface 349
  saps 349
video wholesale 257

X
X.509v3 certificate 254