7210 Service Access System

Release 25.9.R1

7210 SAS-R6, R12 Services Guide

3HE 21185 AAAB TQZZA 01
Edition: 01
September 2025

Nokia is committed to diversity and inclusion. We are continuously reviewing our customer documentation and consulting with standards bodies to ensure that terminology is inclusive and aligned with the industry. Our future customer documentation will be updated accordingly.

Table of contents

List of tables

List of figures

1 Getting started

This chapter provides process flow information to configure and provision services. It also provides an overview of the document organization and content, and describes the terminology used in this guide.

1.1 About this guide

Note:
Unless explicitly noted otherwise, this guide uses 7210 SAS-Dxp to refer to the 7210 SAS-Dxp 12p, 7210 SAS-Dxp 16p, and 7210 SAS-Dxp 24p platforms.

This guide describes the subscriber services support provided by the following 7210 SAS platforms, operating in one of the modes described in Table 1: Supported modes of operation and configuration methods. If multiple modes of operation apply, they are explicitly noted in the topic.

- 7210 SAS-R6
- 7210 SAS-R12

See 7210 SAS modes of operation for information about the modes of operation supported by the 7210 SAS product family.

Note:
Unless explicitly noted otherwise, the phrase "Supported on all 7210 SAS platforms as described in this document" is used to indicate that the topic and CLI commands apply to the following 7210 SAS platforms implicitly operating in the specified modes. See Table 1: Supported modes of operation and configuration methods for more information.

- network mode of operation

  7210 SAS-R6 and 7210 SAS-R12
- standalone mode of operation

  7210 SAS-R6 and 7210 SAS-R12

1.1.1 Document structure and content

This guide uses the following structure to describe routing protocols and route policies content.

Note:
This guide generically covers Release 25.*x*.R*x* content and may include some content that will be released in later maintenance loads. See the 7210 SAS Software Release Notes 25.*x*.R*x*, part number 3HE 21188 000*x* TQZZA, for information about features supported in each load of the Release 25.*x*.R*x* software.

- This guide is organized into functional chapters and provides concepts and descriptions of the implementation flow. Each chapter describes a software area and provides CLI syntax and command usage to configure parameters for the functional area.

- Command outputs shown in this guide are examples only; actual displays may differ depending on supported functionality and user configuration.
- Unless explicitly noted, the CLI commands and their configuration is similar for both network and access-uplink operating modes for features applicable to both modes of operation.

1.2 7210 SAS modes of operation

Unless explicitly noted, the phrase "mode of operation" and "operating mode" refers to the current operating mode of the 7210 SAS router. Each operating mode provides configuration access to a specific group of CLI commands.

Note:
Not all CLI commands are supported on all 7210 SAS platforms in all modes of operation. Users can only configure CLI commands supported by the current operating mode of the router. See the 7210 SAS Software Release Notes 25.*x*.R*x*, part number 3HE 21188 000*x* TQZZA, and to the appropriate 7210 SAS software user guide for information about features and capabilities supported by a 7210 SAS platform when operating in a specific mode.

The following modes of operation are supported by the 7210 SAS product family.

- **access-uplink**

  In the access-uplink operating mode, the 7210 SAS router uplinks to the network using Layer 2 Ethernet VLAN switching (without IP/MPLS).

  Platforms Supported: 7210 SAS-D, 7210 SAS-Dxp, 7210 SAS-K 2F1C2T, 7210 SAS-K 2F6C4T, 7210 SAS-K 3SFP+ 8C, and 7210 SAS-T

- **network**

  In the network operating mode, the 7210 SAS router uses IP/MPLS uplinks to the network. The IP routing protocols and MPLS functionality is available; see the appropriate 7210 SAS software user guide for more information about supported features.

  Platforms Supported: 7210 SAS-K 2F6C4T, 7210 SAS-K 3SFP+ 8C, 7210 SAS-Mxp, 7210 SAS-R6, 7210 SAS-R12, 7210 SAS-Sx/S 1/10GE, 7210 SAS-Sx 10/100GE, and 7210 SAS-T

- **satellite**

  In the satellite operating mode, the 7210 SAS platform uses high-capacity uplinks (for example, 10GE ports on the 7210 SAS-Mxp and 100GE ports on the 7210 SAS-Sx 10/100GE) to connect to the 7750 SR host. The 7210 SAS router is managed by the 7750 SR host. There is no direct CLI access to the satellite node, and all services and protocols are configured on the host.

  See the *7210 SAS-Mxp, R6, R12, S, Sx, T Basic System Configuration Guide* for boot options to configure the satellite mode of operation on the router. See the 7750 SR software user guides for information about service and protocol provisioning, and operating the 7210 SAS router in satellite mode.

  Platforms Supported: 7210 SAS-Mxp, 7210 SAS-Sx/S 1/10GE, and 7210 SAS-Sx 10/100GE

- **standalone**

  In the standalone operating mode, the 7210 SAS platform supports IP/MPLS uplinks. It is operated and managed independently.

The functionality and features available on the standalone 7210 SAS platform are similar to the network operating mode. The standalone mode is primarily used to differentiate between a node being managed by the 7750 SR host (in the satellite operating mode), and a node managed independently (standalone operating mode).

Platforms Supported: 7210 SAS-Mxp, 7210 SAS-Sx/S 1/10GE, and 7210 SAS-Sx 10/100GE

- **standalone-VC**

  In the standalone-VC operating mode, a set of 7210 SAS devices are stacked to provide larger 1GE/10GE port density and control-plane redundancy. The stack of nodes is provisioned and managed as a single chassis, and not as individual nodes.

  The functionality and features available on the 7210 SAS platform are similar to the network operating mode, with additional capabilities, such as control-plane redundancy with non-stop routing and non-stop services.

  Platforms Supported: 7210 SAS-Sx/S 1/10GE

For 7210 SAS platforms that support multiple explicit modes of operation (Table 1: Supported modes of operation and configuration methods), the operating mode must be configured in the Boot Option File (BOF) to ensure that the router boots up in the specified mode. For example, the 7210 SAS-T supports access-uplink and network modes of operation, and the 7210 SAS-Sx/S 1/10GE supports satellite, standalone, and standalone-VC mode of operations. In some cases, the 7210 SAS router operates in a specific mode implicitly, and explicit configuration is not required.

See the appropriate *Basic System Configuration Guide* for boot options and information about how to boot the 7210 SAS platform in a specific operating mode.

The following table lists the supported modes of operation and the configuration methods for the 7210 SAS platforms. Unless explicitly noted otherwise, the operating mode is supported on all variants of the specific 7210 SAS platform.

Table 1: Supported modes of operation and configuration methods

7210 SAS platform	Mode of operation and configuration method				
	Network	Access-uplink	Standalone	Standalone-VC	Satellite
7210 SAS-D		Implicit	Implicit		
7210 SAS-Dxp		Implicit	Implicit		
7210 SAS-K 2F1C2T		Implicit	Implicit		
7210 SAS-K 2F6C4T[1]	Port Mode Configuration[2]	Port Mode Configuration[2]	Implicit		
7210 SAS-K 3SFP+ 8C[1]	Port Mode Configuration[2]	Port Mode Configuration[2]	Implicit		

1 By default, the 7210 SAS-K 2F6C4T and 7210 SAS-K 3SFP+ 8C boot up in the network mode of operation. These platforms also allow the use of access-uplink port mode (without explicit BOF configuration), which provides the option to use Layer 2 uplinks instead of IP/MPLS uplinks to the network core, similar to the 7210 SAS-K 2F1C2T router.

2 See section 7210 SAS port modes for information about port mode configuration

7210 SAS platform	Mode of operation and configuration method				
	Network	Access-uplink	Standalone	Standalone-VC	Satellite
7210 SAS-Mxp	Implicit[3]		Explicit BOF Configuration		Explicit BOF Configuration
7210 SAS-R6 [4]	Implicit		Implicit		
7210 SAS-R12 [4]	Implicit		Implicit		
7210 SAS-Sx/S 1/10GE	Implicit[3]		Explicit BOF Configuration	Explicit BOF Configuration	Explicit BOF Configuration
7210 SAS-Sx 10/100GE	Implicit[3]		Explicit BOF Configuration		Explicit BOF Configuration
7210 SAS-T	Explicit BOF Configuration	Explicit BOF Configuration	Implicit		

1.3 7210 SAS port modes

Unless explicitly noted, the phrase "port mode" refers to the current port configuration of the 7210 SAS node. The 7210 SAS platform supports the configuration of the following port modes.

- **access port mode**

  Access ports are configured for customer-facing traffic if Service Access Points (SAPs) are required. The appropriate encapsulation type must be configured to distinguish the services on the port; services are configured on the port based on the encapsulation value.

  Access ports can be configured on all the 7210 SAS platforms.

- **access-uplink port mode**

  Access-uplink ports provide native Ethernet connectivity in service provider transport or in an infrastructure network. With this option, the encap-type can be configured to only QinQ. Access-uplink SAPs, which are QinQ SAPs, can only be configured on an access-uplink port to allow the operator to differentiate multiple services being carried over a single uplink port.

  This is the default port mode of a 7210 SAS node in the access-uplink mode of operation.

- **network port mode**

  Network ports are configured for network-facing traffic in the service provider transport or infrastructure network, and provide IP/MPLS uplinks.

  This is the default port mode of a 7210 SAS node in the network or standalone mode of operation.

- **hybrid port mode**

  Hybrid ports are configured for access and network facing traffic, and allow a single port to operate in both access and network modes.

[3] Implicitly operates in network mode when standalone mode of operation is configured

[4] Supports MPLS uplinks only and implicitly operates in network mode

Port modes available for configuration on a 7210 SAS node are determined by the current mode of operation of the router.

Note:
The 7210 SAS-K 2F6C4T and 7210 SAS-K 3SFP+ 8C are unique; all port modes listed in Table 2: Supported port modes by mode of operation are available for configuration on the router, regardless of the current mode of operation.

The following table lists the port mode configuration support per 7210 SAS mode of operation.

Table 2: Supported port modes by mode of operation

Mode of operation	Supported port mode			
	Access	Network	Hybrid	Access-uplink
Access-uplink	✓			✓
Network	✓	✓	✓	
Satellite [5]				
Standalone	✓	✓	✓	
Standalone-VC	✓	✓	✓	

The following table lists the port mode configuration supported by the 7210 SAS product family. See the appropriate *Interface Configuration Guide* for more information about configuring the port modes for a specific platform.

Table 3: 7210 SAS platforms supporting port modes

Platform	Port mode			
	Access	Network	Hybrid	Access-uplink
7210 SAS-D	Yes	No	No	Yes
7210 SAS-Dxp	Yes	No	No	Yes
7210 SAS-K 2F1C2T	Yes	No	No	Yes
7210 SAS-K 2F6C4T	Yes	Yes	Yes	Yes
7210 SAS-K 3SFP+ 8C	Yes	Yes	Yes	Yes
7210 SAS-Mxp	Yes	Yes	Yes	No
7210 SAS-R6 IMM-b (IMMv2)	Yes	Yes	Yes	No

[5] Port modes are configured on the 7750 SR host and managed by the host.

Platform	Port mode			
	Access	Network	Hybrid	Access-uplink
7210 SAS-R6 IMM-c 100GE (IMM-c 1QSFP28)	Yes	Yes	Yes	No
7210 SAS-R12 IMM-b	Yes	Yes	Yes	No
7210 SAS-R12 IMM-c 100GE (IMM-c 1QSFP28)	Yes	Yes	Yes	No
7210 SAS-Sx/S 1/10GE	Yes	Yes	Yes	No
7210 SAS-Sx 10/100GE	Yes	Yes	Yes	No
7210 SAS-T	Yes	Yes [6]	Yes [7]	Yes [8]

1.4 7210 SAS services configuration process

The following table lists the tasks necessary to configure subscriber services and configure mirroring.

This guide is presented in an overall logical configuration flow. Each section describes a software area and provides CLI syntax and command usage to configure parameters for a functional area.

Table 4: Configuration process

Area	Task	Chapter
Subscribers	Subscriber services	
	Global entities	Configuring global service entities with CLI
	VLL services	Ethernet pipe (Epipe) services
	EVPN	Ethernet Virtual Private Networks
	VPLS service	Virtual Private LAN Service
	IES service	Internet Enhanced Service
Reference	List of IEEE, IETF, and other proprietary entities.	Standards and protocol support

6 Network ports are supported only if the node is operating in network mode.

7 Hybrid ports are supported only if the node is operating in network mode.

8 Access-uplink ports are supported only if the node is operating in access-uplink mode.

1.5 Conventions

This section describes the general conventions used in this guide.

1.5.1 Precautionary and information messages

The following information symbols are used in the documentation.

DANGER: Danger warns that the described activity or situation may result in serious personal injury or death. An electric shock hazard could exist. Before you begin work on this equipment, be aware of hazards involving electrical circuitry, be familiar with networking environments, and implement accident prevention procedures.

WARNING: Warning indicates that the described activity or situation may, or will, cause equipment damage, serious performance problems, or loss of data.

Caution: Caution indicates that the described activity or situation may reduce your component or system performance.

Note: Note provides additional operational information.

Tip: Tip provides suggestions for use or best practices.

1.5.2 Options or substeps in procedures and sequential workflows

Options in a procedure or a sequential workflow are indicated by a bulleted list. In the following example, at step 1, the user must perform the described action. At step 2, the user must perform one of the listed options to complete the step.

Example: Options in a procedure

1. User must perform this step.
2. This step offers three options. User must perform one option to complete this step:
   - This is one option.
   - This is another option.
   - This is yet another option.

Substeps in a procedure or a sequential workflow are indicated by letters. In the following example, at step 1, the user must perform the described action. At step 2, the user must perform two substeps (a. and b.) to complete the step.

Example: Substeps in a procedure

1. User must perform this step.
2. User must perform all substeps to complete this action:
   a. This is one substep.

b. This is another substep.

2 Services overview

This chapter provides an overview of the 7210 SAS-R6 and 7210 SAS-R12-series subscriber services, service model, and service entities. Additional information about the individual subscriber services is in subsequent chapters.

2.1 Introduction

A service is a globally unique entity that refers to a type of connectivity service for either Internet or VPN connectivity. Each service is uniquely identified by a service ID and an optional service within a service area. The 7210 SAS-series service model uses logical service entities to construct a service. In the service model, logical service entities provide a uniform, service-centric configuration, management, and billing model for service provisioning.

In the 7210 SAS-series routers, services can provide Layer 2/bridged service between a service access point (SAP) and another service access point (a SAP is where traffic enters and exits the service) on the same (local) router or another router (distributed). A distributed service spans more than one router.

Distributed services use service distribution points (SDPs) to direct traffic through a service tunnel to another 7210 SAS router, SR router, or other router that supports MPLS. SDPs are created on each participating router, specifying the origination address (the router participating in the service communication) and the destination address of another router. SDPs are then bound to a specific customer service. Without the binding process, the far-end router is not able to participate in the service (there is no service without associating an SDP with the service).

2.1.1 Service types

The 7210 SAS-R6 and 7210 SAS-R12 provide the following types of subscriber services, which are described in more detail in the referenced chapters:

- Virtual Leased Line (VLL) Ethernet pipe (Epipe) services - a Layer 2 point-to-point VLL service for Ethernet frames. See Ethernet pipe (Epipe) services for more information about Epipe
- Virtual Private LAN Service (VPLS) - a Layer 2 multipoint-to-multipoint VPN. See Virtual Private LAN Service for more information about VPLS
- Internet Enhanced Service (IES) - a routed connectivity service used to provide IP services. See Internet Enhanced Service
- Virtual Private Routed Network (VPRN) - a Layer 3 IP multipoint-to-multipoint VPN service as defined in RFC 2547bis. See Virtual Private Routed Network service

2.1.2 Service policies

Common to all 7210 SAS-series connectivity services are policies that are assigned to the service. Policies are defined at a global level, then applied to a service on the router. Policies are used to define 7210 SAS-

series service enhancements. The types of policies that are common to all 7210 SAS-series connectivity services, and their functions, are:

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

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

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

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

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

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

2.2 Nokia service model

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

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

- Many services can be bound to a single customer.
- QoS policies, filter policies, and accounting policies are applied to each service instead of correlating parameters and statistics from ports to customers to services.

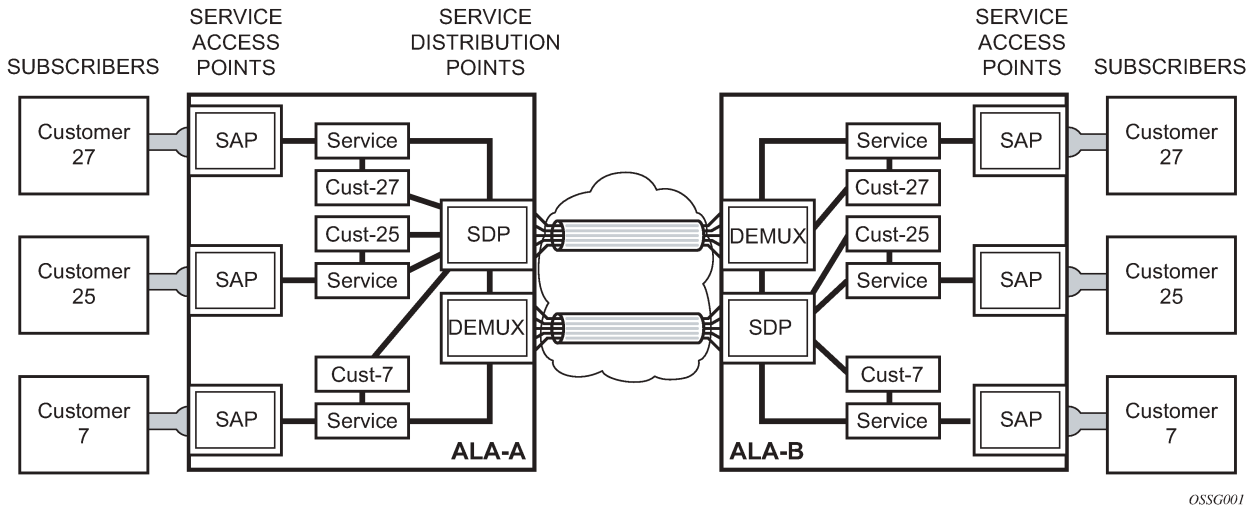
Service provisioning uses logical entities to provision a service where additional properties can be configured for bandwidth provisioning, QoS, security filtering, and accounting/billing to the appropriate entity.

2.3 Service entities

The following sections describe the basic logical entities in the service model used to construct a service.

The following figure shows service entities for 7210 SAS devices configured in network mode.

Figure 1: Service entities for 7210 SAS devices configured in network mode



2.3.1 Customers

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

2.3.2 SAPs

Each subscriber service type is configured with at least one SAP. A SAP identifies the customer interface point for a service on a 7210 SAS router. The SAP configuration requires that slot, MDA, and port information be specified. The slot, MDA, and port parameters must be configured before provisioning a service (see the Cards, MDAs, and Ports sections of the *7210 SAS-Mxp, R6, R12, S, Sx, T Interface Configuration Guide*).

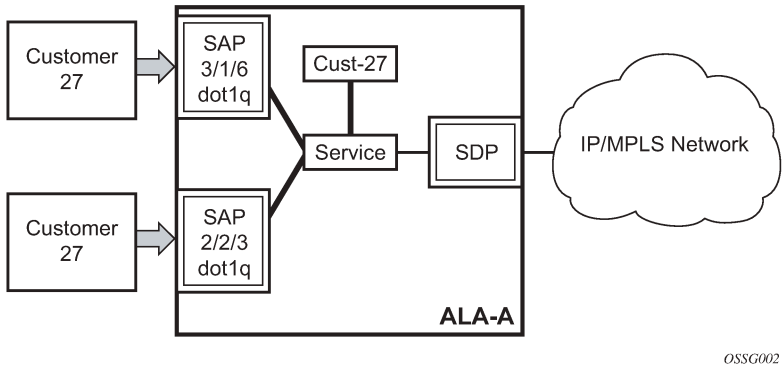
A SAP is a local entity to the router and is uniquely identified by:

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

Depending on the encapsulation, a physical port can have more than one SAP associated with it. SAPs can only be created on ports designated as "access" in the physical port configuration.

The following figure shows SAPs used for customer service delivery, with SDP used for service transport on 7210 SAS devices that support MPLS uplinks (also known as network mode platforms).

Figure 2: SAPs for 7210 SAS configured in network mode



2.3.2.1 SAP encapsulation types and identifiers

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

2.3.2.2 Ethernet encapsulations

The following lists encapsulation service options on Ethernet ports:

- **null**

  Supports a single service on the port. For example, where a single customer with a single service customer edge (CE) device is attached to the port. The encapsulation ID is always 0 (zero).

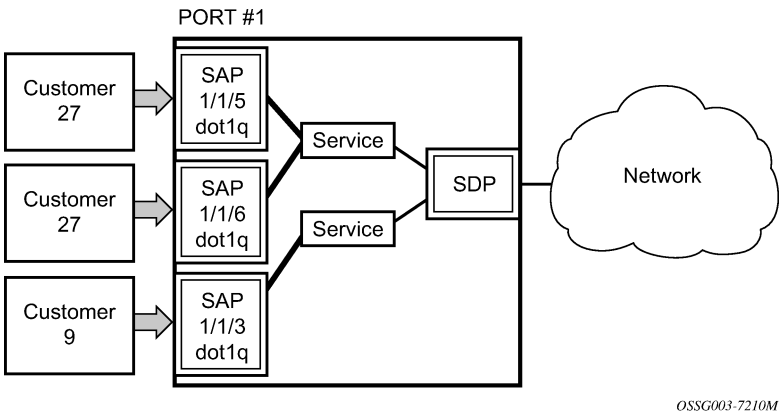
- **dot1q**

  Supports multiple services for one customer or services for multiple customers (Figure 3: Multiple SAPs on a single port). The encapsulation ID used to distinguish an individual service is the VLAN ID in the IEEE 802.1Q header. For example, the port is connected to a Ethernet switch with multiple downstream customers.

- **QinQ**

  The QinQ encapsulation type adds a IEEE 802.1Q tag to the 802.1Q tagged packets entering the network, to expand the VLAN space by tagging tagged packets, producing a double-tagged frame. The 7210 SAS-R6, and 7210 SAS-R12 support QinQ encapsulation for access ports in network mode.

Figure 3: Multiple SAPs on a single port



The preceding figure shows multiple SAPs used for customer service delivery on the same port and belonging to the same service, along with SDP used for service transport on 7210 SAS devices that support MPLS uplinks (also known as network mode platforms). This is supported only in network mode.

2.3.2.3 Services and SAP encapsulations

The following table lists the service and SAP encapsulation information for Ethernet ports.

Table 5: Service and SAP encapsulation

Port type	Encapsulation
Ethernet	null
Ethernet	Dot1q
Ethernet	QinQ

- When a VPLS service with default QinQ SAPs on the ring ports is used for transit traffic in a ring deployment, users can use either G.8032 or M-VPLS with xSTP for ring protection. When using G.8032, the state of the default QinQ SAPs in the VPLS service can be managed using a separate G.8032 control instance.

  Note:
  A G.8032 control instance cannot use default QinQ SAPs.

- MVPLS with xSTP can be used for loop prevention. The default QinQ SAPs inherit the state from the associated MVPLS instance.

2.3.2.4 SAP configuration considerations

The following considerations apply to SAP configurations:

- A SAP is a local entity and only locally unique to a specific device. The same SAP ID value can be used on another 7210 SAS-series device.
- By default, no SAPs are configured on the node. All SAPs in subscriber services must be created.
- At creation, the default administrative state for a SAP is set to administratively enabled.
- When a SAP is deleted, all configuration parameters for the SAP are also deleted.
- A SAP is owned by and associated with the service in which it is created in each router.
- On a port with a dot1q encapsulation type, traffic for the SAP is identified based on a specific IEEE 802.1Q VLAN ID value. The VLAN ID is stripped off at SAP ingress and the appropriate VLAN ID added at SAP egress. As a result, VLAN IDs only have local significance, and configuring identical VLAN IDs for each SAP on a service is not required.
- If a port is administratively shutdown, all SAPs on that port are operationally out of service.
- QinQ access SAPs of type Q1.0 are supported only for IES, VPRN, and R-VPLS services. They are not supported for Layer 2 services.
- A SAP cannot be deleted until it has been administratively disabled (shutdown).
- Each SAP can have one each of the following policies assigned:
  - ingress filter policy
  - egress filter policy
  - ingress QoS policy
  - accounting policy

2.3.3 QinQ SAP configuration restrictions for 7210 SAS in network mode only

The following are the QinQ access SAP configuration guidelines for 7210 SAS in network mode only:

- Tagged packets received on SAPs configured in a service in which a QinQ SAP is also in use are processed (not applicable when a QinQ SAP is not provisioned in a service).
- When a QinQ SAP is configured in a service, the number of VLAN tags in the packets received on null SAP, dot1q SAP, and QinQ SAP configured in the same service should match the number of VLAN tags implied by the port encapsulation mode. Packets that do not match are dropped by the hardware. That is, packets received with more than two VLAN tags on a QinQ SAP are dropped, packets received with more than one VLAN tag on a dot1q SAP are dropped, and packets received with tags (even packets with a priority tag) on a null SAP are dropped. In this document, such packets are referred to as extra-tag packets.
- When a QinQ SAP is configured in a service, the number of VLAN tags in the packets received on the VC/pseudowire of type VC-VLAN should be exactly one and packets received on the VC/pseudowire of type VC-Ether-should contain no tags (not even priority tags). If either case, packets that contain more VLAN tags than the number specified previously are dropped. In this document, such packets are referred to as extra-tag packets.
- The system provides a limited number of counters for the extra-tag packets dropped on SAP ingress. These counters are intended for diagnostic use.

  The following table describes the SAP types allowed in a service when QinQ SAP is in use.

Table 6: SAP types in a service when QinQ SAP is in use (network mode operation)

SAP configured in the service	SAPs not allowed for configuration in same service
QinQ	Q.* SAP, Dot1q default SAP
Q.*	Q1.Q2
Dotq1 default SAP	Q1.Q2

A 0.* QinQ SAP configured in the service only accepts untagged or priority-tagged packets, regardless of whether a QinQ SAP is configured in the service.

Note:
The 7210 SAS supports a mechanism to transport QinQ packets in an Epipe with two or more tags, with some restrictions. For more information, see Ethernet pipe (Epipe) services .

2.3.4 SDPs

An SDP provides a logical way to direct traffic from one router to another through a unidirectional (one-way) service tunnel. The SDP terminates at the far-end router, which directs packets to the correct service egress SAPs on that router. A distributed service consists of a configuration with at least one SAP on a local node, one SAP on a remote node, and an SDP that binds the service to the service tunnel.

An SDP has the following characteristics:

- An SDP is locally unique to a participating router. The same SDP ID can appear on other 7210 SAS-series routers.
- An SDP uses the system IP address to identify the far-end edge router.
- An SDP is not specific to any one service or any type of service. When an SDP is created, services are bound to the SDP. An SDP can also have more than one service type associated with it.
- All services mapped to an SDP use the same transport encapsulation type defined for the SDP.
- An SDP is a management entity. Even though the SDP configuration and the services carried within are independent, they are related objects. Operations on the SDP affect all the services associated with the SDP. For example, the operational and administrative state of an SDP controls the state of services bound to the SDP.

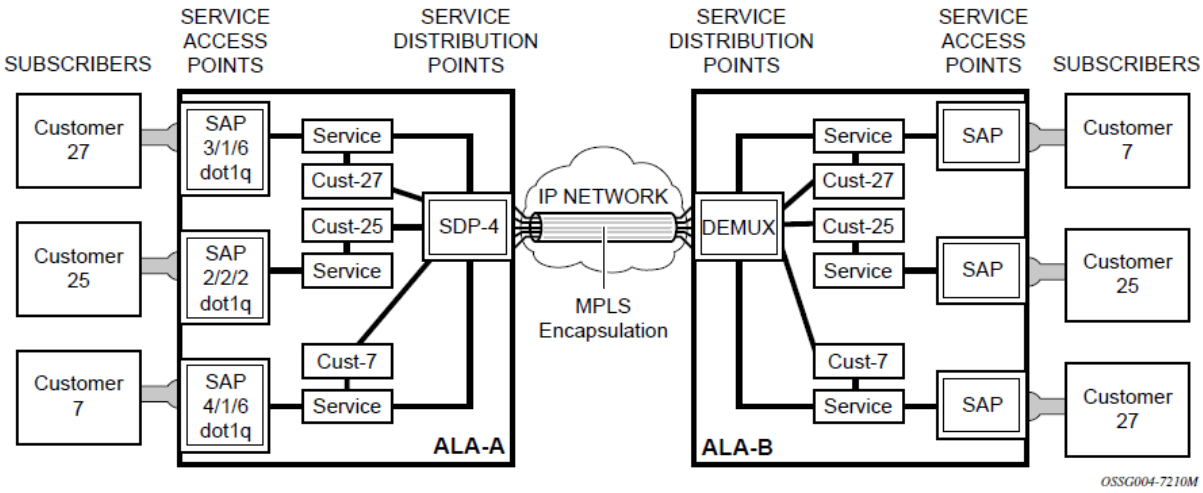
An SDP from the local router to a far-end router requires a return path SDP from the far-end router back to the local router. Each device must have an SDP defined for every remote router to which it needs to provide service. SDPs must be created first, before a distributed service can be configured.

2.3.4.1 SDP binding

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

The following figure shows MPLS service distribution point pointing from ALA-A to ALA-B.

Figure 4: MPLS SDP pointing from ALA-A to ALA-B



2.3.4.2 Spoke and mesh SDPs

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

A spoke-SDP is treated like the equivalent of a traditional bridge "port" where flooded traffic received on the spoke-SDP is replicated on all other "ports" and not transmitted on the port it was received.

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

2.3.4.3 SDP using BGP route tunnel

SDPs are enhanced to use BGP route tunnel to extend inter-AS support for Layer 2 and Layer 3 VPN services. An SDP can be configured to use the MPLS transport method. MPLS SDP support is enhanced to allow a BGP route tunnel to reach the far-end PE. A single method of tunneling is allowed per SDP (for example, LDP, RSVP-TE LSP, or BGP route tunnel). The BGP route tunnel method is excluded if multi-mode transport is enabled for an SDP.

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

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

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

2.3.4.4 SDP keepalives

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

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

- admin up/admin down state
- hello time
- message length
- max drop count
- hold down time

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

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

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

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

For information about configuring keepalive parameters, see Configuring an SDP.

2.3.4.5 SDP administrative groups

This feature provides the support of SDP administrative groups, referred to as SDP admin groups. SDP admin groups provide a way for services using a PW template to automatically include or exclude specific provisioned SDPs. SDPs sharing a specific characteristic or attribute can be made members of the same admin group.

The user first creates the admin groups that are to be used by SDPs on this node:

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

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

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

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

config>service>sdp>sdp-group *group-name*

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

The user then selects which admin groups to include or exclude in a specific PW template:

config>service>pw-template>sdp-include *group-name*

config>service>pw-template>sdp-exclude *group-name*

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

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

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

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

config>service>vpls>bgp>pw-template-binding *policy-id*

config>service>epipe>spoke-sdp-fec>pw-template-bind *policy-id*

The group value is used to uniquely identify an SDP admin group throughout the network in the 5620 SAM. The node sends both the group name and value to 5620 SAM, or other SNMP device, at the creation of the SDP admin group. In all other operations in the node, such as adding an SDP to an admin group or including/excluding an SDP admin group in a service context, only the group name is sent to the 5620 SAM or the SNMP device.

SDP admin groups can be enabled on all 7210 services that make use of the PW template (that is, BGP-AD VPLS service, BGP-VPLS service, BGP-VPWS and FEC129 VLL service).

2.3.4.6 Mixed-LSP mode of operation

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

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

At any specific time, the service manager programs only one type of LSP in the line card, which activates it to forward service packets according to the following priority order:

1. **RSVP LSP type**

   One RSVP LSP can be configured per SDP. This is the highest priority LSP type.

2. **LDP LSP type**

   One LDP FEC is used per SDP. The 7210 SAS does not support LDP ECMP.

3. **BGP LSP type**

   One RFC 3107-labeled BGP prefix programmed by the service manager.

In the case of the RSVP/LDP SDP, the service manager programs the NHLFEs for the active LSP type, preferring the RSVP LSP type over the LDP LSP type. If no RSVP LSP is configured or all configured RSVP LSPs go down, the service manager reprograms the line-card with the LDP LSP, if available. If not, the SDP goes operationally down.

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

Note:
LDP uses a tunnel down damp timer which is set to three seconds by default. When the LDP LSP fails, the SDP will revert to the RSVP LSP type after the expiry of this timer. For an immediate switchover this timer must be set to zero. Use the **configure>router>ldp>tunnel-down-damp-time** command. For more information, see the *7210 SAS-Mxp, R6, R12, S, Sx, T MPLS Guide*.

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

In the case of the LDP/BGP SDP, the service manager prefers the LDP LSP type over the BGP LSP type. The service manager reprograms the line card with the BGP LSP, if available; otherwise, it brings down the SDP operationally.

Note:
The following are differences in behavior of the LDP/BGP SDP compared to that of an RSVP/LDP SDP:

- For a specific /32 prefix, only a single route exists in the routing table: the IGP route or the BGP route. Therefore, either the LDP FEC or the BGP label route is active at any specific time. The impact of this is that the tunnel table needs to be reprogrammed each time a route is deactivated and the other is activated.
- The SDP revert-time cannot be used, because there is no situation where both LSP types are active for the same /32 prefix.

2.3.4.7 G.8032 Ethernet ring protection switching

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

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

Rings are preferred in data networks where the native connectivity is laid out in a ring or there is a requirement for simple resilient LAN services. Because of the symmetry and the simple topology, rings are viewed a good solution for access and core networks where resilient LANS are required. The Nokia implementation of G.8032 Eth-ring can be used for interconnecting access rings and to provide

traffic engineered backbone rings. The 7210 SAS implementation of G.8032 Eth-ring supports dual interconnected rings with sub-rings.

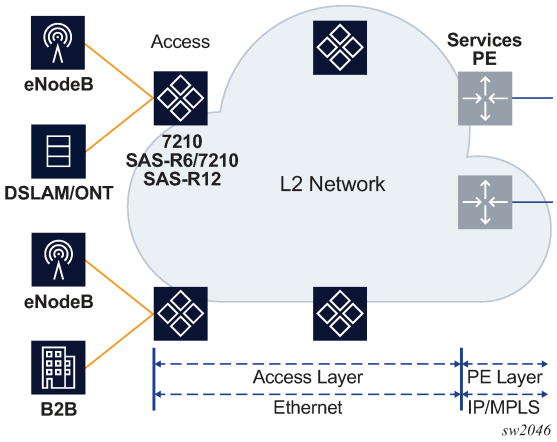
Eth-rings use one VID per control per ring instance and use one (typically) or multiple VIDs for data instances per control instance. A dedicated control VLAN (ERP VLAN) is used to run the protocol on the control VID. G.8032 controls the active state for the data VLANs (ring data instances) associated with a control instance. Multiple control instances allow logically separate rings on the same topology. The Nokia implementation supports dot1q, and QinQ encapsulation for data ring instances. The control channel supports dot1q and QinQ encapsulation.

2.3.5 SAP and service scaling with high SAP scale mode

In Layer 2 access networks that are used to backhaul service traffic from business services, mobile backhaul, and residential services, the 7210 SAS-R6 and 7210 SAS-R12 act as a Layer 2 carrier Ethernet switching platform with VLAN-based Layer 2 uplinks. To perform this role, the 7210 SAS-R6 and 7210 SAS-R12 must support a mode with higher SAP and service scaling. To do so, the 7210 SAS-R6 and 7210 SAS-R12 use the SAP scale mode and port-based access ingress policies.

The following figure shows the use of Layer 2 uplinks in a Layer 2 access network.

Figure 5: Using Layer 2 uplinks in a Layer 2 network



The SAP scale mode is configured using the **configure>system>global-res-profile>sap-scale-mode** {**high** | **low**} command. By default, the **low** option is configured for low SAP scale mode, which provides backward compatibility. The user can configure the **high** option to use high SAP scale mode, which allows the configuration of a higher number of services and SAPs. Before changing the **sap-scale-mode** value, the user must perform the following tasks:

- Remove all service and SAP configurations.
- Change the value of **sap-scale-mode** and enable per-port egress queuing using the **configure>system>global-res-profile>qos>port-scheduler-mode** command.
- Reboot the node.
- Reconfigure all SAPs and services as required.

In high SAP scale mode, the system supports higher SAP and service scaling for Epipe/VLL and VPLS services only. SAP and service scaling for IES, VPRN, and R-VPLS services remain unchanged.

QoS policies support port-based access ingress policies on access ports to facilitate the use of access ports as Layer 2 uplinks. With the use of ports as Layer 2 uplinks, the user can apply a single port-based access ingress policy at ingress of an access port, instead of using per-SAP ingress policies. This allows a single policy definition to be used to classify and rate-limit all traffic received over access ports used as Layer 2 uplinks (similar to a network port-based policy applied to network ports used as uplinks) instead of using per SAP ingress policies. Resources must be allocated using the **configure>system>resource-profile** command to use access ingress QoS policies on an access port.

In addition, only the following QoS policies can be used in the high SAP scale mode to achieve a higher scale:

- access port-based egress queuing and shaping on all ports, including service delivery ports and uplinks
- access port-based ingress classification and policing on uplinks
- Epipe and VPLS SAPs using access port ingress QoS policies (instead of per-SAP ingress policies) on service delivery ports for higher SAP scale
- IES and VPRN SAPs using table-based classification or CAM-based classification
- R-VPLS SAPs using CAM-based classification and policing

The following SAP configuration restrictions apply to the high SAP scale mode; see SAPs for additional SAP configuration guidelines:

- If an R-VPLS Q1.* SAP is configured, SAPs (Q1.Q2 SAP) with a matching Q1 tag cannot be configured in other VPLS, Epipe, IES, and VPRN services on the same port.
- If a VPLS Q1.* SAP enabled with DHCP snooping is configured, SAPs (Q1.Q2 SAP) with a matching Q1 tag cannot be configured in other VPLS, Epipe, IES, and VPRN services on the same port. They can use other values for the Q1 tag. The reverse is also true.
- The dot1p default SAP cannot be configured in R-VPLS services; it is only supported in Epipe, VPLS, IES, and VPRN services.

2.3.5.1 Guidelines for configuring high SAP scale mode

About this task

Perform the following steps to change the **sap-scale-mode low** to the **sap-scale-mode high** configuration:

Procedure

Step 1. Delete all SAPs.

Step 2. Configure the **config>system>global-res-profile>qos>port-scheduler-mode** command.

Step 3. Configure the **sap-scale-mode** command to use the **high** option.

Step 4. Save the configuration and reboot the node.

2.3.5.2 Guidelines for configuring low SAP scale mode

About this task

Perform the following steps to change the **sap-scale-mode high** to the **sap-scale-mode low** configuration:

Procedure

Step 1. Delete all SAPs.

Step 2. If the access ingress QoS policy has attachments, reset the policy.

Step 3. If the **access-ingress-qos-mode** command is set to **port-mode**, configure the command to use the **sap-mode** option.

Step 4. Configure the **sap-scale-mode** command to use the **low** option.

Step 5. Save the configuration and reboot the node.

2.3.6 Overview of G.8032 operation

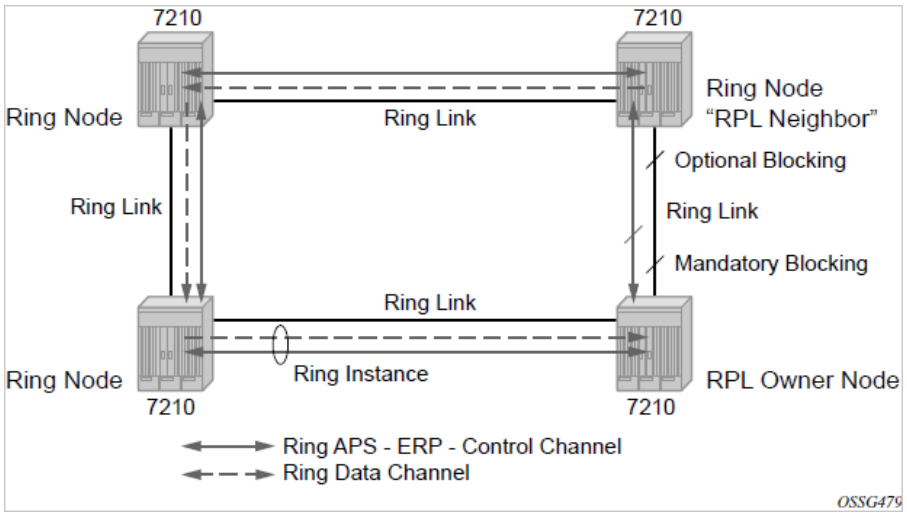
R-APS messages that carry the G.8032 protocol are sent on a dedicated protocol VLAN called ERP VLAN (or ring control instance). In a revertive case, G.8032 protocol ensures that one Ring Protection Link (RPL) owner blocks the RPL link. R-APS messages are periodically sent around in both directions to inform other nodes in the ring about the blocked port in the RPL owner node. In non-revertive mode, any link may be the RPL link.Y.1731 Ethernet OAM CC is the basis of the R-APS messages.

Y.1731 CC messages are typically used by nodes in the ring to monitor the health of each link in the ring in both directions. However, CC messages are not mandatory. Other link layer mechanisms could be considered; for example, LOS (Loss of Signal) when the nodes are directly connected.

Initially, each Ring Node blocks one of its links and notifies other nodes in the ring about the blocked link. When a ring node in the ring learns that another link is blocked, the node unblocks its blocked link, possibly causing FDB flush in all links of the ring for the affected service VLANs, controlled by the ring control instance. This procedure results in unblocking all links except the one link and the ring normal (or idle) state is reached.

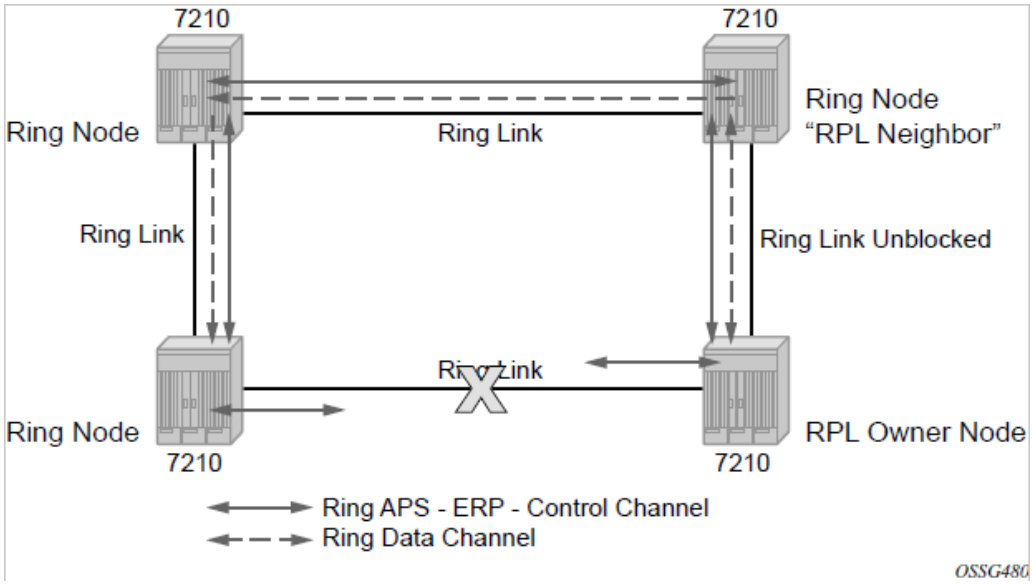
In revertive mode, the RPL link is the link that is blocked when all links are operable after the revert time. In non-revertive mode, the RPL link is no different from other ring links. Revertive mode provides predictability, particularly when there are multiple ring instances, and the operator can control which links are blocked on the different instances. Each time that there is a topology change that affects Reachability, the nodes may flush the FDB and MAC learning takes place for the affected service VLANs, allowing forwarding of packets to continue. The following figure shows this initial operational state.

Figure 6: G.8032 ring in the initial state



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

Figure 7: 0 to 1 G.8032 ring in the protecting state



When the failed link recovers, the nodes that blocked the link again send the R-APS messages indicating no failure this time. This causes the RPL owner to block the RPL link and indicate the blocked RPL link to the ring in R-APS message, when received by the nodes at the recovered link, they unblock that link and restore connectivity (again all nodes in the ring perform an FDB flush and MAC learning takes place). The ring is back in the normal (or idle) state.

Within each path, Y.1731 Maintenance Entity Group (MEG) Endpoints (MEPs) are used to exchange R-APS specific information (specifically to coordinate switchovers) as well as optionally fast Continuity Check Messages (CCMs), providing an inherent failure detection mechanism as part of the protocol. Failure detection of a ring path by one of the mechanisms activates the protection links. Upon failure, reconvergence times are dependent on the failure detection mechanisms.

In the case of Y.1731, the CCM transmit interval determines the response time. The 7210 SAS device supports 100 ms message timers that allow for quicker restoration times. Alternatively, 802.3ah (Ethernet in the First Mile) or LOS can trigger a protection switch where appropriate. In the case of direct connectivity between the nodes, there is no need to use Ethernet CC messaging for liveliness detection.

Revertive and non-revertive behaviors are supported. The RPL is configured and Eth-rings can be configured to revert to the RPL upon recovery.

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

There is no limit on the number of control channels on a port.

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

In the 7210 SAS implementation, the Ethernet ring is built from a VPLS service on each node with VPLS SAPs that provides ring path with SAPs. As a result, most of the VPLS SAP features are available on Ethernet rings, if needed. This results in a fairly feature-rich ring service.

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

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

Flushing is triggered by the G.8032 state machine and the 7210 SAS implementation allows flooding of traffic during the flushing interval to expedite traffic recovery.

2.3.7 Ethernet ring sub-rings

Ethernet sub-rings offer a dual redundant way to interconnect rings. The 7210 SAS supports sub-rings connected to major rings, and a sub-ring connected to a VPLS (LDP based) for access ring support in VPLS networks. Figure 8: Major ring and sub-ring scenario shows a major ring and sub-ring scenario, and Figure 9: 0 to 4 G.8032 sub-ring shows a G.8032 sub-ring. In this scenario, any link can fail in either ring (ERP1 or ERP2) and each ring is protected. Also, the sub-ring (ERP2) relies on the major ring (ERP1) as

part of its protection for the traffic from C and D. The nodes C and D are configured as interconnection nodes.

Figure 8: Major ring and sub-ring scenario

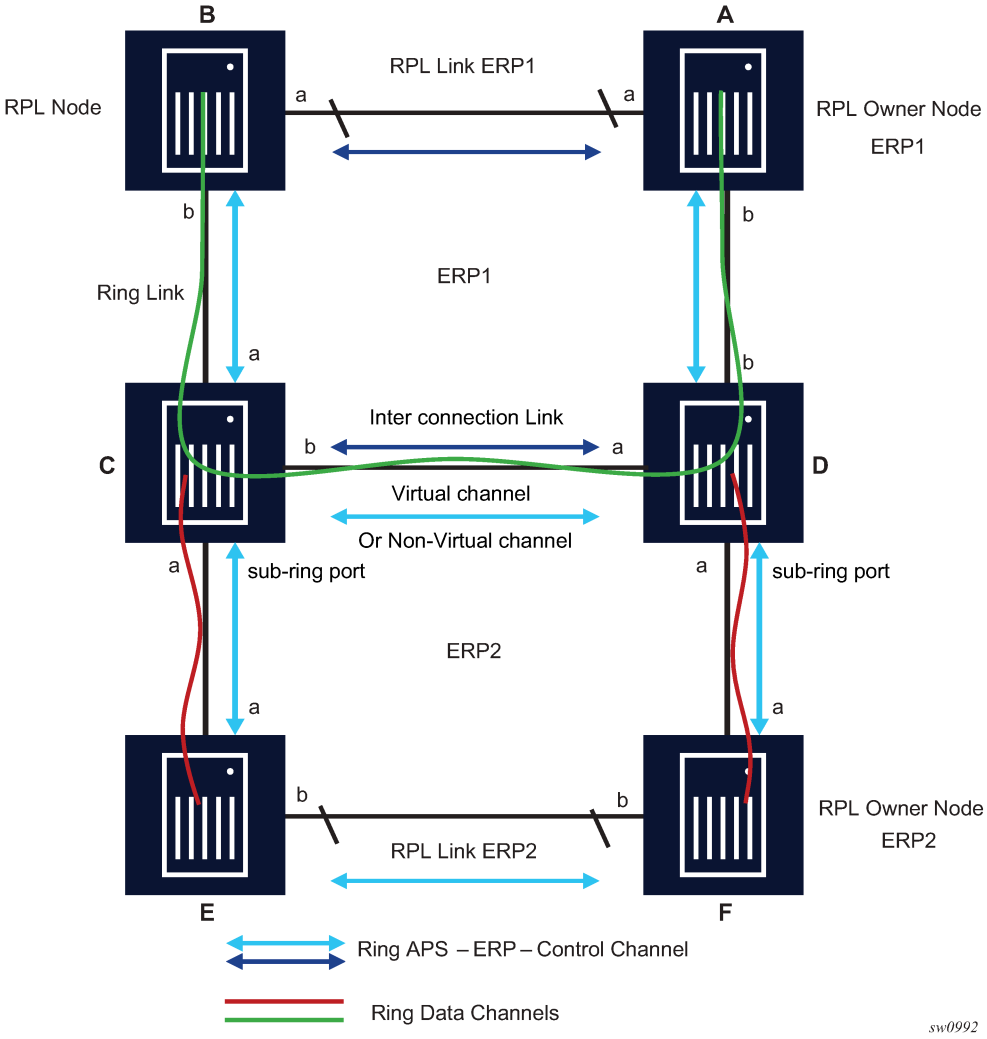
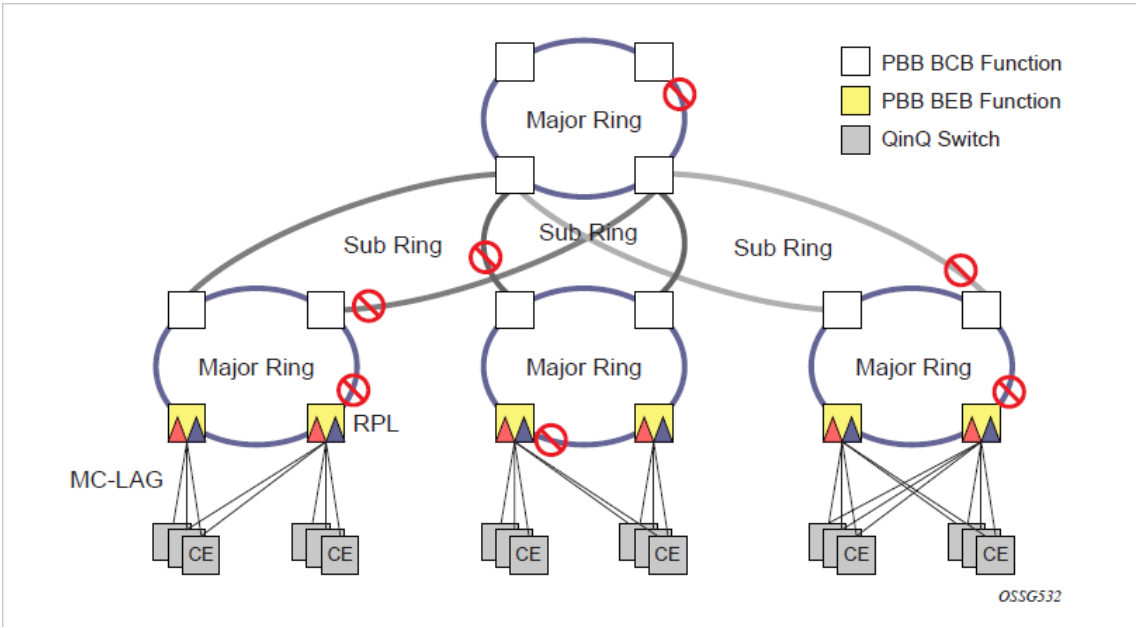


Figure 9: 0 to 4 G.8032 sub-ring



Sub-rings and major rings run similar state machines for the ring logic; however, there are some differences. When sub-rings protect a link, the flush messages are propagated to the major ring. (A special configuration allows control of this option on the 7210 SAS.) When major rings change topology, the flush is propagated around the major ring and does not continue to any sub-rings. The reason for this is that major rings are completely connected but sub-rings are dependent on another ring or network for full connectivity. The topology changes need to be propagated to the other ring or network usually. Sub-rings offer the same capabilities as major rings in terms of control and data so that all link resources may be used.

2.3.7.1 Virtual and non-virtual channel

The following example shows a sub-ring using virtual-link configuration output on Node C, interconnecting node.

Example: Sub-ring using virtual-link configuration output on Node C, interconnecting node

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

```
            no shutdown
        exit
        no shutdown
  exit
```

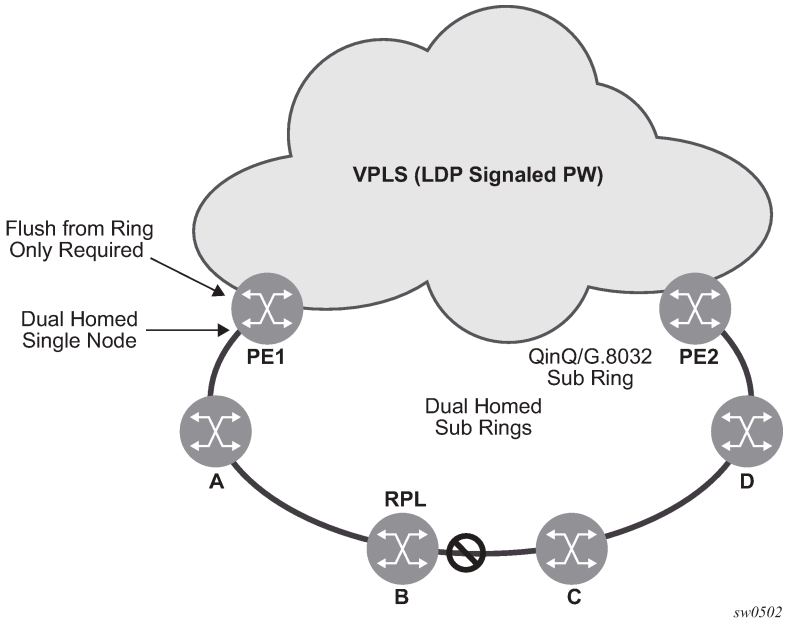
```
sub-ring non-virtual-link // Not using a virtual link

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



# Data configuration for the Sub-Ring

  vpls 11 customer 1 create
      description "Data on VID 11 for Ring 1"
      stp shutdown
      sap 1/1/1:11 eth-ring 1 create // VID 11 used for ring
          stp shutdown
      exit
      sap 1/1/4:11 eth-ring 1 create
          stp shutdown
      exit
      sap 1/1/3:11 eth-ring 2 create // Sub-ring data
          stp shutdown
      exit
      sap 3/2/1:1 create
      description "Local Data SAP"
          stp shutdown
      no shutdown
  exit

# Control Channel for the Sub-Ring using a virtual link. This is
# a data channel as far as Ring 1 configuration. Other Ring 1
# nodes also need this VID to be configured.

  vpls 100 customer 1 create
      description "Control VID 100 for Ring 2 Interconnection"
      split-horizon-group "s1" create //Ring Split horizon Group
      exit
      stp shutdown
      sap 1/1/1:100 split-horizon-group "s1" eth-ring 1 create
          stp shutdown
      exit
      sap 1/1/4:100 split-horizon-group "s1" eth-ring 1 create
          stp shutdown
      exit
      sap 1/1/3:100 eth-ring 2 create
          stp shutdown
      exit
      no shutdown
  exit
```

Example

2.3.7.2 Ethernet ring sub-ring using non-virtual link

The following figure shows 0 to 6 homed to VPLS.

Figure 10: 0 to 6 sub-ring homed to VPLS



Example: Sub-ring using non-virtual link configuration output on PE1, interconnecting node

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

Example: Sub-ring nodes configured with sub-ring non-virtual link option within non-virtual link sub-ring

All the sub ring nodes part of a sub-ring with non-virtual link should be configured with the "sub-ring non-virtual-link" option.

```
eth-ring 1
        sub-ring non-virtual-link
        exit
        path a 1/1/1 raps-tag 1.1
            eth-cfm
                mep 5 domain 1 association 4
                    ccm-enable
                    control-mep
                    no shutdown
                exit
            exit
            no shutdown
        exit
        path b 1/1/2 raps-tag 1.1
            eth-cfm
                mep 6 domain 1 association 3
                    ccm-enable
                    control-mep
                    no shutdown
                exit
            exit
            no shutdown
        exit
        no shutdown
    exit
# Control Channel for Sub-Ring using non-virtual-link on interconnecting node:
vpls 1 customer 1 create
      description "Ring 1 Control termination"
      stp shutdown
      sap 1/1/3:1.1 eth-ring 1 create //path a control
          stp shutdown
      exit
      no shutdown
  exit
# Configuration for the ring data into the VPLS Service

  vpls 5 customer 1 create
      description "VPLS Service at PE1"
      stp
          no shutdown
      exit
      sap 1/1/3:2.2 eth-ring 1 create
          stp shutdown
      exit
      sap 1/1/5:1 create
      exit
      mesh-sdp 5001:5 create //sample LDP MPLS LSPs
      exit
      mesh-sdp 5005:5 create
      exit
      mesh-sdp 5006:5 create
      exit

      no shutdown
  exit
# Control Channel for Sub-Ring using non-virtual-link on sub-Ring nodes:
vpls 1 customer 1 create
```

```
            stp
                shutdown
            exit
            sap 1/1/1:1.1 eth-ring 1 create
                stp
                    shutdown
                exit
            exit
            sap 1/1/2:1.1 eth-ring 1 create
                stp
                    shutdown
                exit
            exit
            no shutdown
        exit
```

Example: Sample sub-ring using non-virtual link configuration output homed to a major ring

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

2.3.8 Support for hardware-based 100ms CCM timers for G.8032 MEPs

On the 7210 SAS-R6 and 7210 SAS-R12, the user must reserve a VLAN-ID for use with only G.8032 MEPs which uses the hardware for CCM processing. No data services or control SAPs can use this VLAN-ID. The CLI command description used to reserve the VLAN-ID is available in the *7210 SAS-Mxp, R6, R12, S, Sx, T Interface Configuration Guide*.

When using hardware CCMs, a limited amount of control instances is supported per port. Multiple data services/instances can be associated with each of these control instances.

Example: Configuration output with control-sap-tag command

The following example shows configuration output with the **control-sap-tag** command.

```
Configure eth-ring 1
```

```
        description "Ethernet Ring 1"
        guard-time 20
        revert-time 60
        rpl-node owner
        path a 1/1/8 raps-tag 1
            description "Ethernet Ring : 1 Path : pathA"
            rpl-end
            eth-cfm
                mep 1 domain 1 association 1
                    ccm-enable
                    control-mep
                    control-sap-tag 513
                    no shutdown
                exit
            exit
            no shutdown
        exit
        path b 1/1/7 raps-tag 1
            description "Ethernet Ring : 1 Path : pathB"
            eth-cfm
                mep 2 domain 1 association 2
                    ccm-enable
                    control-mep
                    control-sap-tag 513
                    no shutdown
                exit
            exit
            no shutdown
        exit
        no shutdown
exit
```

2.3.8.1 Configuration guidelines for 7210 SAS-R6 and 7210 SAS-R12

The user needs to reserve VLANs using the system resource-profile **g8032-control-sap-tags** command. A maximum of up to 4 VLANs need to be reserved per line card. These VLANs are used to internally identify G.8032 CCM messages and R-APS messages. These VLANs cannot be used on any of the ports of the IMM, that is, SAPs cannot be configured with VLAN tag value matching any of the configured VLAN tags using this command.

2.3.8.2 LAG support

The 7210 SAS does not support G.8032 Ethernet rings on LAGs.

2.3.9 OAM considerations

Ethernet CFM can be enabled on each individual path under an Ethernet ring. Only Down MEPs can be configured on each of them and CCM sessions can be enabled to monitor the liveliness of the path using an interval of 100 ms. Different CCM intervals can be supported on path A and path B in an Ethernet ring. CFM is optional if hardware supports LOS, for example.

Service Down MEPs cannot be configured on the same port as the G.8032 ring ports.

2.3.10 QoS considerations

When Ethernet ring is configured on two ports located on different IOMs, the SAP queues and virtual schedulers are created with the actual parameters on each IOM.

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

More information about the Ethernet ring applicability in the services solution, see the respective Layer 2 sections of the *7210 SAS-R6, R12 Services Guide*.

2.3.11 Support service and solution combinations

Ethernet rings are a supported Layer 2 service. The following considerations apply:

- Only ports in access mode can be configured as eth-ring paths.
- Dot1q and QinQ ports are supported as eth-ring path members.
- A mix of regular and multiple eth-ring SAPs and PWs can be configured in the same services.

2.3.12 Configuration guidelines for G.8032

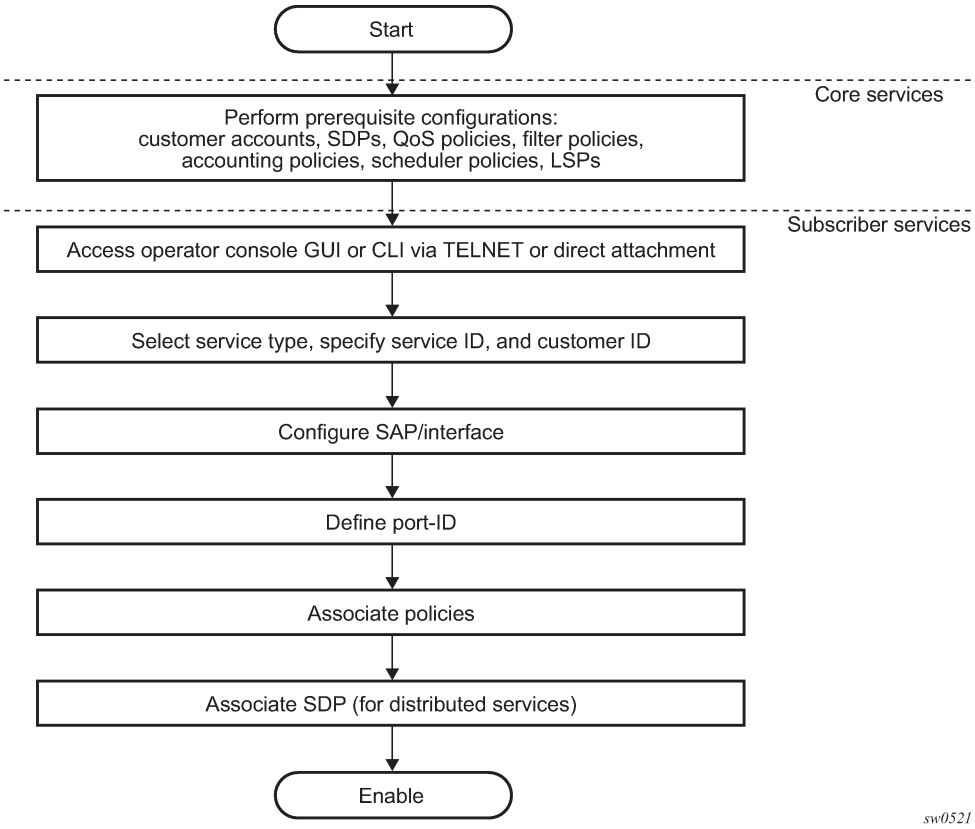
The following are the configuration guidelines for G.8032:

- Service level MEPs are not available on all SAPs tied to an Eth-ring instance on a port.
- On 7210 SAS-R6 and 7210 SAS-R12 with IMMv2 (that is, IMM-sas-r-b), to improve the service failover time because of failures in the ring path, fast flood is enabled by default only for VPLS services (and not for R-VPLS services). On a failure detection in one of the paths of the eth-ring, along with MAC flush the system starts to flood the traffic onto the available path. No explicit user configuration is needed for this and it does not need resources to be allocated from the ingress internal TCAM pool. When G8032 is enabled for R-VPLS services to enable fast-flood, user needs to explicitly assign resources from the 'sf-ingress-internal-tcam' pool using the global system resource profile commands.
- G.8032 instances cannot be configured over a LAG.
- On 7210 SAS-R6 and 7210 SAS-R12, user can enable G.8032 fast-flood by allocating resources to this feature using the command **configure>system>global-system-profile>sf-ingress-internal-tcam>g8032-fast-flood**.

2.4 Service creation process overview

The following figure shows the overall process to provision core and subscriber services.

Figure 11: Service creation and implementation flow



2.5 Deploying and provisioning services

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

- core network construction
- service administration
- service provisioning

2.5.1 Phase 1: core network construction

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

- Build the IP or IP/MPLS core network.
- Configure routing protocols.
- Configure MPLS LSPs (if MPLS is used).

2.5.2 Phase 2: service administration

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

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

2.5.3 Phase 3: service provisioning

For service provisioning, the following tasks should be completed:

- Provision customer account information.
- If necessary, build any customer-specific QoS, filter, or accounting policies.
- Provision the customer services on the service edge routers by defining SAPs, and binding policies to the SAPs.

2.6 Configuration notes

This section describes service configuration restrictions.

2.6.1 General

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

Core tasks include the following:

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

Subscriber services tasks include the following:

- Create Epipe and VPLS services.
- Create a VPRN service (supported only when operating in network mode).
- Bind SDPs.
- Configure interfaces (where required) and SAPs.
- Create exclusive QoS and filter policies.

2.7 Configuring global service entities with CLI

This section provides information to create subscriber (customer) accounts using the command line interface.

2.7.1 Service model entities

The Nokia service model uses logical entities to construct a service. The service model contains four main entities to configure a service.

2.8 Basic configuration

The most basic service configuration must have the following:

- customer ID
- service type
- service ID
- SAP identifying a port and encapsulation value
- associated SDP for distributed services in the network mode

Example: Epipe service configuration output showing SDP and Epipe service entities

The following is a sample Epipe service configuration output showing the SDP and Epipe service entities. SDP ID 1 was created with the far-end node 10.20.1.2. Epipe ID 101 was created for customer ID 1, which uses the SDP ID 1.

```
A:ALA-7210>config>service#
------------------------------------------
...
        sdp 1 mpls create
            description "Default sdp description"
            far-end 10.20.1.2
            lsp "lsp_1_to_B"
            signaling tldp
            no vlan-vc-etype
            path-mtu 9194
            no adv-mtu-override
            keep-alive
                shutdown
                hello-time 10
                hold-down-time 10
                max-drop-count 3
                timeout 5
                no message-length
            exit
            no collect-stats
            no accounting-policy
            no shutdown
        exit
...
    epipe 101 customer 1 vpn 101 create
            description "Default epipe description for service id 101"
            service-mtu 9194
            sap lag-2:101 create
                description "Default sap description for service id 101"
                no tod-suite
                dot1ag
                exit
                ingress
                    qos 1
```

```
                    no filter
                exit
            spoke-sdp 101:101 vc-type ether create
                no vlan-vc-tag
                ingress
                    no vc-label
                exit
                egress
                    no vc-label
                exit
                no control-word
                no
                dot1ag
                    mep 1 domain 5 association 101 direction down
                        ccm-enable
                        no ccm-ltm-priority
                        low-priority-defect remErrXcon
                        no mac-address
                        no shutdown
                    exit
                    mep 1 domain 6 association 101 direction down
                        ccm-enable
                        no ccm-ltm-priority
                        low-priority-defect remErrXcon
                        no mac-address
                        no shutdown
                    exit
                exit
                no collect-stats
                no accounting-policy
                no precedence
                no shutdown
            exit
            no shutdown
...
----------------------------------------
A:ALA-7210>config>service#
```

2.9 Common configuration tasks

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

2.9.1 Configuring customer accounts

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

- description
- contact name
- telephone number

2.9.1.1 Customer information

Use the following syntax to create and input customer information.

```
config>service# customer customer-id create
    contact contact-information
    description description-string
    phone phone-number
```

Example: Basic customer account configuration output

```
A:ALA-12>config>service# info
----------------------------------------
...
       customer 5 create
           description "Nokia Customer"
           contact "Technical Support"
           phone "650 555-5100"
       exit
...
----------------------------------------
A:A:ALA-12>config>service#
```

2.9.2 Configuring an SDP

The most basic SDP must have the following:

- locally unique SDP identification (ID) number
- system IP address of the far-end routers
- SDP encapsulation type, MPLS

2.9.2.1 SDP configuration tasks

About this task

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

Consider the following SDP characteristics:

- SDPs can be created as MPLS.
- Each distributed service must have an SDP defined for every remote router to provide VLL, VPLS, and VPRN services.
- A distributed service must be bound to an SDP. By default, no SDP is associated with a service. When an SDP is created, services can be associated with that SDP.
- An SDP is not specific or exclusive to any one service or any type of service. An SDP can have more than one service bound to it.
- The SDP IP address must be a 7210 SAS-series system IP address.
- To configure an MPLS SDP, LSPs must be configured first, then the LSP-to-SDP association must be explicitly created.

- In the SDP configuration, automatic ingress and egress labeling (targeted LDP) is enabled by default. Ingress and egress VC labels are signaled over a TLDP connection between two 7210 SAS-series routers.

  If signaling is disabled for an SDP, services using that SDP must configure ingress and egress VC labels manually.

Procedure

To configure a basic SDP, perform the following steps:

Step 1. Specify an originating node.

Step 2. Create an SDP ID.

Step 3. Specify an encapsulation type.

Step 4. Specify a far-end node.

2.9.2.2 Configuring an SDP

Use the following syntax to create an SDP and select an encapsulation type. Only MPLS encapsulation is supported.

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

When specifying MPLS SDP parameters, you must specify an LSP. If an LSP name is specified, RSVP is used for dynamic signaling within the LSP.

LSPs are configured in the **config>router>mpls** context. See the *7210 SAS-Mxp, R6, R12, S, Sx, T MPLS Guide* for configuration and command information.

Use the following syntax to create an MPLS SDP.

```
config>service>sdp sdp-id [mpls] create
    adv-mtu-override
    description description-string
    far-end ip-address
    keep-alive
    hello-time seconds
    hold-down-time seconds
    max-drop-count count
    message-length octets
    timeout timeout
    no shutdown
```

```
            lsp lsp-name [lsp-name]    (only for MPLS SDPs)
    path-mtu octets
    signaling {off | tldp}
    no shutdown
```

Example: LSP-signaled MPLS SDP configuration output

The following example shows LSP-signaled MPLS SDP configuration output.

```
A:ALA-12>config>service# info
----------------------------------------
...
        sdp 8 mpls create
            description "MPLS-10.10.10.104"
            far-end 10.10.10.104
            lsp "to-104"
            keep-alive
            mixed-lsp-mode
                revert-time 1
                shutdown
            exit
            no shutdown
        exit
...
----------------------------------------
A:ALA-12>config>service#
```

2.9.2.3 Configuring a mixed-LSP SDP

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

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

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

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

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

config>service>sdp mpls>mixed-lsp-mode>revert-time *revert-time*

An *infinite* value for the timer dictates that the SDP must never revert to another higher priority LSP type unless the currently active LSP type is down:

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

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

2.10 Ethernet Connectivity Fault Management

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

The configuration is split into multiple CLI contexts. The base ETH-CFM configuration defines the different management constructs and administrative elements. This configuration is performed in the **eth-cfm**

context. The individual management points are configured within the specific service contexts in which they are applied (port, SAP, and so on).

See the *7210 SAS-R6, R12 Services Guide* for detailed information about the basic service-applicable material to build the service-specific management points, MEPs, and MIPs. The different service types support a subset of the features from the complete ETH-CFM suite.

ETH-CC used for continuity is available to all MEPs configured within a service. The 7210 SAS devices support Down MEPs and Up MEPs, though the support is not available on all platforms. See the *7210 SAS-Mxp, R6, R12, S, Sx, T OAM and Diagnostics Guide* for more information about platform support.

The troubleshooting tools ETH-LBM, ETH-LBR, LTM ETH-TST, and LTR ETH-TST, defined by the IEEE 802.1ag specification and the ITU-T Y.1731 recommendation, are applicable to all MEPs (and MIPs where appropriate). The advanced notification function, Alarm Indication Signal (AIS), defined by the ITU-T Y.1731, is supported on Epipe services.

The advanced performance functions, 1DM, DMM/DMR, and SLM/SLR, are supported on all service MEPs.

See the *7210 SAS-Mxp, R6, R12, S, Sx, T OAM and Diagnostics Guide* for more information about the individual features and functions that are supported and configuration guidelines applicable to CFM entities on the 7210 SAS.

The following table lists ETH-CFM acronym expansions.

Table 7: ETH-CFM acronym expansions

Acronym	Expansion
1DM	One-way Delay Measurement (Y.1731)
AIS	Alarm Indication Signal
BNM	Bandwidth Notification Message (Y.1731 sub OpCode of GMN)
CCM	Continuity Check Message
CFM	Connectivity Fault Management
DMM	Delay Measurement Message (Y.1731)
DMR	Delay Measurement Reply (Y.1731)
GMN	Generic Message Notification
LBM	Loopback Message
LBR	Loopback Reply
LTM	Linktrace Message
LTR	Linktrace Reply
ME	Maintenance Entity

Acronym	Expansion
MA	Maintenance Association
MA-ID	Maintenance Association Identifier
MD	Maintenance Domain
MEP	Maintenance Association Endpoint
MEP-ID	Maintenance Association Endpoint Identifier
MHF	MIP Half Function
MIP	Maintenance Domain Intermediate Point
OpCode	Operational Code
RDI	Remote Defect Indication
TST	Ethernet Test (Y.1731)
SLM	Synthetic Loss Message (Y.1731)
SLR	Synthetic Loss Reply (Y.1731)

ETH-CFM capabilities may be deployed in many different Ethernet service architectures. The Ethernet-based SAPs and SDP bindings provide the endpoint on which the management points may be created. The basic functions can be used in different services, VPLS and Epipe. The following figures show two possible example scenarios for ETH-CFM deployment in Ethernet access and aggregation networks.

Figure 12: Ethernet OAM model for Ethernet access - business

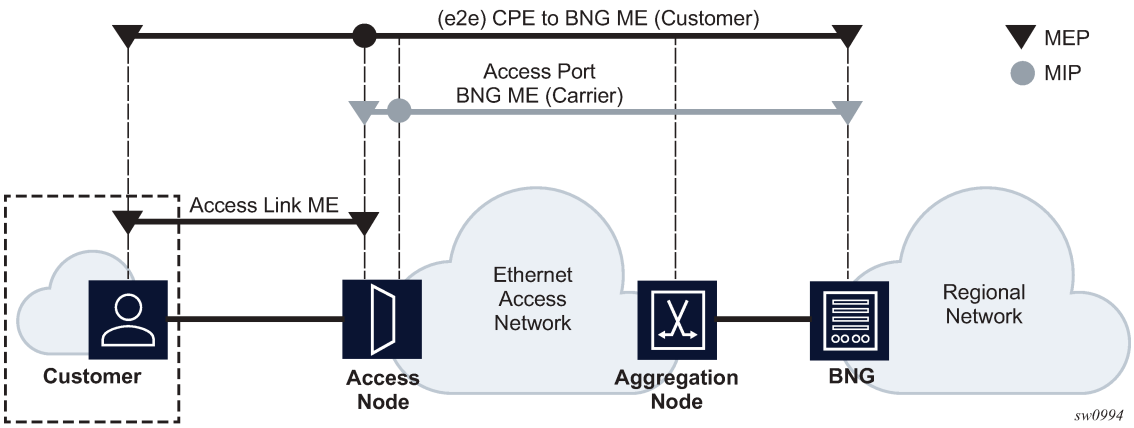
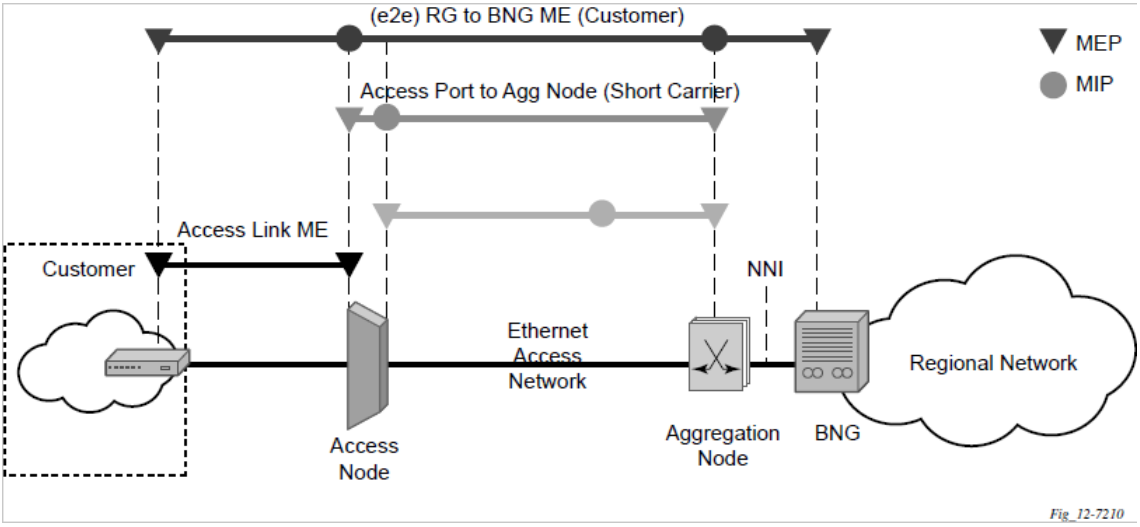


Figure 13: Ethernet OAM model for Ethernet access – wholesale



The following functions are supported:

- CFM can be enabled or disabled on a SAP or SDP bindings basis.
- The eight ETH-CFM levels are suggested to be broken up numerically between customer 7 to 5, service provider 4 to 3 and operator 2 to 1. Level 0 typically is meant to monitor direct connections without any MIPs and should be reserved for port-based G8032 MEPs. These can be configured, deleted or modified.
- Down MEP and Up MEP with an MEP-ID on a SAP/SDP binding for each MD level can be configured, modified, or deleted. Each MEP is uniquely identified by the MA-ID, MEP-ID tuple.
  - MEP creation on a SAP is only allowed for Ethernet ports (with null, q-tags, QinQ encapsulations).
  - MEP support in different services and the endpoints configured in the services (SAPs, SDPs, IP interfaces, and so on) varies across services and 7210 platforms. See the *7210 SAS-Mxp, R6, R12, S, Sx, T OAM and Diagnostics Guide* for more information about MEP support on 7210 SAS platforms.
- MIP creation on a SAP for each MD level can be enabled and disabled. MIP creation is automatic or manual when it is enabled. When MIP creation is disabled for an MD level, the existing MIP is removed. The 7210 SAS platforms have the notion of ingress and egress MIPs. Ingress MIP responds to OAM messages that are received. Egress MIP responds to OAM messages that are sent. Ingress and egress MIP support for SAP, SDP bindings and services varies and is listed in the following table. See the *7210 SAS-Mxp, R6, R12, S, Sx, T OAM and Diagnostics Guide* for more information about MEP support on 7210 SAS platforms.

2.10.1 Common actionable failures

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

Table 8: Defect conditions and priority settings

Defect	Low priority defect	Description	Causes	Priority
DefNone	N/A	No faults in the association	Normal operations	N/A
DefRDICCM	allDef	Remote Defect Indication	Feedback mechanism to inform that unidirectional faults exist. It provides the feedback loop to the node with the unidirectional failure conditions.	1
DefMACStatus (default)	macRemErr Xcon	MAC Layer	Remote MEP is indicating that a remote port or interface is not operational.	2
DefRemoteCCM	remErrXon	No communication from remote peer	MEP is not receiving CCM from a configured peer. The timeout of CCM occurs at 3.5 times the local CC interval. As per the specification, this value is not configurable.	3
DefErrorCCM	errXcon	Remote and local configurations do not match required parameters	Caused by different interval timer, domain-level issues (lower value arriving at a MEP configured with a higher value), MEP receiving CCM with its MEPID	4
DefXconn	Xcon	Cross Connected Service	The service is receiving CCM packets from a different association. This could indicate that two services have merged or there is a configuration error on one of the SAPs or bindings of the service, incorrect association identification.	5

2.10.2 MEP and MIP support

See the *7210 SAS-Mxp, R6, R12, S, Sx, T OAM and Diagnostics Guide* for more information about ETH-CFM support for different services and endpoints.

2.10.3 Configuring ETH-CFM parameters

Note:
See the *7210 SAS-Mxp, R6, R12, S, Sx, T OAM and Diagnostics Guide* for more information about ETH-CFM configuration guidelines for 7210 SAS platforms.

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

This section provides a sample of the global ETH-CFM configuration, which defines the domains, associations, linkage of the service ID or function, and the globally applicable CCM parameters, including the interval and building of the remote MEPs database.

Example: ETH-CFM configuration output

The following example shows ETH-CFM configuration output.

```
*A:ALU-7_A>config>eth-cfm# info
----------------------------------------------
        domain 1 name "1" level 1
            association 2 name "1345"
                bridge-identifier 100
                exit
                ccm-interval 60
                remote-mepid 2
                remote-mepid 3
            exit
        exit
----------------------------------------------
*A:ALU-7_A>config>eth-cfm#
```

Example: MEP and service-specific ETH-CFM parameters configured on a SAP

Defining the MEP and configuring service-specific ETH-CFM parameters is performed within the service on the specific SAP or SDP binding. The following example shows service VPLS 100 showing this configuration output on the SAP.

```
#*A:ALU-7_A>config>service# info
----------------------------------------------
vpls 100 customer 1 create
description "VPLS service 100 - Used for MEP configuration example"
sap 2/2/1:20 create
description "2/2/1:20"
eth-cfm
mep 1 domain 1 association 1 direction down
no shutdown
exit
exit
exit
exit
no shutdown
exit
customer 1 create
description "Default customer"
exit
exit
----------------------------------------------
*A:ALU-7_A>config>service#
```

All of the preceding examples were based on IEEE 802.1ag. They are not capable of running Y.1731 functions. To build a Y.1731 context, the domain format must be none.

Example: Global ETH-CFM configuration outputs and advanced Y.1731 functions

The following example shows global ETH-CFM configuration outputs and the advanced Y.1731 functions that can be configured. The configuration rejects the configuration of Y.1731 functions within an IEEE 802.1ag context.

```
*A:7210-2# config>eth-cfm# info
----------------------------------------------
        domain 1 format none level 1
            association 1 format icc-based name "1234567890123"
                bridge-identifier 100
                exit
                ccm-interval 1
            exit
        exit


*A:7210-2# config>service# info
----------------------------------------------
        vpls 100 customer 1 create
            stp
                shutdown
            exit
            sap 2/2/1:40 create
                eth-cfm
                    mep 1 domain 1 association 1 direction up
                        ais-enable
                            priority 2
                            interval 60
                        exit
                        eth-test-enable
                            test-pattern all-ones crc-enable
                        exit
                        no shutdown
                    exit
                exit
            exit
            no shutdown
        exit
----------------------------------------------
```

Note:

- To be able to transmit and also receive AIS PDUs, a Y.1731 MEP must have **ais-enable** set.
- To be able to transmit and also receive ETH-Test PDUs, a Y.1731 MEP must have **eth-test-enable** set.

2.10.4 Applying ETH-CFM parameters

Use the following syntax to apply ETH-CFM parameters to the following entities.

```
config>service>epipe>sap
    eth-cfm
    mep mep-id domain md-index association ma-index [direction
    {up | down}]
```

```
            ais-enable
                client-meg-level [[level [level ...]]
                interval {1 | 60}
                priority priority-value
            ccm-enable
            ccm-ltm-priority priority
            eth-test-enable
                test-pattern {all-zeros | all-ones} [crc-enable]
            low-priority-defect {allDef | macRemErrXcon | remErrXcon | errXcon | xcon | noXcon}
            [no] shutdown
```

```
config>service>epipe>spoke-sdp
    eth-cfm
    mep mep-id domain md-index association ma-index [direction
    {up | down}]
        ccm-enable
        ccm-ltm-priority priority
        eth-test-enable
            test-pattern {all-zeros | all-ones} [crc-enable]
        low-priority-defect {allDef | macRemErrXcon | remErrXcon | errXcon | xcon | noXcon}
        [no] shutdown
```

```
config>service>vpls>sap
    eth-cfm
    mip
    mep mep-id domain md-index association ma-index [direction {up | down}]
    no mep mep-id domain md-index association ma-index
        ccm-enable
        ccm-ltm-priority priority
        eth-test-enable
            test-pattern {all-zeros | all-ones} [crc-enable]
        low-priority-defect {allDef | macRemErrXcon | remErrXcon | errXcon | xcon | noXcon}
        mac-address mac-address
        [no] shutdown
```

```
config>service>vpls>mesh-sdp sdp-id[:vc-id] [vc-type {ether | vlan}]
    eth-cfm
    mep mep-id domain md-index association ma-index [direction
    {up | down}]
        ccm-enable
        ccm-ltm-priority priority
        eth-test-enable
            test-pattern {all-zeros | all-ones} [crc-enable]
        low-priority-defect {allDef | macRemErrXcon | remErrXcon | errXcon | xcon | noXcon}
        mac-address mac-address
        [no] shutdown
```

```
config>service>vpls
    spoke-sdp sdp-id:vc-id [vc-type {ether | vlan}] [split-horizon-group group-name] [no-
endpoint]
    spoke-sdp sdp-id:vc-id [vc-type {ether | vlan}] [split-horizon-group group-name]
 endpoint endpoint
    eth-cfm
    map mep-id domain md-index association ma-index [direction
    {up | down}]
        ccm-enable
        ccm-ltm-priority priority
        eth-test-enable
            test-pattern {all-zeros | all-ones} [crc-enable]
        low-priority-defect {allDef | macRemErrXcon | remErrXcon | errXcon | xcon | noXcon}
        mac-address mac-address
```

```
        [no] shutdown
```

```
oam
    eth-cfm linktrace mac-address mep mep-id domain md-index association ma-index [ttl ttl-
value]
    eth-cfm loopback mac-address mep mep-id domain md-index association ma-index [send-
count send-count] [size data-size] [priority priority]
    eth-cfm eth-test mac-address mep mep-id domain md-index association ma-index
 [priority priority] [data-length data-length]
    eth-cfm one-way-delay-test mac-address mep mep-id domain md-index association ma-index
 [priority priority]
    eth-cfm two-way-delay-test mac-address mep mep-id domain md-index association ma-index
 [priority priority]
    eth-cfm two-way-slm-test mac-address mep mep-id domain md-index association ma-index
 [priority priority]
```

2.11 Service management tasks

This section describes the service management tasks.

2.11.1 Modifying customer accounts

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

```
config>service# customer customer-id create
    [no] contact contact-information
    [no] description description-string
    [no] phone phone-number
```

Example: Modifying customer accounts

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

2.11.2 Deleting customers

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

```
config>service# no customer customer-id
```

Example: Deleting customers

```
config>service# epipe 5 customer 27 shutdown
config>service# epipe 9 customer 27 shutdown
config>service# no epipe 5
config>service# no epipe 9
```

```
config>service# no customer 27
```

2.11.3 Modifying SDPs

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

Note:
You cannot modify the SDP encapsulation type after the SDP is created.

```
config>service# sdp sdp-id
```

Example: Modifying SDPs

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

2.11.4 Deleting SDPs

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

```
config>service# no sdp 79
```

Example: Deleting SDPs

```
config>service# epipe 5 spoke-sdp 79:5
config>service>epipe>sdp# shutdown
config>service>epipe>sdp# exit
config>service>epipe# exit
config>service# no sdp 79
```

2.12 Layer 2 Control Processing

Operators providing Epipe service need to be able to transparently forward Layer 2 Control Processing (L2CP) control frames received from the customers. This allows their customers to run these control protocols between the different locations that are part of the Layer 2 VPN service. The 7210 SAS platforms provide the user with the following capability:

- An option to tunnel, discard, or peer for EFM OAM, LLDP, Dot1x, and LACP.
- BPDU translation and Layer 2 protocol tunneling support for xSTP and Cisco control protocols. This is supported only in a VPLS service. For more information, see L2PT and BPDU translation.

Note:
The CDP, VTP, DTP, PAgP, and UDLD management protocols are forwarded transparently in an Epipe service.

By default, LACP, LLDP, EFM OAM, and Dot1x L2CP untagged packets are discarded if the protocol is not enabled on the port where these frames are received. The user has an option to enable peering by enabling the protocol on the port and configuring the appropriate parameters for the protocol. The user also has an option to tunnel these packets using an Epipe or VPLS service.

In a VPLS service, the Layer 2 control frames are sent out of all the SAPs configured in the VPLS service. Nokia recommends using this feature carefully and only when a VPLS is used to emulate an end-to-end Epipe service (that is, an Epipe configured using a three-point VPLS service, with one access SAP and two access-uplink SAP/SDPs for redundant connectivity). That is, if the VPLS service is used for multipoint connectivity, Nokia does not recommend using this feature. When a Layer 2 control frame is forwarded out of a dot1q SAP or a QinQ SAP, the SAP tags of the egress SAP are added to the packet.

The following SAPs can be configured for tunneling the untagged L2CP frames (corresponding protocol tunneling needs to be enabled on the port):

- If the port encapsulation is null, the user has an option to tunnel these packets by configuring a null SAP on a port.
- If the port encapsulation is dot1q, the user has an option to use dot1q explicit null SAP (for example, 1/1/10:0) or a dot1q default SAP (for example, 1/1/11:*) to tunnel these packets.
- If the port encapsulation is QinQ, the user has an option to use 0.* SAP (for example, 1/1/10:0.*) to tunnel these packets.

In addition to the preceding list of protocols, protocols that are not supported on 7210 SAS (for example, GARP, GVRP, ELMI, and others) are transparently forwarded in case of a VPLS service. These protocols are transparently forwarded if a null SAP, dot1q default SAP, dot1q explicit null SAP, or 0.* SAP is configured on the port and the received packet is untagged. If the received packet is tagged and matches the tag of any of the SAPs configured on the port, it is forwarded in the context of the SAP and the service. Otherwise, if the received packet is untagged and none of the null or dot1q default or dot1q explicit null or 0.* SAP is configured, it is discarded.

If a 7210 SAS receives a tagged L2CP packet on any SAP (including null, dot1q, dot1q range, QinQ, QinQ default), it is forwarded transparently in the service similar to normal service traffic (xSTP processing behavior is different in VPLS service and is listed as follows).

The xSTP processing behavior in a VPLS service is as follows:

- If xSTP is enabled in the service, and if the tag in the STP BPDU matches the tag of the configured SAP, the received xSTP BPDU is processed by the local xSTP instance on the node for that service when xSTP is enabled on the SAP, and discarded when xSTP is disabled on the SAP.
- If the tags do not match, xSTP BPDU packets are transparently forwarded in the service similar to normal service traffic.
- If xSTP is disabled in the service, STP BPDU packets are transparently forwarded in the service similar to normal service traffic.

The following table describes L2CP support for the 7210 SAS-R6 and 7210 SAS-R12.

Table 9: L2CP support for 7210 SAS-R6 and 7210 SAS-R12

Packet type	7210 SAS-R6 and 7210 SAS-R12
LACP	Option to tunnel or discard or peer
Dot1x	Option to tunnel or discard or peer
LLDP	Option to tunnel or discard or peer[9]
EFM	Option to tunnel or discard or peer
L2TP	Supported [10]
BPDU Tunneling	Supported
xSTP	Option to peer or tunnel
ESMC protocol	Option to tunnel or discard or peer

2.13 Global services command reference

2.13.1 Command hierarchies

- Customer commands
- Pseudowire (PW) commands (applicable only for 7210 SAS devices configured in network mode)
- SAP commands for 7210 SAS devices configured in access or network mode
- ETH-CFM configuration commands
- Show commands
- Tools perform commands

2.13.1.1 Customer commands

```
config
    - service
        - [no] customer customer-id
            - contact contact-information
            - no contact
            - description description-string
            - no description
            - [no] phone phone-number
```

9 See the *7210 SAS-Mxp, R6, R12, S, Sx, T Interface Configuration Guide* for more information about options available for LLDP tunneling.

10 L2TP support on 7210 SAS platforms varies depending on the platforms. Not all platforms support tunneling of all CISCO protocols. For more information, see L2PT and BPDU translation.

2.13.1.2 Pseudowire (PW) commands (applicable only for 7210 SAS devices configured in network mode)

```
config
    - service
        - pw-routing
            - boot-timer secs
            - no boot-timer
            - local-prefix local-prefix [create]
            - no local-prefix local-prefix
                - advertise-bgp route-distinguisher rd [community community]
                -  no advertise-bgp route-distinguisher rd
            - path name [create]
            - no path name
                - hop hop-index ip-address
                - no hop hop-index
                - [no] shutdown
            - retry-count [10..10000]
            - no retry-count
            - retry-timer secs
            - no retry-timer
            - spe-address global-id:prefix
            - no spe-address
            - [no] static-route route-name
```

```
config
    - service
        - [no] pw-template policy-id [use-provisioned-sdp] [create]
            - accounting-policy acct-policy-id
            - no accounting-policy
            - [no] collect-stats
            - [no] control-word
            - [no] disable-learning
            - [no] disable-aging
            - hash-label [signal-capability]
            - no hash-label
            - igmp-snooping
                - import policy-name
                - no import
                - last-member-query-interval 1/10 seconds
                - no last-member-query-interval
                - max-num-groups max-num-groups
                - no max-num-groups
                - query-interval seconds
                - no query-interval
                - query-response-interval seconds
                - no query-response-interval
                - robust-count robust-count
                - no robust-count
                - [no] send-queries
                - version version
                - no version
            -
vc-type  {blockable | non-blockable}
            - no
vc-type
            - [no] mac-pinning
            - max-nbr-mac-addr table-size
            - no max-nbr-mac-addr
            - split-horizon-group group-name
            - no split-horizon-group
```

```
                - description description-string
                - no description
            -
vc-type  {ether | vlan}
            - vlan-vc-tag  0..4094
            - no vlan-vc-tag
```

```
config
    - service
        - sdp sdp-id [mpls] [create]
        - no sdp sdp-id
            - accounting-policy acct-policy-id
            - no accounting-policy
            - collect-stats acct-policy-id
            - no collect-stats
            - [no] adv-mtu-override
            - [no] bgp-tunnel
            - [no] collect-stats
            - description description-string
            - no description
            - far-end ip-address node-id node-id [global-id global-id]
            - no far-end
            - keep-alive
                - hello-time seconds
                - no hello-time
                - hold-down-time seconds
                - no hold-down-time
                - max-drop-count count
                - no max-drop-count
                - message-length octets
                - no message-length
                - [no] shutdown
                - timeout timeout
                - no timeout
            - [no] ldp
            - metric metric
            - no metric
            -  no mixed-lsp-mode
            - mixed-lsp-mode
                - no revert-time
                - revert-time {revert-time | infinite}
            - [no] lsp lsp-name
            - path-mtu octets
            - no path-mtu
            - [no] shutdown
            - signaling [off | tldp]
            - [no] sr-isis
            - [no] sr-ospf
```

2.13.1.3 SAP commands for 7210 SAS devices configured in access or network mode

```
config
    - service
        - epipe
            - sap sap-id [create] [no-endpoint] with-aggregate-meter
            - no sap sap-id [create] endpoint endpoint-name
            - no sap sap-id
        - vpls
            - sap sap-id [split-horizon-group group-name] [eth-ring ring-index] [create]
            - no sap sap-id
```

```
        - vprn
            - interface ip-int-name [create]
            - no interface ip-int-name
                - sap sap-id [create]
                - no sap sap-id
```

2.13.1.4 ETH-CFM configuration commands

Note:
For command descriptions, see the *7210 SAS-Mxp, R6, R12, S, Sx, T OAM and Diagnostics Guide*.

```
config
    - eth-cfm
        - domain md-index [format md-name-format] [name md-name] level level
        - domain md-index
        - no domain md-index
            - association ma-index [format ma-name-format] name ma-name
            - association ma-index
            - no association ma-index
                - [no] bridge-identifier bridge-id
                    - mhf-creation {none | explicit | default | static}
                    - no mhf-creation
                    - mip-ltr-priority priority
                    - vlan vlan-id
                    - no vlan
                - ccm-interval {10ms | 100ms | 1 | 10 | 60 | 600}
                - no ccm-interval
                - [no] remote-mep-id mep-id
        - slm
            - inactivity-timer timer
            - no inactivity-timer
```

2.13.1.5 Show commands

```
show
    - service
        - customer [customer-id] [site customer-site-name]
        - fdb-mac [ieee-address] [expiry]
        - id service vpls-group
        - id service vpls-group vpls-group-id non-template-saps
        - sdp sdp-id keep-alive-history
        - sdp far-end ip-address keep-alive-history
        - sdp [sdp-id] [detail]
        - sdp far-end ip-address [detail]
        - sdp-using [sdp-id[:vc-id] | far-end ip-address]
        - service-using [epipe] [mirror] [customer customer-id]
    - eth-ring [status]
    - eth-ring ring-index hierarchy
    - eth-ring ring-index [path {a | b}]
    - eth-cfm
        - association [ma-index] [detail]
        - cfm-stack-table [port [port-id [vlan vlan-id]] [level 0..7] [direction down]
        - cfm-stack-table
        - cfm-stack-table port [{all-ports] [level 0..7] [direction down]
        - cfm-stack-table port-id [vlan qtag[.qtag]] [level 0..7] [direction down]
        - mep mep-id domain md-index association ma-index [loopback] [linktrace]
```

```
        - mep mep-id domain md-index association ma-index remote-mepid mep-id | all-remote-
mepids
        - mep mep-id domain md-index association ma-index eth-test-results [remote-peer mac-
address]
        - mep mep-id domain md-index association ma-index one-way-delay-test [remote-peer mac-
address]
        - mep mep-id domain md-index association ma-index two-way-delay-test [remote-peer mac-
address]
        - mip
        - pw-routing {local-prefix | static-route | paths | all}
        - pw-routing route-table [all-routes]
        - pw-routing route-table summary
        - pw-template
```

2.13.1.6 Tools perform commands

```
tools
    - perform
        - service
            - eval-pw-template  policy-id [allow-service-impact]
            - id service-id
                - endpoint endpoint-name
                    - force-switchover sdp-id:vc-id
                    - no force-switchover
                    - force-switchover spoke-sdp-fec [1..4294967295]
                - eval-pw-template  policy-id [allow-service-impact]
            - eval-expired-fec
                - eval-expired-fec  spoke-sdp-fec-id
                - eval-expired-fec  all
            - spoke-sdp-fec-release global-id[:prefix[:ac-id]]
```

2.13.2 Command descriptions

- Configuration commands
- Show commands
- Tools perform commands

2.13.2.1 Configuration commands

2.13.2.1.1 Generic commands

shutdown

Syntax

[**no**] **shutdown**

Context

config>dot1ag>mep

config>service>sdp

config>service>sdp>keep-alive

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

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

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

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

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

Special Cases

Service Admin State

Bindings to an SDP within the service are put into the out-of-service state when the service is shut down. While the service is shut down, all customer packets are dropped and counted as discards for billing and debugging purposes.

SDP (global)

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

SDP (service level)

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

SDP Keepalives

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

description

Syntax

description *description-string*

no description

Context

config>service>customer

config>service>sdp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

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

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

Parameters

string

Specifies the description character string. Allowed values are any string up to 80 characters composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

2.13.2.1.2 Customer management commands

customer

Syntax

customer *customer-id* [**create**]

no customer *customer-id*

Context

config>service

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command creates a customer ID and customer context that associates information with a specific customer. Services can later be associated with this customer at the service level.

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

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

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

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

Parameters

customer-id

Specifies the ID number to be associated with the customer, expressed as an integer.

Values 1 to 2147483647

contact

Syntax

contact *contact-information*

no contact *contact-information*

Context

config>service>customer

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures contact information for a customer.

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

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

Parameters

contact-information

Specifies the customer contact information entered as an ASCII character string up to 80 characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes. Any printable, seven bit ASCII characters may be used within the string.

phone

Syntax

[**no**] **phone** *string*

Context

config>service>customer

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command adds telephone number information for a customer ID.

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

Parameters

string

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

2.13.2.1.3 Pseudowire commands

pw-routing

Syntax

pw-routing

Context

config>service

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

Commands in this context configure dynamic multi-segment pseudowire (MS-PW) routing. Pseudowire routing must be configured on each node that is a T-PE or an S-PE.

Default

disabled

boot-timer

Syntax

boot-timer *timer-value*

no boot-timer

Context

config>service>pw-routing

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

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

The **no** form of this command removes a previously configured timer and reverts it to the default value.

Default

boot-timer 10

Parameters

timer-value

Specifies the value of the boot timer in seconds.

Values 0 to 600

local-prefix

Syntax

local-prefix local-prefix [**create**]

no local-prefix local-prefix

Context

config>service>pw-routing

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

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

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

Default

no local-prefix

Parameters

local-prefix

Specifies a 32-bit prefix for the AII. One or more prefix values, up to a maximum of 16, may be assigned to the node. The global ID can contain the 2-octet or 4-octet value of the provider Autonomous System Number (ASN). The presence of a global ID based on the

provider ASN ensures that the AII for spoke-SDPs configured on the node are globally unique.

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

raw-prefix 1

4294967295

global-id 1

4294967295

advertise-bgp

Syntax

advertise-bgp route-distinguisher rd [**community** *community*]

no advertise-bgp route-distinguisher rd

Context

config>service>pw-routing>local-prefix

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

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

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

Default

no advertise-bgp

Parameters

rd

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

Values (6 bytes, other 2 Bytes of type will be automatically generated) asn:number1 (RD Type 0): 2bytes ASN and 4 bytes locally administered number ip-address:number2 (RD Type 1): 4bytes IPv4 and 2 bytes locally administered number;

community *community*

Specifies an optional BGP community attribute associated with the advertisement. To delete a previously advertised community, **advertise-bgp route-distinguisher** must be run again with the same value for the RD but excluding the community attribute.

Values community {2-byte-as-number:comm-va1} 2-byte-as-number 1 to 65535 comm-val 0 to 65535

path

Syntax

path name [**create**]

no path name

Context

config>service>pw-routing

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures an explicit path between this 7210 SAS T-PE and a remote 7210 SAS T-PE. For each path, one or more intermediate S-PE hops must be configured. A path can be used by multiple multisegment pseudowires. Paths are used by a 7210 T-PE to populate the list of Explicit Route TLVs included in the signaling of a dynamic MS-PW.

A path may specify all or only some of the hops along the route to reach a T-PE.

The **no** form of this command removes a specified explicit path from the configuration.

Default

no path

Parameters

name

Specifies a locally unique, case-sensitive alphanumeric name label for the MS-PW path of up to 32 characters.

hop

Syntax

hop hop-index ip-address

no hop hop-index

Context

config>service>pw-routing>path

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

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

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

Default

no hop

Parameters

hop-index

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

Values 1 to 16

ip-address

Specifies the system IP address or terminating IP address for the T-LDP session to the S-PE corresponding to this hop. For a specific IP address on a hop, the system chooses the SDP.

retry-count

Syntax

retry-count [**10..10000**]

no retry-count

Context

config>service>pw-routing

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This optional command specifies the number of attempts software should make to reestablish the spoke-SDP after it has failed. After each successful attempt, the counter is reset to zero.

When the specified number is reached, no more attempts are made, and the spoke-SDP is put into the shutdown state. Use the **no shutdown** command to bring up the path after the retry limit is exceeded.

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

Default

30

Parameters

retry-count

Specifies the maximum number of retries before putting the spoke-SDP into the shutdown state.

Values 10 to 10000

retry-timer

Syntax

retry-timer *secs*

no retry-timer

Context

config>service>pw-routing

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

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

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

Default

retry-timer 30

Parameters

secs

Specifies the initial retry timer value in seconds.

10 to 480

spe-address

Syntax

spe-address global-id:prefix

no spe-address

Context

config>service>pw-routing

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

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

If the S-PE address is not configured, spoke-SDPs that use dynamic MS-PWs and pw-routing localprefixes cannot be configured on a T-PE. Also, a 7210 SAS node sends a label release for any label mappings received for FEC129 AII type 2.

The S-PE address cannot be changed unless the dynamic ms-pw configuration is removed.

Changing the S-PE address also results in all dynamic MS-PWs for which this node is an S-PE being released. Nokia recommends that the S-PE address be configured for the life of an MS-PW configuration after reboot of the 7210 SAS.

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

Default

no spe-address

Parameters

global-id

Specifies a 4-octet value that is unique to the service provider. For example, the global ID can contain the 2-octet or 4-octet value of the provider Autonomous System Number (ASN).

Syntax: *<global-id:prefix>: <global-id>:{<prefix>|<ipaddress>} global-id 1 to 4294967295 prefix 1 to 4294967295 ipaddress a.b.c.d*

static-route

Syntax

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

Context

config>service>pw-routing

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

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

A default static route is entered as follows:

static-route 0:0:next_hop_ip_addresss

or

static-route 0:0.0.0.0:next_hop_ip_address

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

Default

no static-route

Parameters

route-name

Specifies the static pseudowire route.

Values route-name <global-id>:<prefix>:<next-hop-ip_addr>

<global-id>:0

4294967295 prefix a.b.c.d | 0— 4294967295 ip_addr a.b.c.d

pw-template

Syntax

[**no**] **pw-template** *policy-id* [**use-provisioned-sdp**] [**create**]

Context

config>service

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures an SDP template.

Parameters

use-provisioned-sdp

Specifies whether to use an already provisioned SDP. When specified, the tunnel manager is consulted for an existing active SDP. Otherwise, the default SDP template is used for instantiation of the SDP.

create

This keyword is required when creating the configuration context. When the context is created, it is possible to navigate to the context without the create keyword.

control-word

Syntax

[**no**] **control-word**

Context

config>service>pw-template

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables the use of the control word on pseudowire packets in VPLS and enables the use of the control word individually on each mesh-sdp or spoke-SDP. By default, the control word is disabled. When the control word is enabled, all VPLS packets, including the BPDU frames, are encapsulated with the control word when sent over the pseudowire. The T-LDP control plane behavior is the same as in the implementation of the control word for VLL services. The configuration for the two directions of the Ethernet pseudowire should match.

The **no** form of this command reverts the mesh SDP or spoke-SDP to the default behavior of not using the control word.

Default

no control-word

2.13.2.1.4 SDP commands

sdp

Syntax

sdp *sdp-id* [**mpls**] [**create**]

no sdp *sdp-id*

Context

config>service

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

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

An SDP is a logical mechanism that ties a far-end 7210 SAS device to a particular service without having to specifically define far-end SAPs. Each SDP represents a method to reach a far-end 7210 SAS router.

The 7210 SAS supports only MPLS encapsulation as the method to reach the far-end router It does not support GRE or other encapsulation methods. A 7210 SAS router supports both signaled and non-signaled LSPs through the network. Non-signaled paths are defined at each hop through the network. Signaled paths are communicated by protocol from end to end using Resource ReserVation Protocol (RSVP). Paths may be manually defined or a constraint-based routing protocol (such as OSPF-TE or CSPF) can be used to determine the best path with specific constraints. An LDP LSP can also be used for an SDP when the encapsulation is MPLS. The use of an LDP LSP type or an RSVP/Static LSP type are mutually exclusive except when the mixed-lsp option is enabled on the SDP.

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

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

If the *sdp-id* parameter exists, the current CLI context is changed to that SDP for editing and modification. For editing an existing SDP, the **mpls** keyword is specified. If a keyword is specified for an existing *sdp-id*, an error is generated and the context of the CLI is not changed to the specified *sdp-id*.

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

Parameters

sdp-id

Specifies the SDP identifier.

Values 1 to 17407

accounting-policy

Syntax

accounting-policy *acct-policy-id*

no accounting-policy

Context

config>service>sdp

config>service>pw-template

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

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

A maximum of one accounting policy can be associated with a SDP at one time. Accounting policies are configured in the **config>log** context.

The **no** form of this command removes the accounting policy association from the SDP, and the accounting policy reverts to the default.

Parameters

acct-policy-id

Specifies the accounting policy-id, as configured in the **config>log>accounting-policy** context.

Values 1 to 99

collect-stats

Syntax

[**no**] **collect-stats**

Context

config>service>sdp

config>service>pw-template

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables accounting and statistical data collection for the SDP. When applying accounting policies, the data, by default, is collected in the appropriate records and written to the designated billing file.

When the **no collect-stats** command is issued, the statistics are still accumulated by the IOM cards; however, the CPU does not obtain the results and write them to the billing file. If a subsequent **collect-stats** command is issued, the counters written to the billing file include all the traffic while the **no collect-stats** command was in effect.

Default

no collect-stats

hash-label

Syntax

hash-label [**signal-capability**]

no hash-label

Context

config>service>pw-template

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the hash label on VLL or VPLS services that are bound to an LDP or RSVP SDP using the **auto-bind** mode with the **ldp**, **rsvp-te**, or **mpls** options. When this command is enabled, the ingress datapath is modified such that the result of the hash on the packet header is communicated to the egress datapath for use as the value of the label field of the hash label. The egress datapath appends the hash label at the bottom of the stack (BoS) and sets the S-bit to one (1).

Note:
On 7210 SAS devices, the hash label is not used on the local node for ECMP and LAG hashing. It is available for use by LSR nodes, through which the traffic flows, that are capable of using the labels for hashing.

Packets generated in the CPM that are forwarded with a label within the context of a service (for example, OAM packets) must also include a hash label at the BoS and set the S-bit accordingly.

The TTL of the hash label is set to a value of 0.

Signaling of the hash label capability is enabled by adding the **signal-capability** option under the VLL spoke-SDP, VPLS spoke-SDP, or mesh-SDP interface, or PW template instance. In this case, the decision of the local PE to insert the hash label on the user and control plane packets is determined by the outcome of the signaling process and can override the local PE configuration. The following process flow applies when the **hash-label** and the **signal-capability** options are enabled on the local PE.

- The 7210 SAS local PE inserts the Flow Label Interface Parameters sub-TLV with T=1 and R=1 in the PW ID FEC element in the label mapping message for the specific spoke-SDP or mesh-SDP.
- If a remote PE does not send the Flow Label sub-TLV in the PW ID FEC element, or sends a Flow Label sub-TLV in the PW ID FEC element with T=FALSE and R=FALSE, the local node disables the hash label capability. Consequently, the local PE node does not insert a hash label in the user and control plane packets that it forwards on the spoke-SDP or mesh-SDP. The local PE node also drops user and control plane packets received from remote PE if they include a hash label. The dropped packets may be caused by any of the following:
  - a remote 7210 SAS PE that does not support the **hash-label** command

  - a remote 7210 SAS PE that has the **hash-label** command enabled but does not support the **signal-capability** option
  - a remote 7210 SAS PE that supports the **hash-label** command and the **signal-capability** option, but the user did not enable them due to a misconfiguration
- If the remote PE sends Flow Label sub-TLV in the PW ID FEC element with T=TRUE and R=TRUE, the local PE enables the hash label capability. Consequently, the local PE node inserts a hash label in the user and control plane packets that it forwards on the spoke-SDP or mesh-SDP. The local PE node also accepts user and control plane packets from the remote PE with or without the hash label.

If the **hash-label** command is enabled on the local PE with **signal-capability** option configured and on the remote PE without the **signal-capability** option configured on the spoke-SDP or mesh-SDP, the hash label is included in the pseudowire packets received by the local PE node. These packets must be dropped. To resolve this situation, disable the **signaling-capability** option on the local node, which results in the insertion of the hash label by both the local and remote PE nodes.

If the **hash-label** option is not supported or is not enabled on the local configuration of the spoke-SDP or mesh-SDP at the remote PE, the hash label is not included in the pseudowire received by the local PE.

If the **signal-capability** option is enabled or disabled in the CLI, the router must withdraw the label it sent to its peer and send a new label mapping message with the new value of the F bit in the Flow Label Interface Parameters sub-TLV of the PW ID FEC element.

Note:

- This feature is supported only for VLL and VPLS services. It is not supported for VPRN services. It is also not supported on multicast packets forwarded using RSVP P2MP LPS or mLDP LSP in both the base router instance and in the multicast VPN (mVPN) instance.
- To allow applications where the egress LER infers the presence of the hash label implicitly from the value of the label, the Most Significant Bit (MSB) of the result of the hash is set before copying into the hash label. This means that the value of the hash label is always in the range [524,288 to 1,048,575] and does not overlap with the signaled/static LSP and signaled/static service label ranges. This also guarantees that the hash label does not match a value in the reserved label range. This is not supported on 7210 SAS for service traffic (for MPLS OAM traffic the MSB bit is set). That is, 7210 SAS devices do not set the MSB bit in the hash label value for service traffic; therefore, the user must ensure that both the ends are correctly configured to either process hash labels or disable them.

The **no** form of this command disables the use of the hash label.

Default

no hash-label

Parameters

signal-capability

Keyword that enables the signaling and negotiation of hash label use between the local and remote PE nodes.

vc-type

Syntax

vc-type {**ether** | **vlan**}

Context

config>service>pw-template

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command overrides the default VC type signaled for the binding to the far-end SDP. The VC type is a 15 bit-quantity containing a value which represents the type of VC. The actual signaling of the VC type depends on the signaling parameter defined for the SDP. If signaling is disabled, the vctype command can still be used to define the dot1q value expected by the far-end provider equipment.

A change of the bindings VC type causes the binding to signal the new VC type to the far end when signaling is enabled.

VC types are derived according to IETF *draft-martini-l2circuit-trans-mpls*.

- The VC type value for Ethernet is 0x0005.
- The VC type value for an Ethernet VLAN is 0x0004.

Parameters

ether

Defines the VC type as Ethernet. The **ether** and **vlan** keywords are mutually exclusive. When the VC type is not defined then the default is Ethernet for spoke-SDP bindings. Defining Ethernet is the same as executing no vc-type and restores the default VC type for the spoke-SDP binding. (hex 5)

vlan

Defines the VC type as VLAN. The **ether** and **vlan** keywords are mutually exclusive. When the VC type is not defined, the default is Ethernet for spoke-SDP bindings.

vlan-vc-tag

Syntax

vlan-vc-tag *vlan-id*

no vlan-vc-tag

Context

config>service>pw-template

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command specifies an explicit dot1q value used when encapsulating to the SDP far end. When signaling is enabled between the near and far end, the configured dot1q tag can be overridden by a received TLV specifying the dot1q value expected by the far end. This signaled value must be stored as the remote signaled dot1q value for the binding. The provisioned local dot1q tag must be stored as the administrative dot1q value for the binding.

When the dot1q tag is not defined, the default value of zero is stored as the administrative dot1q value. Setting the value to zero is equivalent to specifying no value.

The **no** form of this command disables the command.

Default

no vlan-vc-tag

Parameters

vlan-id

Specifies a valid VLAN identifier to bind an 802.1Q VLAN tag ID.

Values 0 to 4094

adv-mtu-override

Syntax

[**no**] **adv-mtu-override**

Context

config>service>sdp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command overrides the advertised VC-type MTU of all spoke-SDPs of Layer 2 services using this SDP-ID. When enabled, the router signals a VC MTU equal to the service MTU, which includes the Layer 2 header. It also allows this router to accept an MTU advertised by the far-end PE which value matches either its advertised MTU or its advertised MTU minus the Layer 2 headers.

By default, the router advertises a VC-MTU equal to the Layer 2 service MTU minus the Layer 2 header and always matches its advertised MTU to the one signaled by the far-end PE router, otherwise the spoke-SDP goes operationally down.

When this command is enabled on the SDP, it has no effect on a spoke-SDP of an IES/VPRN spoke interface using this SDP-ID. The router continues to signal a VC MTU equal to the net IP interface MTU,

which is min (ip-mtu, sdp operational path mtu - Layer 2 headers). The router also continues to ensure that the advertised MTU values of both PE routers match or the spoke-SDP goes operationally down.

The **no** form of this command disables the VC-type MTU override and reverts to the default behavior.

Default

no adv-mtu-override

bgp-tunnel

Syntax

[**no**] **bgp-tunnel**

Context

config>service>sdp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables BGP route tunnels available in the tunnel table to reach SDP far-end nodes. Use of BGP route tunnels are available only with MPLS-SDPs. Only one of the transport methods is allowed per SDP - LDP, RSVP-LSP or BGP-Tunnel (BGP-Tunnel is not supported on multimode LSP).

Note:
The 7210 SAS provides an option to install labels for only those BGP 3107 labeled routes that are in use by services. For more information about this option, refer to the *7210 SAS-Mxp, R6, R12, S, Sx, T Routing Protocols Guide*.

The **no** form of this command disables resolving BGP route tunnel LSP for SDP far-end.

Default

no bgp-tunnel

far-end

Syntax

far-end *ip-address* **node-id** *node-id* [**global-id** *global-id*]

no far-end

Context

config>service>sdp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the system IP address of the far-end destination 7210 SAS-R6 and 7210 SAS-R12 router for the Service Distribution Point (SDP) that is the termination point for a service.

The far-end IP address must be explicitly configured. The destination IP address must be a 7210 SAS device system IP address.

If the SDP uses MPLS encapsulation, the **far-end** *ip-address* is used to check LSP names when added to the SDP. If the "**to** IP address" defined within the LSP configuration does not exactly match the SDP **far-end** *ip-address*, the LSP is not added to the SDP and an error is generated.

If the SDP uses MPLS encapsulation, the **far-end** *ip-address* is used to check LSP names when added to the SDP. If the "to IP address" defined within the LSP configuration does not exactly match the SDP far-end ip-address, the LSP is not added to the SDP and an error is generated. Alternatively, an SDP that uses MPLS can have an MPLS-TP node with an MPLS-TP node-id and (optionally) global-id. In this case, the SDP must use an MPLS-TP LSP and the SDP signaling parameter must be set to off.

An SDP cannot be administratively enabled until a far-end ip-address or MPLS-TP node-id is defined. The SDP is operational when it is administratively enabled (no shutdown) and the far-end ip-address is contained in the IGP routing table as a host route. OSPF ABRs should not summarize host routes between areas. This can cause SDPs to become operationally down. Static host routes (direct and indirect) can be defined in the local device to alleviate this issue.

The **no** form of this command removes the currently configured destination IP address for the SDP. The *ip-address* parameter is not specified and will generate an error if used in the **no far-end** command. The SDP must be administratively disabled using the **config service sdp shutdown** command before the **no far-end** command can be executed. Removing the far end IP address causes all *lsp-name* associations with the SDP to be removed.

Parameters

ip-address

Specifies the system address of the far-end 7210 SAS devices for the SDP in dotted-decimal notation.

node-id node-id

Specifies the MPLS-TP Node ID of the far-end system for the SDP, either in dotted-decimal notation (a.b.c.d) or an unsigned 32-bit integer (1 – 4294967295). This parameter is mandatory for an SDP using an MPLS-TP LSP.

global-id global-id

Specifies the MPLS-TP Global ID of the far-end system for the SDP, in an unsigned 32-bit integer. This parameter is optional for an SDP using an MPLS-TP LSP. If not entered, a default value for the Global ID of "0" is used, which indicates that the far-end node is in the same domain as the local node. The user must explicitly configure a Global ID if its value is non-zero.

Values 0 to 4294967295

metric

Syntax

metric *metric*

no metric

Context

config>service>sdp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command specifies the metric used within the tunnel table manager for decision-making purposes. When multiple SDPs going to the same destination exist, this value is used as a tie-breaker by tunnel table manager users such as MP-BGP to select the route with the lower value.

Parameters

metric

Specifies the SDP metric.

Values 0 to 65535

mixed-lsp-mode

Syntax

[**no**] **mixed-lsp-mode**

Context

config>service>sdp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables the use by an SDP of the mixed-LSP mode of operation. This command indicates to the service manager that it must allow a primary LSP type and a backup LSP type in the same SDP configuration. For example, the **lsp** and **ldp** commands are allowed concurrently in the SDP configuration. The user can configure one or two types of LSPs under the same SDP. Without this command, these commands are mutually exclusive.

The user can configure an RSVP LSP as a primary LSP type with an LDP LSP as a backup type. The user can also configure a BGP RFC 3107 BGP LSP as a backup LSP type.

If the user configures an LDP LSP as a primary LSP type, the backup LSP type must be an RFC 3107 BGP labeled route.

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

1. RSVP LSP type. One RSVP LSP can be configured per SDP. This is the highest priority LSP type.
2. LDP LSP type. One LDP FEC is used per SDP. 7210 SAS does not support LDP ECMP.
3. BGP LSP type. One RFC 3107-labeled BGP prefix programmed by the service manager.

In the case of the RSVP/LDP SDP, the service manager programs the NHLFEs for the active LSP type preferring the RSVP LSP type over the LDP LSP type. If no RSVP LSP is configured or all configured RSVP LSPs go down, the service manager reprograms the linecard with the LDP LSP, if available. If not, the SDP goes operationally down.

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

Note:
LDP uses a tunnel down damp timer that is set to three seconds by default. When the LDP LSP fails, the SDP reverts to the RSVP LSP type after the expiry of this timer. For an immediate switchover, this timer must be set to zero. Use the **configure router ldp tunnel-down-damp-time** command. For more information about the **configure router ldp tunnel-down-damp-time** command, see the *7210 SAS-Mxp, R6, R12, S, Sx, T MPLS Guide*.

If the user changes the value of the sdp-revert-time timer, it takes effect only at the next use of the timer. Any timer that is outstanding at the time of the change is restarted with the new value.

In the case of the LDP/BGP SDP, the service manager prefers the LDP LSP type over the BGP LSP type. The service manager reprograms the linecard with the BGP LSP if available, otherwise it brings down the SDP operationally.

Also, the following difference in behavior exists for the LDP/BGP SDP compared to that of an RSVP/LDP SDP. For a specific /32 prefix, only a single route exists in the routing table: the IGP route or the BGP route; therefore, either the LDP FEC or the BGP label route is active at any specific time. The impact of this is that the tunnel table needs to be reprogrammed each time a route is deactivated and the other is activated. Also, the SDP revert-time cannot be used because there is no situation where both LSP types are active for the same /32 prefix.

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

Default

no mixed-lsp-mode

revert-time

Syntax

revert-time {*revert-time* | **infinite**}

no revert-time

Context

config>service>sdp>mixed-lsp-mode

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the delay period the SDP must wait before it reverts to a higher priority LSP type when one becomes available.

The **no** form of this command resets the timer to the default value of 0. This means the SDP reverts immediately to a higher priority LSP type when one becomes available.

Default

0

Parameters

revert-time

Specifies the delay period, in seconds, that the SDP must wait before it reverts to a higher priority LSP type when one becomes available. A value of zero means the SDP reverts immediately to a higher priority LSP type when one becomes available.

Values 0 to 600

infinite

This keyword forces the SDP to never revert to another higher priority LSP type unless the currently active LSP type is down.

ldp

Syntax

[**no**] **ldp**

Context

config>service>sdp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables LDP-signaled LSPs on MPLS-encapsulated SDPs.

In MPLS SDP configurations either one LSP can be specified or LDP can be enabled. The SDP **ldp** and **lsp** commands are mutually exclusive. If an LSP is specified on an MPLS SDP, LDP cannot be enabled on the SDP. To enable LDP on the SDP when an LSP is already specified, the LSP must be removed from the configuration using the **no lsp** *lsp-name* command.

Alternatively, if LDP is already enabled on an MPLS SDP, an LSP cannot be specified on the SDP. To specify an LSP on the SDP, the LDP must be disabled. The LSP must have already been created in the **config>router>mpls** context using a valid far-end IP address. The preceding rules are relaxed when the mixed-lsp option is enabled on the SDP.

Default

no ldp

lsp

Syntax

lsp *lsp-name*

no lsp *lsp-name*

Context

config>service>sdp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command creates associations between one LSP and an Multi-Protocol Label Switching (MPLS) Service Distribution Point (SDP). This command is implemented only on MPLS-type encapsulated SDPs.

In MPLS SDP configurations either one LSP can be specified.

The LSP must have already been created in the **config>router>mpls** context using a valid far-end IP address. RSVP must be enabled.

If no LSP is associated with an MPLS SDP, the SDP cannot enter the operationally up state. The SDP can be administratively enabled (**no shutdown**) with no LSP associations. The *lsp-name* may be shutdown, causing the association with the SDP to be operationally down (the LSP is not used by the SDP).

If an exact match of *lsp-name* does not already exist as a defined LSP, an error message is generated. If the *lsp-name* exists and the LSP **to** IP address matches the SDP **far-end** IP address, the association is created.

The **no** form of this command deletes one LSP association from an SDP. If the *lsp-name* does not exist as an association or as a configured LSP, no error is returned. An *lsp-name* must be removed from all SDP associations before the *lsp-name* can be deleted from the system. The SDP must be administratively disabled (**shutdown**) before the last *lsp-name* association with the SDP is deleted.

Parameters

lsp-name

Specifies the name of the LSP to associate with the SDP. An LSP name is case-sensitive and is limited to 32 ASCII 7-bit printable characters with no spaces.

signaling

Syntax

signaling {**off** | **tldp**}

Context

config>service>sdp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command specifies the signaling protocol used to obtain the ingress and egress pseudowire labels in frames transmitted and received on the SDP. When signaling is **off**, labels are manually configured when the SDP is bound to a service. The signaling value can only be changed while the administrative status of the SDP is down.

To modify the signaling configuration, the SDP must be administratively shut down, then the signaling parameter can be modified and reenabled.

Default

tldp

Parameters

off

Specifies that ingress and egress signal auto-labeling is not enabled. If this keyword is selected, each service using the specified SDP must manually configure VPN labels. This configuration is independent of the SDP transport type, MPLS (RSVP or LDP).

tldp

Specifies that ingress and egress pseudowire signaling using T-LDP is enabled.

path-mtu

Syntax

path-mtu *bytes*

no path-mtu

Context

config>service>sdp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the Maximum Transmission Unit (MTU) in bytes that the Service Distribution Point (SDP) can transmit to the far-end device router without packet dropping or IP fragmentation overriding the SDP-type default path-mtu.

The default SDP-type **path-mtu** can be overridden on a per SDP basis. Dynamic maintenance protocols on the SDP like RSVP may override this setting.

If the physical **mtu** on an egress interface indicates the next hop on an SDP path cannot support the current **path-mtu**, the operational **path-mtu** on that SDP is modified to a value that can be transmitted without fragmentation. By default, the default **path-mtu** defined on the system for the type of SDP is used.

The **no** form of this command removes any **path-mtu** defined on the SDP, and the SDP uses the system default for the SDP type.

sr-isis

Syntax

[**no**] **sr-isis**

Context

config>service>sdp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the IS-IS segment routing LSP type for an MPLS SDP. The SDP of LSP type **sr-isis** can be used with the **far-end** command. The signaling protocol for the service labels for an SDP using an SR tunnel can be configured to static (**off**), T-LDP (**tldp**), or BGP (**bgp**).

The **no** form of this command disables the use of the IS-IS segment routing LSP type for an MPLS SDP.

Default

no sr-isis

sr-ospf

Syntax

[**no**] **sr-ospf**

Context

config>service>sdp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures an OSPF segment routing LSP type for an MPLS SDP. The SDP of LSP type **sr-ospf** can be used with the **far-end** command. The signaling protocol for the service labels for an SDP using an SR tunnel can be configured to static (**off**), T-LDP (**tldp**), or BGP (**bgp**).

The **no** form of this command disables the use of the OSPF segment routing LSP type for an MPLS SDP.

Default

no sr-ospf

2.13.2.1.5 SDP keepalive commands

keep-alive

Syntax

keepalive

Context

config>service>sdp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

Commands in this context configure SDP connectivity monitoring keepalive messages for the SDP ID.

SDP-ID keepalive messages use SDP Echo Request and Reply messages to monitor SDP connectivity. The operating state of the SDP is affected by the keepalive state on the SDP-ID. SDP Echo Request messages are sent only when the SDP-ID is completely configured and administratively up. If the SDP-ID is administratively down, keepalives for that SDP-ID are disabled. SDP Echo Requests (when sent for keepalive messages) are always sent with the *originator-sdp-id*. All SDP-ID keepalive SDP Echo Replies are sent using generic IP OAM encapsulation.

When a keepalive response is received that indicates an error condition, the SDP ID is immediately brought operationally down. When a response is received that indicates the error has cleared and the **hold-down-time** interval has expired, the SDP ID is eligible to be put into the operationally up state. If no other condition prevents the operational change, the SDP ID enters the operational state.

A set of event counters track the number of keepalive requests sent, the size of the message sent, non-error replies received, and error replies received. A keepalive state value is kept indicating the last response event. A keepalive state timestamp value is kept indicating the time of the last event. With each keepalive event change, a log message is generated indicating the event type and the timestamp value.

The following table describes the keepalive interpretation of SDP echo reply response conditions and the effect on the SDP ID operational status.

Table 10: SDP echo reply response conditions

Result of request	Stored response state	Operational state
keepalive request timeout without reply	Request Timeout	Down
keepalive request not sent because of non-existent *orig-sdp-id*[11]	Orig-SDP Non-Existent	Down
keepalive request not sent because of administratively down *orig-sdp-id*	Orig-SDP Admin-Down	Down
keepalive reply received, invalid origination-id	Far End: Originator-ID Invalid	Down
keepalive reply received, invalid responder-id	Far End: Responder-ID Error	Down
keepalive reply received, No Error	Success	Up (If no other condition prevents)

hello-time

Syntax

hello-time *seconds*

no hello-time

Context

config>service>sdp>keep-alive

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the time period between SDP keepalive messages on the SDP-ID for the SDP connectivity monitoring messages.

The **no** form of this command reverts the **hello-time** *seconds* value to the default.

[11] This condition should not occur.

Default

hello-time 10

Parameters

seconds

Specifies the time in seconds between SDP keepalive messages, expressed as a decimal integer.

Values 1 to 3600

hold-down-time

Syntax

hold-down-time *seconds*

no hold-down-time

Context

config>service>sdp>keep-alive

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the minimum time period the SDP remains in the operationally down state in response to SDP keepalive monitoring.

This parameter can be used to prevent the SDP operational state from "flapping" by rapidly transitioning between the operationally up and operationally down states based on keepalive messages.

When an SDP keepalive response is received that indicates an error condition or the **max-drop-count** keepalive messages receive no reply, the *sdp-id* is immediately brought operationally down. If a keepalive response is received that indicates the error has cleared, the *sdp-id* is eligible to be put into the operationally up state only after the **hold-down-time** interval has expired.

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

Default

hold-down-time 10

Parameters

seconds

Specifies the time in seconds, expressed as a decimal integer, the *sdp-id* remains in the operationally down state before it is eligible to enter the operationally up state. A value of 0 indicates that no **hold-down-time** is enforced for *sdp-id*.

Values 0 to 3600

max-drop-count

Syntax

max-drop-count *count*

no max-drop-count

Context

config>service>sdp>keep-alive

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the number of consecutive SDP keepalive failed request attempts or remote replies that can be missed after which the SDP is take operationally down. If the **max-drop-count** consecutive keepalive request messages cannot be sent or no replies are received, the SDP-ID is taken operationally down by the keepalive SDP monitoring.

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

Default

max-drop-count 3

Parameters

count

Specifies he number of consecutive SDP keepalive requests that are failed to be sent or replies missed, expressed as a decimal integer.

Values 1 to 5

message-length

Syntax

message-length *octets*

no message-length

Context

config>service>sdp>keep-alive

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the SDP monitoring keepalive request message length that is transmitted.

The message length should be equal to the SDP operating path MTU, as configured in the path-mtu command. If the default size is overridden, the actual size used is the smaller of the operational SDP-ID Path MTU and the size specified.

The **no** form of this command reverts the default value.

Default

message-length 0

Parameters

octets

Specifies the size of the keepalive request messages in octets, expressed as a decimal integer. The **size** keyword overrides the default keepalive message size.

Values 40 to 9198

timeout

Syntax

timeout *timeout*

no timeout

Context

config>service>sdp>keep-alive

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the time interval that the SDP waits before tearing down the session.

Default

timeout 5

Parameters

timeout

Specifies the timeout time, in seconds.

Values 1 to 10

2.13.2.2 Show commands

2.13.2.2.1 Service show commands

customer

Syntax

customer [*customer-id*] [**site** *customer-site-name*]]

Context

show>service

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays service customer information.

Parameters

customer-id

Displays only information for the specified customer ID.

Default All customer IDs display.

Values 1 to 2147483647

site *customer-site-name*

Specifies the customer site, which is an anchor point for an ingress and egress virtual scheduler hierarchy.

Output

The following output is an example of service customer information, and Table 11: Output fields: customer describes the output fields.

Sample output

```
*A:ALA-12# show service customer
===============================================================
Customers
===============================================================
Customer-ID : 1
Contact     : Manager
Description : Default customer
Phone       : (123) 555-1212

Customer-ID : 2
Contact     : Tech Support
```

```
Description : TiMetra Networks
Phone       : (234) 555-1212

Customer-ID : 3
Contact     : Test
Description : TiMetra Networks
Phone       : (345) 555-1212

Customer-ID : 6
Contact     : Test1
Description : Epipe Customer
Phone       : (456) 555-1212

Customer-ID : 7
Contact     : Test2
Description : VPLS Customer
Phone       : (567) 555-1212

Customer-ID : 274
Contact     : TestA
Description : ABC Company
Phone       : 650 123-4567

Customer-ID : 94043
Contact     : Test Engineer on Duty
Description : TEST Customer
Phone       : (789) 555-1212
-------------------------------------------------------
Total Customers : 8
-------------------------------------------------------
*A:ALA-12#
*A:ALA-12# show service customer 274
===============================================================================
Customer  274
===============================================================================
Customer-ID : 274
Contact     : Mssrs. Beaucoup
Description : ABC Company
Phone       : 650 123-4567
-------------------------------------------------------------------------------
Multi Service Site
-------------------------------------------------------------------------------
Site        : west
Description : (Not Specified)
===============================================================================
*A:ALA-12#
```

Table 11: Output fields: customer

Label	Description
Customer-ID	The ID that uniquely identifies a customer.
Contact	The name of the primary contact person.
Description	Generic information about the customer.
Phone	The phone or pager number to reach the primary contact person.
Total Customers	The total number of customers configured.

Label	Description
Site	Multi-service site name. A multi-service customer site is a group of SAPs with common origination and termination points.
Description	Displays information about the multi-service site of a specific customer.
Assignment	The port ID, MDA, or card number, where the SA's that are members of this multi- service site are defined.
I. Sched Pol	The ingress QoS scheduler policy assigned to this multi-service site.
E. Sched Pol	The egress QoS scheduler policy assigned to this multi-service site.
Service-ID	The ID that uniquely identifies a service.
SAP	Specifies the SAP assigned to the service.

fdb-mac

Syntax

fdb-mac [*ieee-address*] [**expiry**]

Context

show>service

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays the FDB entry for a specific MAC address.

Parameters

ieee-address

Specifies the 48-bit MAC address in the form aa:bb:cc:dd:ee:ff or aa-bb-cc-dd-ee-ff where aa, bb, cc, dd, ee, and ff are hexadecimal numbers.

expiry

Keyword to display the amount of time until MAC is aged out.

Output

The following output is an example of FDB MAC information, and Table 12: Output fields: FDB MAC describes the output fields.

Sample output

```
*A:ALA-48# show service fdb-mac
===============================================================================
Service Forwarding Database
===============================================================================
ServId    MAC               Source-Identifier     Type/Age  Last Change
-------------------------------------------------------------------------------
103       12:34:56:78:90:0f sap:1/1/7:0           Static    02/02/2009 09:27:57
700       90:30:ff:ff:ff:8f cpm                   Host      02/02/2009 09:27:57
-------------------------------------------------------------------------------
No. of Entries: 2
===============================================================================
*A:ALA-48#


*A:ALA-48# show service fdb-mac expiry
===============================================================================
Service Forwarding Database
===============================================================================
ServId    MAC               Source-Identifier     Type/     Last Change
                                                  Expiry
-------------------------------------------------------------------------------
103       12:34:56:78:90:0f sap:1/1/7:0           Static    02/02/2009 09:27:57
700       90:30:ff:ff:ff:8f cpm                   Host      02/02/2009 09:27:57
-------------------------------------------------------------------------------
No. of Entries: 2
===============================================================================
*A:ALA-48#
```

Table 12: Output fields: FDB MAC

Label	Description
ServId	Displays the configured service ID
MAC	Displays the MAC address
Source-Identifier	Displays the location where the MAC is defined
Type/Age	Static — FDB entries created by management Learned — Dynamic entries created by the learning process OAM — Entries created by the OAM process H — Host, the entry added by the system for a static configured subscriber host D or DHCP — DHCP-installed MAC. Learned addresses can be temporarily frozen by the DHCP snooping application for the duration of a DHCP lease. P — Indicates the MAC is protected by the MAC protection feature
Last Change	Displays the time when the specific row entry was last changed

sdp

Syntax

sdp *sdp-id* **keep-alive-history**

sdp far-end *ip-address* **keep-alive-history**

sdp [*sdp-id*] [**detail**]

sdp far-end *ip-address* [**detail**]

Context

show>service

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays SDP information.

If no optional parameters are specified, a summary SDP output for all SDPs is displayed.

Parameters

sdp-id

Specifies the SDP ID for which to display information.

Default All SDPs.

Values 1 to 17407

far-end *ip-address*

Displays only SDPs matching with the specified far-end IP address.

Default SDPs with any far-end IP address.

detail

Displays detailed SDP information.

Default SDP summary output.

keep-alive-history

Displays the last fifty SDP keepalive events for the SDP.

Default SDP summary output.

Output

The following output is an example of SDP information, and Table 13: Output fields: service SDP describes the output fields.

Sample output

```
*A:ALA-7210# show service sdp
===============================================================================
Services: Service Destination Points
===============================================================================
SdpId    Adm MTU   Opr MTU   IP address       Adm  Opr         Del LSP Signal
-------------------------------------------------------------------------------
10       4462      4462      10.20.1.3        Up   Dn NotReady MPLS B TLDP
40       4462      1534      10.20.1.20       Up   Up          MPLS B TLDP
60       4462      1514      10.20.1.21       Up   Up          MPLS B TLDP
100      4462      4462      10.0.0.2         Down Down        MPLS B TLDP
500      4462      4462      10.20.1.50       Up   Dn NotReady MPLS B TLDP
-------------------------------------------------------------------------------
Number of SDPs : 5
===============================================================================
*A:ALA-7210#


*7210SAS>show>service# sdp 1 detail

===============================================================================
Service Destination Point (Sdp Id : 1) Details
===============================================================================
-------------------------------------------------------------------------------
 Sdp Id 1  -0.0.0.0
-------------------------------------------------------------------------------
Description           : (Not Specified)
SDP Id                : 1                     SDP Source         : manual
Admin Path MTU        : 0                     Oper Path MTU      : 0
Far End               : 0.0.0.0               Delivery           : MPLS
Tunnel Far End        : n/a                   LSP Types          : None

Admin State           : Down                  Oper State         : Down
Signaling             : TLDP                  Metric             : 0
Acct. Pol             : None                  Collect Stats      : Disabled
Last Status Change    : 11/04/2099 22:56:41   Adv. MTU Over.     : No
Last Mgmt Change      : 11/10/2099 15:56:44   VLAN VC Etype      : 0x8100
Bw BookingFactor      : 100                   PBB Etype          : 0x88e7
Oper Max BW(Kbps)     : 0                     Avail BW(Kbps)     : 0
Net-Domain            : default               Egr Interfaces     : n/a
Flags                 : SdpAdminDown NoSysIPAddr
                        TranspTunnDown

Mixed LSP Mode Information :
Mixed LSP Mode        : Enabled               Active LSP Type    : RSVP....also be
                                                                   LDP, BGP
Revert Time           : 200                   Revert Count Down  : n/a

KeepAlive Information :
Admin State           : Disabled              Oper State         : Disabled
Hello Time            : 10                    Hello Msg Len      : 0
Hello Timeout         : 5                     Unmatched Replies  : 0
Max Drop Count        : 3                     Hold Down Time     : 10
Tx Hello Msgs         : 0                     Rx Hello Msgs      : 0

-------------------------------------------------------------------------------
RSVP/Static LSPs
-------------------------------------------------------------------------------
Associated LSP List :
No LSPs Associated

===============================================================================
```

```
*7210SAS>show>service#
```

Table 13: Output fields: service SDP

Label	Description
SDP Id	Displays the SDP identifier
Description	Displays a text string describing the SDP
Admin Path MTU	Displays the required largest service frame size (in octets) that can be transmitted through this SDP to the far-end ESR, without requiring the packet to be fragmented. The default value of zero indicates that the path MTU should be computed dynamically from the corresponding MTU of the tunnel.
Opr Path MTU	Displays the actual largest service frame size (in octets) that can be transmitted through this SDP to the far-end ESR, without requiring the packet to be fragmented. To be able to bind this SDP to a specific service, the value of this object minus the control word size (if applicable) must be equal to or larger than the MTU of the service, as defined by its service MTU.
Far End	Displays the far end IP address
Delivery	The type of delivery used by the SDP: MPLS
IP address	Specifies the IP address of the remote end of the MPLS tunnel defined by this SDP
Adm Admin State	The administrative state of the SDP
Opr Oper State	The operating state of the SDP
Flags	Specifies all the conditions that affect the operating status of this SDP
Signal Signaling	The signaling protocol used to obtain the ingress and egress labels used in frames transmitted and received on the SDP
Last Status Change	The time of the most recent operating status change to this SDP
Adv. NTU Over	Specifies whether the advertised MTU of a VLL spoke-SDP bind includes the 14-byte Layer 2 header, so that it is backward compatible with pre-2.0 software.
Last Mgmt Change	The time of the most recent management-initiated change to this SDP.
KeepAlive Information	This section displays Keepalive information.

Label	Description
Hello Time	Specifies how often the SDP echo request messages are transmitted on this SDP.
Hello Msg Len	The length of the SDP echo request messages transmitted on this SDP.
Hello Timeout	The number of seconds to wait for an SDP echo response message before declaring a timeout.
Unmatched Replies	The number of SDP unmatched message replies timer expired.
Max Drop Count	The maximum number of consecutive SDP echo request messages that can be unacknowledged before the keepalive protocol reports a fault.
Hold Down Time	The amount of time to wait before the keepalive operating status is eligible to enter the alive state.
TX Hello Msgs	The number of SDP echo request messages transmitted after the keepalive was administratively enabled or the counter was cleared.
Rx Hello Msgs	The number of SDP echo request messages received after the keepalive was administratively enabled or the counter was cleared.
Associated LSP List	When the SDP type is MPLS, a list of LSPs used to reach the far-end router displays. All the LSPs in the list must terminate at the IP address specified in the far end field.
Lsp Name	Displays the LSP name.
Time Since Last Transaction	Displays the time of the last transaction.
Signaling	Specifies the signaling type.
Metric	Displays the metric to be used within the Tunnel Table Manager for decision making purposes. When multiple SDPs going to the same destination exist, this value is used as a tie-breaker by Tunnel Table Manager users like MP-BGP to select route with lower value.
Acct. Pol	Displays the policy to use to collect accounting statistics on this SDP. The value zero indicates that the agent should use the default accounting policy, if one exists.
Collect Stats	Specifies whether the agent collects accounting statistics for this SDP. When the value is true the agent collects accounting statistics on this SDP.
VLAN VC Etype	Displays the VLAN VC type.

Label	Description
BW Booking Factor	Specifies the value used to calculate the max SDP available bandwidth. The value specifies the percentage of the SDP max available bandwidth for VLL call admission. When the value of is set to zero (0), no new VLL spoke-SDP bindings with non-zero bandwidth are permitted with this SDP. Overbooking >100% is allowed.
PBB Etype	Displays the Ethertype used in frames sent out on this SDP when specified as **vlan** for Provider Backbone Bridging frames.
Oper Max BW (Kbps)	Indicates the operational bandwidth in kilo-bits per seconds (Kbps) available for this SDP. The value is determined by the sum of the bandwidth of all the RSVP LSPs used by the SDP.
Avail BW (Kbps)	Indicates the bandwidth that is still free for booking by the SDP bindings on the SDP.
Net-Domain	Specifies the network-domain name configured on this SDP. The default value of this object is the default'network-domain.
Egr Interface	Indicates whether all the egress network interfaces that can carry traffic on this SDP are associated with the network-domain configured on this SDP. Not applicable — Indicates that there is no egress network interface that can carry traffic on this SDP. Consistent — Indicates that the network-domains for all the egress network interfaces that can carry traffic on this SDP are consistent. Inconsistent — Indicates that the network-domain for one or more egress network interfaces that can carry traffic on this SDP are inconsistent.
Mixed LSP Mode	Indicates whether the SDP is enabled to use mixed-mode-lsp.
Active LSP Type	Displays the LSP type that is currently active and in use to transport service packets. When multiple LSPs are configured under the SDP and enabled with the command **mixed-mode-lsp**, the active LSP could be one of the configured ones. It displays RSVP, if the LSP in use is of type RSVP LSP, LDP if the LSP in use is of type LDP LSP and BGP 3107, if LSP if of type RFC 3107 BGP Labeled route LSP.
Revert Time	Specifies the time to wait before reverting back from LDP to the configured LSPs, after having failed over to LDP.
Revert Count Down	Indicates the timer countdown before reverting back from LDP on this SDP. The timer countdown begins after the first configured LSP becomes active.

Label	Description
Flags	Displays all the conditions that affect the operating status of this SDP.
Class Forwarding	Indicates the admin state of class-based forwarding on this SDP. When the value is true, class-based forwarding is enabled.
EnforceDSTELspFc	Specifies whether service manager must validate with RSVP the support of the FC by the LSP.
Default LSP	Specifies the LSP ID that is used as a default when class-based forwarding is enabled on this SDP. This object must be set when enabling class-based forwarding.
Multicast LSP	Displays the LSP ID that all multicast traffic is forwarded on when class-based forwarding is enabled on this SDP. When this object has its default value, multicast traffic is forwarded on an LSP according to its forwarding class mapping.
Number of SDPs	The total number of SDPs displayed according to the criteria specified.

sdp-using

Syntax

sdp-using [*sdp-id*[**:***vc-id*] | **far-end** *ip-address*]

Context

show>service

Platforms

Supported on all 7210 SAS platforms as described in this document

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 to 17407

vc-id

Specifies the virtual circuit identifier.

Values 1 to 4294967295

far-end *ip-address*

Displays only services matching the specified far-end IP address.

Default Services with any far-end IP address.

Output

The following output is an example of service SDP information, and Table 14: Output fields: SDP using describes the output fields.

Sample output

```
*A:ALA-7210# show service sdp-using 300
===============================================================================
Service Destination Point (Sdp Id : 300)
===============================================================================
SvcId       SdpId               Type Far End        Opr State I.Label  E.Label
-------------------------------------------------------------------------------
1           300:1               Spok 10.0.0.13      Up        131071   131071
2           300:2               Spok 10.0.0.13      Up        131070   131070
100         300:100             Spok 10.0.0.13      Up        131069   131069
101         300:101             Spok 10.0.0.13      Up        131068   131068
-------------------------------------------------------------------------------
Number of SDPs : 4
===============================================================================
*A:ALA-7210#
```

Table 14: Output fields: SDP using

Label	Description
Svc ID	The service identifier.
Sdp ID	The SDP identifier.
Type	Type of SDP: spoke
Far End	The far end address of the SDP.
Oper State	The operational state of the service.
Ingress Label	The label used by the far-end device to send packets to this device in this service by this SDP.
Egress Label	The label used by this device to send packets to the far-end device in this service by this SDP.

service-using

Syntax

service-using [**sdp** *sdp-id*] [**b-vpls**] [**m-vpls**] [**sdp** *sdp-id*] [**customer** *customer-id*]

Context

show>service

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays the services matching specified usage properties. If no optional parameters are specified, all services defined on the system are displayed.

Parameters

epipe

Displays matching Epipe services.

vpls

Displays matching VPLS instances.

sdp *sdp-id*

Displays only services bound to the specified SDP ID.

Default Services bound to any SDP ID.

Values 1 to 17407

customer *customer-id*

Displays services only associated with the specified customer ID.

Default Services associated with a customer.

Values 1 to 2147483647

Output

The following output is an example of service information, and Table 15: Output fields: service using describes the output fields.

Sample output

```
*7210SAS>show>service# service-using customer 1

===============================================================================
Services  Customer 1
===============================================================================
ServiceId    Type      Adm  Opr  CustomerId Service Name
-------------------------------------------------------------------------------
1            VPLS      Up   Up   1
2            VPLS      Up   Up   1
3            VPLS      Up   Up   1
4            VPLS      Up   Up   1
2147483648   IES       Up   Down 1          _tmnx_InternalIesService
2147483649   intVpls   Up   Down 1          _tmnx_InternalVplsService
-------------------------------------------------------------------------------
Matching Services : 6
-------------------------------------------------------------------------------
```

```
===============================================================================
*7210SAS>show>service#
```

Table 15: Output fields: service using

Label	Description
Service Id	The service identifier.
Type	Specifies the service type configured for the service ID.
Adm	The administrative state of the service.
Opr	The operating state of the service.
CustomerID	The ID of the customer who owns this service.
Service name	The name of the service.

eth-ring

Syntax

eth-ring [**status**]

eth-ring [**ring-index**] **hierarchy**

eth-ring ring-index [**path** {**a** | **b**}]

Context

show

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays the Ethernet rings information.

Parameters

status

Displays the status information of the Ethernet rings configured on the system.

hierarchy

Displays Eth-ring hierarchical relationships.

path {a | b}

Displays information related to the configured Ethernet rings.

ring-index

Specifies the ring index of the Ethernet ring.

Values 1 to 128

Output

The following outputs are examples of Ethernet ring information, and the associated tables describe the output fields.

- Sample output, Sample for 7210 SAS-R6 and 7210 SAS-R12, Table 16: Output fields: show Ethernet ring
- Sample output for Ethernet ring status, Table 17: Output fields: Ethernet ring status

Sample output

```
*A:NS1015C0821>show# eth-ring 10

===============================================================================
Ethernet Ring 10 Information
===============================================================================
Description        : (Not Specified)
Admin State        : Down               Oper State       : Down
Node ID            : 00:25:ba:03:48:04
Guard Time         :    5 deciseconds   RPL Node         : rplNone
Max Revert Time    :  300 seconds       Time to Revert   : N/A
CCM Hold Down Time :    0 centiseconds  CCM Hold Up Time :   20 deciseconds
Compatible Version : 2
APS Tx PDU         : N/A
Defect Status      :
Sub-Ring Type      : virtualLink        Interconnect-ID  : N/A

-------------------------------------------------------------------------------
Ethernet Ring Path Summary
-------------------------------------------------------------------------------
Path Port     Raps-Tag     Admin/Oper      Type            Fwd State
-------------------------------------------------------------------------------
  a  -        -                -/-         -               -
  b  -        -                -/-         -               -
===============================================================================
*A:NS1015C0821>show#
```

Sample for 7210 SAS-R6 and 7210 SAS-R12

```
*A:7210SAS>show# eth-ring

===============================================================================
Ethernet Rings (summary)
===============================================================================
Ring Int  Admin Oper           Paths Summary                      Path States
ID   ID   State State                                             a     b
-------------------------------------------------------------------------------
1    -    Up    Up    a - 1/1/3    1         b - 1/1/1    1         B     U
10   -    Up    Up    a - 1/1/3    10        b - 1/1/1    10        B     U
30   -    Up    Up    a - 1/1/3    30        b - 1/1/1    30        B     U
===============================================================================
Ethernet Ring Summary Legend:   B - Blocked    U - Unblocked
*A:7210SAS>show#
```

Table 16: Output fields: show Ethernet ring

Label	Description
Description	The ring description.
Admin State	Displays the administrative state.
Oper State	Displays the operational state.
Node ID	Displays the node identifier.
Guard Time	Displays the configured guard time.
Max Revert time	Displays the configured maximum revert time.
CCM Hold down time	Displays the configured CCM Hold down time.
APS TX PDU	Displays the APS TX PDU information.
Defect Status	Displays the defect status.
RPL Node	Displays the RPL node information.
Time to revert	Displays the configured time to revert.
CCM Hold Up Time	Displays the configured CCM Hold up time.
Sub-Ring Type	Displays the sub-ring type information, the sub-ring type can be virtual link or on-virtual link.
Interconnect-ID	Displays the interconnect ID. The ID can be a ring-index ID or VPLS service ID.
Compatible Version	Displays the Ethernet ring version information.

Sample output for Ethernet ring status

```
*A:NS1015C0821>show# eth-ring status

===============================================================================
Ethernet Ring (Status information)
===============================================================================
Ring   Admin  Oper       Path Information               MEP Information
ID     State  State  Path         Tag       State     Ctrl-MEP CC-Intvl Defects
-------------------------------------------------------------------------------
1      Up     Up     a - 1/1/1    100       Up        Yes      100ms     -----
                     b - 1/1/2    100       Up        Yes      100ms     -----
10     Down   Down   a - N/A                -         -        -         -----
                     b - N/A                -         -        -         -----
===============================================================================
Ethernet Tunnel MEP Defect Legend:
R = Rdi, M = MacStatus, C = RemoteCCM, E = ErrorCCM, X = XconCCM
*A:NS1015C0821>show#
```

Table 17: Output fields: Ethernet ring status

Label	Description
Ring Id	The ring identifier
Admin State	Displays the administrative state
Oper State	Displays the operational state
Path Information	
Path	Displays the path information
Tag	Displays the tag information
State	Displays the state of the path
MEP Information	
Ctrl-MEP	Displays the Ctrl-MEP information
CC-Intvl	Displays the Ctrl-Interval information
Defects	Displays the defects

pw-routing

Syntax

pw-routing {**local-prefix** | **static-route** | **paths** | **all**}

pw-routing route-table [**all-routes**]

pw-routing route-table summary

Context

show>service

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays PW routing information at this 7210 node.

Parameters

local-prefix | static-route | paths | all

Shows details of the T-PE prefixes configured on this node, static routes from this node, explicit PW paths configured on this node, or all of these.

route-table [all-routes]

Displays the PW routing table on this node. If all-routes is specified, the full routing table is displayed.

route-table summary

Displays a summary of the PW routing table for this node.

Output

The following output is an example of PW routing information.

Sample output

```
*A:Dut-C# show service pw-routing local-prefix
===============================================================================
Service PW Routing Information
===============================================================================
===============================================================================
Service PW Routing Local-Prefix RD Information
===============================================================================
Local-Prefix               Route-Dist                Community       Adv-Bgp
-------------------------------------------------------------------------------
3:10.20.1.3                100:3                     100:3           enabled
                           100:4                     100:4           enabled
-------------------------------------------------------------------------------
Local-Prefix Entries found: 1
===============================================================================
===============================================================================
*A:Dut-C# show service pw-routing static-route
===============================================================================
Service PW Routing Information
===============================================================================
=========================================================
Service PW Routing Static-Route Information
=========================================================
Prefix                        Next-Hop
---------------------------------------------------------
6:10.20.1.6/64                10.20.1.5
---------------------------------------------------------
Static Route Entries found: 1
=========================================================
===============================================================================


*A:Dut-C# show service pw-routing paths
===============================================================================
Service PW Routing Information
===============================================================================
============================================================
Service PW Routing Path Information
============================================================
Path                             Adm     Hop IP Address
------------------------------------------------------------
path1_to_F                       up      1   10.20.1.5
                                         2   10.20.1.2
path1_to_F2                      up      1   10.20.1.2
                                         2   10.20.1.5
------------------------------------------------------------
Path Entries found: 2
============================================================
===============================================================================
```

```
*A:Dut-C# show service pw-routing all
===============================================================================
Service PW Routing Information
===============================================================================
SPE-Address       : 3:10.20.1.3
Boot Timer        : 10 secs
Boot Timer Remain : 0 secs
Retry Timer       : 30 secs
Retry Count       : 30

===============================================================================
Service PW Routing Local-Prefix RD Information
===============================================================================
Local-Prefix               Route-Dist                Community       Adv-Bgp
-------------------------------------------------------------------------------
3:10.20.1.3                100:3                     100:3           enabled
                           100:4                     100:4           enabled
-------------------------------------------------------------------------------
Local-Prefix Entries found: 1
===============================================================================
=========================================================
Service PW Routing Static-Route Information
=========================================================
Prefix                        Next-Hop
---------------------------------------------------------
6:10.20.1.6/64                10.20.1.5
---------------------------------------------------------
Static Route Entries found: 1
=========================================================
=============================================================
Service PW Routing Path Information
=============================================================
Path                             Adm     Hop IP Address
-------------------------------------------------------------
path1_to_F                       up      1   10.20.1.5
                                         2   10.20.1.2
path1_to_F2                      up      1   10.20.1.2
                                         2   10.20.1.5
-------------------------------------------------------------
Path Entries found: 2
=============================================================
===============================================================================


*A:Dut-C# show service pw-routing route-table all-routes
===============================================================================
Service PW L2 Routing Information
===============================================================================
AII-Type2/Prefix-Len                           Next-Hop       Owner  Age
 Route-Distinguisher                            Community      Best
-------------------------------------------------------------------------------
3:10.20.1.3:0/64                               10.20.1.3      local  00h32m08s
 0:0                                            0:0            yes
3:10.20.1.3:1/96                               10.20.1.3      host   00h32m08s
 0:0                                            0:0            yes
3:10.20.1.3:2/96                               10.20.1.3      host   00h32m08s
 0:0                                            0:0            yes
3:10.20.1.3:3/96                               10.20.1.3      host   00h32m08s
 0:0                                            0:0            yes
3:10.20.1.3:4/96                               10.20.1.3      host   00h32m08s
 0:0                                            0:0            yes
3:10.20.1.3:5/96                               10.20.1.3      host   00h32m08s
 0:0                                            0:0            yes
```

```
3:10.20.1.3:6/96                                  10.20.1.3      host   00h32m08s
 0:0                                               0:0            yes
3:10.20.1.3:7/96                                  10.20.1.3      host   00h32m08s
 0:0                                               0:0            yes
3:10.20.1.3:8/96                                  10.20.1.3      host   00h32m08s
 0:0                                               0:0            yes
3:10.20.1.3:9/96                                  10.20.1.3      host   00h32m08s
 0:0                                               0:0            yes
3:10.20.1.3:10/96                                 10.20.1.3      host   00h32m07s
 0:0                                               0:0            yes
6:10.20.1.6:0/64                                  10.20.1.5      static 00h07m33s
 0:0                                               0:0            yes
6:10.20.1.6:0/64                                  10.20.1.5      bgp    00h31m34s
 100:6                                             100:6          no
-------------------------------------------------------------------------------
Entries found: 13
===============================================================================


*A:Dut-C# show service pw-routing route-table summary
=======================================
Service PW L2 Routing Summary
=======================================
Source              Active
---------------------------------------
BGP                 1
Static              1
Host                10
Local               3
---------------------------------------
Total               15
=======================================
```

pw-template

Syntax

pw-template

Context

show>service

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays information about PW templates.

Output

The following output is an example of PW template information.

Sample output

```
*A:Dut-B#    show service  pw-template 1
===============================================================================
```

```
PW Template Information
===============================================================================
PW Tmpl Id           : 1
Use Provisioned Sdp  : enabled             VcType           : vlan
Acctg Policy         : default             Collect Stats    : disabled
Mac-Learning         : enabled             Mac-Ageing       : enabled
Discard Unkn Src     : disabled            Limit MacMove    : blockable
Mac-Pinning          : disabled            Vlan VcTag       : 4095
MAC Address Limit    : no limit            Rest Prot Src Mac: disabled
Auto Learn Mac Prot  : disabled            RestProtSrcMacAct: disable
Block On Peer Fault  : disabled

SHG
Name                 :
Description          : (Not Specified)
Rest Prot Src Mac    : disabled            Rest Unprot Dst  : disabled
Auto Learn Mac Prot  : disabled            RestProtSrcMacAct: disable

Egress
Mac FilterId         : none                Ip FilterId      : none
Ipv6 FilterId        : none                QoS NetPlcyId    : none
Port RedirectQGrp    : none                Instance Id      : none

Ingress
Mac FilterId         : none                Ip FilterId      : none
Ipv6 FilterId        : none                QoS NetPlcyId    : none
Fp RedirectQGrp      : none                Instance Id      : none

IGMP
Fast Leave           : disabled            Import Plcy      : none
Last Memb Intvl      : 10 deci-secs        Max Nbr Grps     : 0
Send Queries         : disabled
Version              : 3

Force VlanVc Fwd     : disabled            Control Word     : disabled
Hash Label           : disabled            Hash Lbl Sig Cap : disabled
Last Changed         : 02/12/2013 22:11:49
-------------------------------------------------------------------------------
Included SDP-Groups
-------------------------------------------------------------------------------
red
-------------------------------------------------------------------------------
```

saii-type2-using

Syntax

saii-type2-using *global-id*[**:***prefix*[**:***ac-id*]]

Context

show>service

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays the SDP used by a spoke-SDP FEC with a specified FEC129 Type 2 SAII.

Parameters

global-id[:prefix[:ac-id]]

Specifies the switch-point information using SAII-Type2.

Values <global-id[:prefix*> : <global-id>[:<prefix>[:<ac-id>]] global-id 1..4294967295 prefix a.b.c.d | 1..4294967295 ac-id 1..4294967295

Output

The following output is an example of information for a spoke-SDP FEC using FEC129 Type 2 SAII.

Sample output

```
*A:Dut-E# show service saii-type2-using 3:10.20.1.3:1
===============================================================================
Service Switch-Point Information
===============================================================================
SvcId      Oper-SdpBind      SAII-Type2
-------------------------------------------------------------------------------
2147483598 17407:4294967195  3:10.20.1.3:1
-------------------------------------------------------------------------------
Entries found: 1
===============================================================================
```

spoke-sdp-fec-using

Syntax

spoke-sdp-fec-using [**spoke-sdp-fec-id <***spoke-sdp-fec-id***>**] [**saii-type2 <***global-id:prefix:ac-id***>**] [**taii-type2 <***global-id:prefix:ac-id***>**] [**path <***name***>**] [**expired**] **taii-type2-using** *global-id*[*:prefix*[*:ac-id*]]

Context

show>service

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays the SDPs used by spoke-SDP FECs at this node.

Output

The following output is an example of information for spoke-SDP FECs using SDPs.

Sample output

```
*A:Dut-C# show service spoke-sdp-fec-using
===============================================================================
Service Spoke-SDP-Fec Information
```

```
===============================================================================
SvcId SpokeSdpFec Oper-SdpBind SAII-Type2
Path TAII-Type2
-------------------------------------------------------------------------------
1 1 17407:4294967245 3:10.20.1.3:1
n/a 6:10.20.1.6:1
2 2 17407:4294967247 3:10.20.1.3:2
n/a 6:10.20.1.6:2
3 3 17407:4294967248 3:10.20.1.3:3
n/a 6:10.20.1.6:3
4 4 17407:4294967249 3:10.20.1.3:4
n/a 6:10.20.1.6:4
5 5 17407:4294967250 3:10.20.1.3:5
n/a 6:10.20.1.6:5
6 6 17407:4294967251 3:10.20.1.3:6
n/a 6:10.20.1.6:6
7 7 17407:4294967252 3:10.20.1.3:7
n/a 6:10.20.1.6:7
8 8 17407:4294967253 3:10.20.1.3:8
n/a 6:10.20.1.6:8
9 9 17407:4294967254 3:10.20.1.3:9
n/a 6:10.20.1.6:9
10 10 17407:4294967255 3:10.20.1.3:10
n/a 6:10.20.1.6:10
-------------------------------------------------------------------------------
Entries found: 10
===============================================================================
```

taii-type2-using

Syntax

taii-type2-using *global-id*[**:***prefix*[**:***ac-id*]]

Context

show>service

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays switch-point information using TAII.

Parameters

global-id[:prefix[:ac-id]]

Specifies the switch-point information using SAII-Type2.

Values <global-id[:prefix*> : <global-id>[:<prefix>[:<ac-id>]] global-id 1..4294967295 prefix a.b.c.d | 1..4294967295 ac-id 1..4294967295

Output

The following output is an example of information for switch-point using TAII.

Sample output

```
*A:Dut-E# show service taii-type2-using 6:10.20.1.6:1
===============================================================
Service Switch-Point Information
===============================================================
SvcId      Oper-SdpBind      TAII-Type2
---------------------------------------------------------------
2147483598 17407:4294967195  6:10.20.1.6:1
---------------------------------------------------------------
Entries found: 1
===============================================
```

2.13.2.2.2 ETH-CFM show commands

eth-cfm

Syntax

eth-cfm

Context

show

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays ETH-CFM information.

eth-tunnel

Syntax

eth-tunnel

Context

show

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays Ethernet tunnel information. Any data SAP missing a tag for a defined path has the EthTunTagMismatch flag generated. In the following example, SAP eth-tunnel-1:1 does not have the tag for

path 2 configured. Therefore, it is operationally down with the reason indicated by the EthTunTagMismatch flag.

association

Syntax

association [*ma-index*] [**detail**]

Context

show>eth-cfm

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays eth-cfm association information.

Parameters

ma-index

Specifies the maintenance association (MA) index.

Values 1 to 4294967295

detail

Displays more information for the ETH-CFM association.

Output

The following output is an example of Ethernet CFM association information, and Table 18: Output fields: ETH CFM association describes the output fields.

Sample output

```
A:dut-b# show eth-cfm association

===============================================================================
CFM Association Table
===============================================================================
Md-index   Ma-index   Name                    CCM-interval Bridge-id
-------------------------------------------------------------------------------
1          1          a1                      1            1
1          2          a2                      1            2
2          1          a1                      1            2
2          2          a2                      1            1
===============================================================================
A:dut-b#
```

Table 18: Output fields: ETH CFM association

Label	Description
Md-index	Displays the maintenance domain (MD) index.
Ma-index	Displays the maintenance association (MA) index.
Name	Displays the part of the maintenance association identifier which is unique within the maintenance domain name.
CCM-interval	Displays the CCM transmission interval for all MEPs in the association.
Bridge-id	Displays the bridge-identifier value for the domain association.
MHF Creation	Displays the MIP half function (MHF) for the association.
Primary VLAN	Displays the primary bridge-identifier VLAN ID.
Num Vids	Displays the number of VIDs associated with the VLAN.
Remote Mep Id	Displays the remote maintenance association endpoint (MEP) identifier.

cfm-stack-table

Syntax

cfm-stack-table [{**all-ports**}] [**level <0..7>**] [**direction <down>**]

cfm-stack-table port <port-id> [**vlan <qtag**[**.qtag**]**>**] [**level <0..7>**] [**direction <down>**]

cfm-stack-table facility [{**all-ports** | **all-lags** | **all-lag-ports** | **all-tunnel-meps** | **all-router-interfaces**}] [**level <0..7>**] [**direction <down>**]

cfm-stack-table facility lag <*id***>** [**tunnel <1..4094>**] [**level <0..7>**] [**direction <down>**]

cfm-stack-table facility port <*id***>** [**level <0..7>**] [**direction <down>**]

cfm-stack-table facility router-interface <*ip-int-name***>** [**level <0..7>**] [**direction <down>**]

Context

show>eth-cfm

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays stack-table information. This stack-table is used to display the various management points MEPs and MIPs that are configured on the system. This can be service based. The

options allow the user to display specific information. If no parameters are included, the entire stack-table is displayed.

Parameters

port *port-id*

Displays the bridge port or aggregated port on which MEPs or MHFs are configured.

vlan *vlan-id*

Displays the associated VLAN ID.

level

Displays the MD level of the maintenance point.

Values 0 to 7

direction down

Displays the direction in which the MP faces on the bridge port.

Output

The following output is an example of Ethernet CFM stack table information, and Table 19: Output fields: ETH-CFM CFM stack table describes the output fields.

Sample output

```
*A:7210SAS>show>eth-cfm# cfm-stack-table

===============================================================================
CFM SAP Stack Table
===============================================================================
Sap            Level Dir  Md-index   Ma-index   Mep-id Mac-address
-------------------------------------------------------------------------------
1/1/18:100     7     Up   7          100        1      00:25:ba:0d:21:13
===============================================================================

===============================================================================
CFM Ethernet Tunnel Stack Table
===============================================================================
Eth-tunnel     Level Dir  Md-index   Ma-index   Mep-id Mac-address
-------------------------------------------------------------------------------
No Matching Entries
===============================================================================

===============================================================================
CFM SDP Stack Table
===============================================================================
Sdp            Level Dir  Md-index   Ma-index   Mep-id Mac-address
-------------------------------------------------------------------------------
No Matching Entries
===============================================================================

===============================================================================
CFM Virtual Stack Table
===============================================================================
Service        Level Dir  Md-index   Ma-index   Mep-id Mac-address
-------------------------------------------------------------------------------
No Matching Entries
===============================================================================
*A:7210SAS>show>eth-cfm#
```

Sample for 7210 SAS-R6 and 7210 SAS-R12 IMMv2:

```
*A:7210SAS>show>eth-cfm# cfm-stack-table

===============================================================================
CFM SAP Primary VLAN Stack Table
===============================================================================
Sap
  Primary VlanId Lvl Dir Md-index Ma-index MepId Mac-address Defect
-------------------------------------------------------------------------------
lag-2:1
     200 7 Both 10 1 MIP 00:11:11:11:11:11 ------
lag-2:2
     200 7 Both 10 2 MIP 00:11:11:11:11:12 ------
lag-2:3

*A:7210SAS>show>
```

Table 19: Output fields: ETH-CFM CFM stack table

Label	Description
Sap	Displays associated SAP IDs
Sdp	Displays the SDP binding for the bridge
Level Dir	Displays the MD level of the maintenance point
Md-index	Displays the maintenance domain (MD) index
Ma-index	Displays the maintenance association (MA) index
Mep-id	Displays the integer that is unique among all the MEPs in the same MA
Mac-address	Displays the MAC address of the MP

domain

Syntax

domain [*md-index*] [**association** *ma-index* | **all-associations**] [**detail**]

Context

show>eth-cfm

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays domain information.

Parameters

md-index

Displays the index of the MD to which the MP is associated, or 0, if none.

association ma-index

Displays the index to which the MP is associated, or 0, if none.

all-associations

Displays all associations to the MD.

detail

Displays detailed domain information.

Output

The following output is an example of Ethernet CFM domain information, and Table 20: Output fields: ETH-CFM domain describes the output fields.

Sample output

```
A:dut-b# show eth-cfm domain

===============================================================================
CFM Domain Table
===============================================================================
Md-index   Level Name                                          Format
-------------------------------------------------------------------------------
1          6     d1                                          charString
2          7     d2                                          charString
===============================================================================
A:dut-b#
```

Table 20: Output fields: ETH-CFM domain

Label	Description
Md-index	Displays the Maintenance Domain (MD) index value
Level	Displays an integer identifying the Maintenance Domain Level (MD Level). Higher numbers correspond to higher Maintenance Domains, those with the greatest physical reach, with the highest values for customers' CFM PDUs. Lower numbers correspond to lower Maintenance Domains, those with more limited physical reach, with the lowest values for CFM PDUs protecting single bridges or physical links.
Name	Displays a generic Maintenance Domain (MD) name
Format	Displays the type of the Maintenance Domain (MD) name. Values include **dns**, **mac**, and **string**.

mep

Syntax

mep *mep-id* **domain** *md-index* **association** *ma-index* [**loopback**] [**linktrace**]

mep *mep-id* **domain** *md-index* **association** *ma-index* **remote-mepid** *mep-id* | **all-remote-mepids**

mep *mep-id* **domain** *md-index* **association** *ma-index* **eth-test-results** [**remote-peer** *mac-address*]

mep *mep-id* **domain** *md-index* **association** *ma-index* **one-way-delay-test** [**remote-peer** *mac-address*]

mep*mep-id* **domain** *md-index* **association** *ma-index* **two-way-delay-test** [**remote-peer** *mac-address*]

mep *mep-id* **domain** *md-index* **association** *ma-index* **two-way-slm-test** [**remote-peer** *macaddress*]

Context

show>eth-cfm

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays Maintenance Endpoint (MEP) information.

Note:

- The **show eth-cfm mep** *mep-id* **domain** *md-id* **association** *ma-id* command does not display CCM ERROR, CCM XCON frames in the output.
- The **show eth-cfm mep** *mep-id* **domain** *md-id* **association** *ma-id* **remote-mep** *rmep-id* command does not display some TLVs details.

Parameters

mep-id

Displays the integer that is unique among all the MEPs in the same MA.

domain *md-index*

Displays the index of the MD to which the MP is associated, or 0, if none.

association *ma-index*

Displays the index to which the MP is associated, or 0, if none.

loopback

Displays loopback information for the specified MEP.

linktrace

Displays linktrace information for the specified MEP.

remote-mepid *mep-id*

Includes specified remote mep-id information for specified the MEP.

all-remote-mepids

Includes all remote mep-id information for the specified MEP.

eth-test-results

Includes eth-test-result information for the specified MEP.

one-way-delay-test

Includes one-way-delay-test information for the specified MEP.

two-way-delay-test

Includes two-way-delay-test information for the specified MEP.

two-way-slm-test

Includes two-way-slm-test information for the specified MEP.

remote-peer *mac-address*

Includes specified remote mep-id information for the specified MEP.

Output

The following outputs are examples of MEP information, and Table 21: Output fields: MEP describes the output fields.

Sample output

```
A:dut-b# show eth-cfm mep 1 domain 1 association 1 linktrace
-------------------------------------------------------------------------------
Mep Information
-------------------------------------------------------------------------------
Md-index           : 1                       Direction         : Down
Ma-index           : 1                       Admin             : Enabled
MepId              : 1                       CCM-Enable        : Enabled
IfIndex            : 35946496                PrimaryVid        : 1
FngState           : fngReset                ControlMep        : False
LowestDefectPri    : macRemErrXcon           HighestDefect     : none
Defect Flags       : None
Mac Address        : 00:25:ba:01:c3:6a       CcmLtmPriority    : 7
CcmTx              : 0                       CcmSequenceErr    : 0
Eth-1Dm Threshold  : 3(sec)
Eth-Ais:           : Disabled
Eth-Tst:           : Disabled
CcmLastFailure Frame:
    None
XconCcmFailure Frame:
    None
-------------------------------------------------------------------------------
Mep Linktrace Message Information
-------------------------------------------------------------------------------
LtRxUnexplained    : 0                       LtNextSequence    : 2
LtStatus           : False                   LtResult          : False
TargIsMepId        : False                   TargMepId         : 0
TargMac            : 00:00:00:00:00:00       TTL               : 64
EgressId           : 00:00:00:25:ba:01:c3:6a SequenceNum       : 1
LtFlags            : useFDBonly
-------------------------------------------------------------------------------
Mep Linktrace Replies
-------------------------------------------------------------------------------
SequenceNum        : 1                       ReceiveOrder      : 1
Ttl                : 63                      Forwarded         : False
LastEgressId       : 00:00:00:25:ba:01:c3:6a TerminalMep       : True
NextEgressId       : 00:00:00:25:ba:00:5e:bf Relay             : rlyHit
ChassisIdSubType   : unknown value (0)
ChassisId:
    None
```

```
ManAddressDomain:
    None
ManAddress:
    None
IngressMac          : 00:25:ba:00:5e:bf        Ingress Action    : ingOk
IngrPortIdSubType   : unknown value (0)
IngressPortId:
    None
EgressMac           : 00:00:00:00:00:00        Egress Action     : egrNoTlv
EgrPortIdSubType    : unknown value (0)
EgressPortId:
    None
Org Specific TLV:
    None
A:dut-b#
A:dut-b#

A:dut-b# show eth-cfm mep 1 domain 1 association 1 loopback
-------------------------------------------------------------------------------
Mep Information
-------------------------------------------------------------------------------
Md-index            : 1                        Direction         : Down
Ma-index            : 1                        Admin             : Enabled
MepId               : 1                        CCM-Enable        : Enabled
IfIndex             : 35946496                 PrimaryVid        : 1
FngState            : fngReset                 ControlMep        : False
LowestDefectPri     : macRemErrXcon            HighestDefect     : none
Defect Flags        : None
Mac Address         : 00:25:ba:01:c3:6a        CcmLtmPriority    : 7
CcmTx               : 0                        CcmSequenceErr    : 0
Eth-1Dm Threshold   : 3(sec)
Eth-Ais:            : Disabled
Eth-Tst:            : Disabled
CcmLastFailure Frame:
    None
XconCcmFailure Frame:
    None
-------------------------------------------------------------------------------
Mep Loopback Information
-------------------------------------------------------------------------------
LbRxReply           : 1                        LbRxBadOrder      : 0
LbRxBadMsdu         : 0                        LbTxReply         : 0
LbSequence          : 2                        LbNextSequence    : 2
LbStatus            : False                    LbResultOk        : True
DestIsMepId         : False                    DestMepId         : 0
DestMac             : 00:00:00:00:00:00        SendCount         : 0
VlanDropEnable      : True                     VlanPriority      : 7
Data TLV:
    None
A:dut-b#


*A:dut-b# show eth-cfm mep 1 domain 4 association 4 two-way-delay-test remote-
peer 00:25:ba:00:5e:bf

===============================================================
Eth CFM Two-way Delay Test Result Table
===============================================================
Peer Mac Addr         Delay (us)          Delay Variation (us)
---------------------------------------------------------------
00:25:ba:00:5e:bf     507                 507
===============================================================
*A:dut-b#
```

```
*A:dut-b# show eth-cfm mep 1 domain 4 association 4 two-way-delay-test

===============================================================
Eth CFM Two-way Delay Test Result Table
===============================================================
Peer Mac Addr         Delay (us)          Delay Variation (us)
---------------------------------------------------------------
00:25:ba:00:5e:bf     507                 507
===============================================================
*A:dut-b#

*A:dut-a# show eth-cfm mep 2 domain 4 association 4  eth-test-results remote-
peer 00:25:ba:01:c3:6a

===============================================================
Eth CFM ETH-Test Result Table
===============================================================
                                Current        Accumulate
                  FrameCount    ErrBits        ErrBits
Peer Mac Addr     ByteCount     CrcErrs        CrcErrs
---------------------------------------------------------------
00:25:ba:01:c3:6a 6             0              0
                  384           0              0
===============================================================
*A:dut-a#

*A:dut-a# show eth-cfm mep 2 domain 4 association 4  eth-test-results

===============================================================
Eth CFM ETH-Test Result Table
===============================================================
                                Current        Accumulate
                  FrameCount    ErrBits        ErrBits
Peer Mac Addr     ByteCount     CrcErrs        CrcErrs
---------------------------------------------------------------
00:25:ba:01:c3:6a 6             0              0
                  384           0              0
===============================================================

*A:dut-a# show eth-cfm mep 2 domain 4 association 4 one-way-delay-test remote-
peer 00:25:ba:01:c3:6a

===============================================================
Eth CFM One-way Delay Test Result Table
===============================================================
Peer Mac Addr         Delay (us)          Delay Variation (us)
---------------------------------------------------------------
00:25:ba:01:c3:6a     402                 402
===============================================================
*A:dut-a#


*A:dut-a# show eth-cfm mep 2 domain 4 association 4 one-way-delay-test

===============================================================
Eth CFM One-way Delay Test Result Table
===============================================================
Peer Mac Addr         Delay (us)          Delay Variation (us)
---------------------------------------------------------------
00:25:ba:01:c3:6a     402                 402
===============================================================
*A:dut-a#
```

Sample output for two-way-slm-test

```
*A:7210SAS# show eth-cfm mep 1 domain 7 association 100 two-way-slm-test
===============================================================================
Eth CFM Two-way SLM Test Result Table (Test-id: 1)
===============================================================================
Peer Mac Addr      Remote MEP       Count     In Loss    Out Loss         Unack
-------------------------------------------------------------------------------
00:25:ba:0d:1e:12          2           1           0           0            0
===============================================================================
*A:7210SAS#
```

Table 21: Output fields: MEP

Label	Description
Mep Information	
Md-index	Displays the MD index of the domain.
Direction	Displays the direction of OAMPDU transmission.
Ma-index	Displays the MA index of the association.
Admin	Displays the administrative status of the MEP.
MepId	Displays the MEP identifier.
CCM-Enable	Displays the status of the CCM (enabled or disabled).
IfIndex	Displays the index of the interface.
PrimaryVid	Displays the identifier of the primary VLAN.
FngState	Indicates the different states of the Fault Notification Generator.
LowestDefectPri	Displays the lowest priority defect (a configured value) that is allowed to generate a fault alarm.
HighestDefect	Identifies the highest defect that is present (for example, if defRDICCM and defXconCCM are present, the highest defect is defXconCCM).
Defect Flags	Displays the number of defect flags.
Mac Address	Displays the MAC address of the MEP.
CcmLtmPriority	Displays the priority value transmitted in the linktrace messages (LTM)s and CCMs for this MEP. The MEP must be configured on a VLAN.
CcmTx	Displays the number of Continuity Check Messages (CCM) sent. The count is taken from the last polling interval (every 10 s).

Label	Description
CcmSequenceErr	Displays the number of CCM errors.
Eth-1DM Threshold	Displays the one-way-delay threshold value.
Eth-Ais	Displays the state of the ETH-AIS test (enabled or disabled).
Eth-Test	Displays the state of the ETH-Test (enabled or disabled).
CcmLastFailure Frame	Displays the frame that caused the last CCM failure.
XconCcmFailure Frame	Displays the frame that caused the XconCCMFailure.
Mep Loopback Information	
LbRxReply	Displays the number of received loopback (LB) replies.
LbRxBadOrder	Displays the number of received loopback messages that are in a bad order.
LbRxBadMsdu	Displays the number of loopback replies that have been received with the wrong destination MAC address (MSDU = MAC Service Data Unit).
LbTxReply	Displays the number of loopback replies transmitted out this MEP.
LbTxReply (Total)	Displays the total number of LBRs (loopback replies) transmitted from this MEP.
LbTxReplyNoTLV	Displays the number of LBRs (loopback replies) transmitted from this MEP with no TLV. Because only LBMs with no TLVs are used for throughput testing, the LbTxReply (Total), LbTxReplyNoTLV, and LbTxReplyWithTLV counters can help debug problems if throughput testing is not working.
LbTxReplyWithTLV	Displays the number of LBRs (loopback replies) transmitted from this MEP with TLV.
LbSequence	Displays the sequence number in the loopback message.
LbNextSequence	Displays the next loopback sequence.
LbStatus	Displays the loopback status as True or False: True — loopback is in progress False — no loopback is in progress
LbResultOk	Displays the result of the loopback test.
DestIsMepId	Identifies whether the destination interface has a MEP-ID (true or false).

Label	Description
DestMepId	Displays the MEP-ID of the destination interface.
DestMac	Displays the MAC address of the destination interface.
SendCount	Indicates the number of loopback messages sent.
VlanDropEnable	Identifies whether the VLAN drop is enabled (true or false).
VlanPriority	Displays the VLAN priority.
Data TLV	Displays the data TLV information.
Mep Linktrace Message Information	
LtRxUnexplained	Displays the number of unexplained linktrace messages (LTM) that have been received.
LtNextSequence	Displays the sequence number of the next linktrace message.
LtStatus	Displays the status of the linktrace.
LtResult	Displays the result of the linktrace.
TargIsMepId	Identifies whether the target interface has a MEP-ID (true or false).
TargMepId	Displays the MEP-ID of the target interface.
TargMac	Displays the MAC address of the target interface.
TTL	Displays the TTL value.
EgressId	Displays the egress ID of the linktrace message.
SequenceNum	Displays the sequence number of the linktrace message.
LtFlags	Displays the linktrace flags.
Mep Linktrace Replies	
SequenceNum	Displays the sequence number returned by a previous transmit linktrace message, indicating which linktrace message response will be returned.
ReceiveOrder	Displays the order in which the linktrace initiator received the linktrace replies.
Ttl	Displays the TTL field value for a returned linktrace reply.
Forwarded	Indicates whether the linktrace message was forwarded by the responding MEP.

Label	Description
LastEgressId	Displays the last egress identifier returned in the linktrace reply egress identifier TLV of the linktrace reply. The last egress identifier identifies the MEP linktrace initiator that initiated, or the linktrace responder that forwarded, the linktrace message for which this linktrace reply is the response. This is the same value as the egress identifier TLV of that linktrace message.
TerminalMep	Indicates whether the forwarded linktrace message reached a MEP enclosing its MA.
NextEgressId	Displays the next egress identifier returned in the linktrace reply egress identifier TLV of the linktrace reply. The next egress identifier identifies the linktrace responder that transmitted this linktrace reply and can forward the linktrace message to the next hop. This is the same value as the egress identifier TLV of the forwarded linktrace message, if any.
Relay	Displays the value returned in the Relay Action field.
ChassisIdSubType	Displays the format of the chassis ID returned in the Sender ID TLV of the linktrace reply, if any. This value is meaningless if the chassis ID has a length of 0.
ChassisId	Displays the chassis ID returned in the Sender ID TLV of the linktrace reply, if any. The format is determined by the value of the ChassisIdSubType.
ManAddressDomain	Displays the TDomain that identifies the type and format of the related ManAddress, used to access the SNMP agent of the system transmitting the linktrace reply. Received in the linktrace reply Sender ID TLV from that system.
ManAddress	Displays the TAddress that can be used to access the SNMP agent of the system transmitting the CCM. Received in the CCM Sender ID TLV from that system.
IngressMac	Displays the MAC address returned in the ingress MAC address field.
Ingress Action	Displays the value returned in the Ingress Action field of the linktrace message.
IngressPortIdSubType	Displays the format of the ingress port ID.
IngressPortId	Displays the ingress port ID; the format is determined by the value of the IngressPortIdSubType.

Label	Description
EgressMac	Displays the MAC address returned in the egress MAC address field.
Egress Action	Displays the value returned in the Egress Action field of the linktrace message.
EgressPortIdSubType	Displays the format of the egress port ID.
EgressPortId	Displays the egress port ID; the format is determined by the value of the EgressPortIDSubType.
Org Specific TLV	Displays all organization-specific TLVs returned in the linktrace reply, if any. Includes all octets including and following the TLV length field of each TLV, concatenated.
Eth-Test	
Peer Mac Addr	Displays the MAC address of the peer (remote) entity.
FrameCount	Displays the number of test frames sent between the MEP and the peer entity.
ByteCount	Displays the number of bytes sent between the MEP and the peer entity.
Current ErrBits	Displays the number of bit errors in the current test.
Current CrcErrs	Displays the number of CRC errors in the current test.
Accumulate ErrBits	Displays the accumulated number of bit errors in the current test.
Accumulate CrcErrs	Displays the accumulated number of CRC errors in the current test.
Delay Measurement Test	
Peer Mac Addr	Displays the MAC address of the peer (remote) entity.
Delay (us)	Displays the measured delay (in microseconds) for the DM test.
Delay Variation (us)	Displays the measured delay variation (in microseconds) for the DV test.

mip

Syntax

mip

Context

show>eth-cfm>mip

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays Maintenance Intermediate Point (MIP) information.

Output

The following output is an example of MIP information, and Table 22: Output fields: MIP describes the output fields.

Sample output

```
*A:7210SAS#  show eth-cfm mip
===============================================================================
CFM SAP MIP Table
===============================================================================
Sap                                   Mip-Enabled     Mip Mac Address
-------------------------------------------------------------------------------
1/1/16                                yes             00:a1:b1:c1:d1:e1
===============================================================================
===============================================================================
CFM SDP MIP Table
===============================================================================
Sdp                                   Mip-Enabled     Mip Mac Address
-------------------------------------------------------------------------------
456:123                               yes             00:a2:b2:c2:d2:e2
===============================================================================
*A:7210SAS#
```

Table 22: Output fields: MIP

Label	Description
Mip-Enabled	Displays the state of the MIP service
Mip Mac Address	Displays the MAC address of the MIP

connection-profile

Syntax

connection-profile [*conn-prof-id*] [**associations**]

Context

show

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays connection profile information.

Parameters

conn-prof-id

Specifies the connection profile ID.

Values 1 to 8000

associations

Displays the SAP and the service ID that use this connection profile.

Output

The following outputs are examples of connection profile information, and Table 23: Output fields: connection profile describes the output fields.

- Sample output
- Sample output for connection-profile associations

Sample output

```
*7210SAS>show# connection-profile

===============================================================================
Connection Profile Summary Information
===============================================================================
CP Index  Number of HasRange
          Members
-------------------------------------------------------------------------------
1         0         Yes
2         0         Yes
3         0         Yes
5         0         Yes
6         0         Yes
100       0         Yes
200       0         Yes
300       0         Yes
400       0         Yes
500       0         Yes
600       0         Yes
700       0         Yes
800       0         Yes
900       0         Yes
===============================================================================
*7210SAS>show#
```

Sample output for connection-profile associations

```
*A:7210SAS>show# connection-profile associations

===============================================================================
Connection Profile Summary Information
===============================================================================
CP Index  Number of HasRange
          Members
-------------------------------------------------------------------------------
1         0         No
```

```
===============================================================================
*A:7210SAS>show#
```

Table 23: Output fields: connection profile

Label	Description
CP Index	Identifies the connection-profile.
Number of Members	Indicates the number of ATM connection profile members not applicable for 7210 SAS.
HasRange	Indicates whether VLAN range is configured.

2.13.2.3 Tools perform commands

tools

Syntax

tools

Context

root

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

Commands in this context enable tools for debugging purposes.

Parameters

dump

Enables dump tools for the various protocols.

perform

Enables tools to perform specific tasks.

perform

Syntax

perform

Context

tools

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

Commands in this context enable tools to perform specific tasks.

service

Syntax

service

Context

tools>perform

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

Commands in this context configure tools for services.

id

Syntax

id *service-id*

Context

tools>perform>service

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configured tools for a specific service.

Parameters

service-id

Specifies an existing service ID.

Values 1 to 2147483647

endpoint

Syntax

endpoint *endpoint-name*

Context

tools>perform>service>id

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures tools for a specific VLL service endpoint.

Parameters

endpoint-name

Specifies an existing VLL service endpoint name.

force-switchover

Syntax

force-switchover *sdp-id:vc-id*

no force-switchover

force-switchover spoke-sdp-fec [*1..4294967295*]

Context

tools>perform>service>id>endpoint

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command forces a switch of the active spoke-SDP for the specified service.

Parameters

sdp-id:vc-id

Specifies an existing spoke-SDP for the service.

spoke-sdp-fec spoke-sdp-fec-id

The spoke-sdp-fec-id for a FEC129 AII Type 2 spoke-sdp. This parameter and sdp:vc-id used for a FEC 128 spoke-sdp are mutually exclusive.

Sample output

```
*A:Dut-B# show service id 1 endpoint
===============================================================================
Service 1 endpoints
===============================================================================
Endpoint name : mcep-t1
Description : (Not Specified)
Revert time : 0
Act Hold Delay : 0
Ignore Standby Signaling : false
Suppress Standby Signaling : false
Block On Mesh Fail : true
Multi-Chassis Endpoint : 1
MC Endpoint Peer Addr : 10.1.1.3
Psv Mode Active : No
Tx Active : 221:1(forced)
Tx Active Up Time : 0d 00:00:17
Revert Time Count Down : N/A
Tx Active Change Count : 6
Last Tx Active Change : 02/14/2009 00:17:32
-------------------------------------------------------------------------------
Members
-------------------------------------------------------------------------------
Spoke-sdp: 221:1 Prec:1 Oper Status: Up
Spoke-sdp: 231:1 Prec:2 Oper Status: Up
===============================================================================
*A:Dut-B#
```

eval-pw-template

Syntax

eval-pw-template

Context

tools>perform>service

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command reevaluates the pseudowire template policy.

Parameters

policy-id

Specifies the pseudowire template policy.

eval-expired-fec

Syntax

eval-expired-fec spoke-sdp-fec-id

eval-expired-fec all

Context

tools>perform>service>pw-routing

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command resets the retry counter and retry timer for the specified spoke-SDP and attempts to reestablish the spoke-SDP.

spoke-sdp-fec-release

Syntax

spoke-sdp-fec-release *global-id*[*:prefix*[*:ac-id*]]

Context

tools>perform>service

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command clears the MS-PW bindings associated with particular SAII or TAII on an S-PE.

3 VLL services

This section provides information about Virtual Leased Line (VLL) services and implementation notes.

3.1 Ethernet pipe (Epipe) services

This section provides information about the Epipe service and implementation notes.

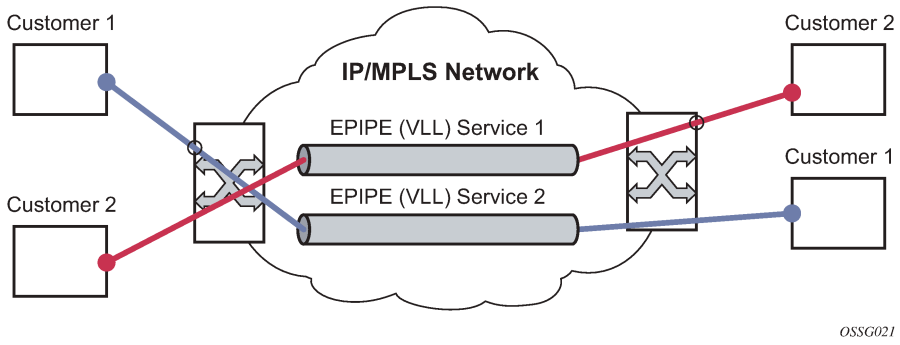
3.1.1 Epipe service overview

An Epipe service is a Layer 2 point-to-point service where the customer data is encapsulated and transported across a service provider network. An Epipe service is completely transparent to the subscriber data and protocols. The Epipe service does not perform any MAC learning. A local Epipe service consists of two SAPs on the same node, whereas a distributed Epipe service consists of two SAPs on different nodes.

Each SAP configuration includes a specific port on which service traffic enters the 7210 SAS from the customer side (also called the access side). Each port is configured with an encapsulation type. If a port is configured with an IEEE 802.1Q (referred to as dot1q) encapsulation, then a unique encapsulation value (ID) must be specified.

The following figure shows Epipe/VLL service.

Figure 14: Epipe/VLL service



3.1.2 Support for processing of packets received with more than 2 tags on a QinQ SAP in Epipe service (only on 7210 SAS devices configured in network mode)

To forward packets with 2 or more tags using a QinQ SAP, a new Epipe service type is available for use when 7210 SAS devices are operating in 'network' mode. This new service allows for configuration of a QinQ SAP as one endpoint and the following service entities as the other endpoint:

- MPLS spoke-SDP with **vc-type** set to **vc-vlan**: The VC VLAN tag to be must match the inner tag VLAN ID value specified in the QinQ SAP.
- dot1q SAP: The VLAN value configured for the dot1q SAP must match the inner-tag VLAN ID value of the QinQ SAP.
- QinQ SAP: The inner VLAN tag of both QinQ SAPs configured in the service must be the same.

The device processes the packet as follows in the forward direction:

- If the packet is received on a QinQ SAP, assign an incoming packet to this service based on matching the outermost two tags in the packet header (that is, the first two tags in the packet header). It strips only the outermost tag (only a single tag) on ingress and forward the rest on to the other endpoint in the service (as follows).
- If the other endpoint the packet is sent out of is a MPLS SDP, then MPLS encapsulation is added.
- If the other endpoint the packet is sent out of is a dot1q SAP packet is forwarded as is, without any egress VLAN checks. The operator must ensure the inner tag of the packet matches the dot1q VLAN value.
- If the other endpoint the packet is sent out of is another QinQ SAP (for example, Q1.Q2 SAP), then another tag (that is, Q2 tag) is added to the packet and sent out of the QinQ SAP.

In the reverse direction, the device processes the packet as follows:

- When traffic is received on the MPLS SDP, the VC VLAN tag is retained as is and the VLAN tag corresponding to the outermost tag configured for the QinQ SAP (that is, the other endpoint) is added to the packet. The system does not match the VC VLAN tag received in the packet with the configured value (that is, the inner tag of the QinQ SAP). The operator must configure both ends of the service appropriately to ensure only appropriate packets enter the service.
- When traffic is received on the dot1q SAP, the outermost tag is stripped and the VLAN tag corresponding to the outermost tag configured for the QinQ SAP is added to the packet.
- If the packet is received on a QinQ SAP, assign an incoming packet to this service based on matching the outermost two tags in the packet header (that is, that is, the first two tags in the packet header). It strips only the outermost tag (only a single tag) on ingress. The VLAN tag corresponding to the outermost tag configured for the QinQ SAP (that is, the other endpoint) is added to the packet and it is sent out of the QinQ SAP.

Therefore, the device processes packets received with 2 or more tags using the MPLS SDP or a dot1q SAP while classifying on the QinQ SAP ingress using 2 tags.

3.1.3 Feature support, configuration notes and restrictions

A new **svc-sap-type** value **qinq-inner-tag-preserve** is available for configuring the service. This must be used when creating a new Epipe service if this functionality is desired (For example: **epipe 10 svc-sap-type qinq-inner-tag-preserve create**):

- This service is available only in network mode.
- Epipe service created with the parameter **svc-sap-type** set to **qinq-inner-tag-preserve** allows for only one QinQ SAP and only one SDP of **vc-type vc-vlan**. The system does not allow the user to use any other SAP in this new service, that is, NULL SAP, Q1. * SAP, 0.* SAP, and so on, are not allowed for configuration in this service. The SDP cannot be of **vc-type vc-ether**.
- User can configure vlan-vc-tag value for the SDP, the dot1q SAP VLAN tag value and the inner tag VLAN value of a QinQ SAP to match the VLAN ID value of the inner tag specified in the Q1.Q2 SAP

configured in the service (example: if the SAP is 1/1/10:Q1.Q2, then vlan-vc-tag must be set to Q2, the dot1q SAP VLAN value must be Q2, and the inner tag of another QinQ SAP must be set to Q2). If any other value, other than QinQ SAP's inner tag is configured for vlan-vc-tag or dot1q SAP VLAN value, or for the inner tag of the QinQ SAP then it is errored out by the software. If **vlan-vc-tag** value is not configured, it defaults to use the inner VLAN tag value. It is highly recommended that the customer configure the **vlan-vc-tag** value to match the VLAN ID value of the inner tag configured for the QinQ SAP, to avoid mis-configuration.

- Existing QoS and ACL functionality for the Epipe service entities continues to be available, with the following exceptions:
  - If the packet is received with more than 2 tags, then IP match-criteria cannot be used with SAP ingress QoS classification and ACLs (both Ingress and Egress ACLs).
  - If the packet is received with more than 2 tags, then Ethertype value in the mac-criteria cannot be used with SAP ingress QoS classification and ACLs (both Ingress and Egress ACLs).
  - Dot1p bits from the outermost tag (that is, Q1 VLAN tag, if the SAP is 1/1/10:Q1.Q2) are used for SAP ingress classification. Dot1p bits of the outermost tag are marked on egress, if marking is enabled on the egress port. The Dot1p bit value of the **vlan-vc-tag** is not used to mark the Dot1p bits of the outermost VLAN tag, when the packets is exiting the QinQ SAP.
- OAM tools:
  - MPLS OAM tools such as VCCV ping and VCCV trace are supported for the SDPs
  - Accounting and Statistics for the service entities (for example, SAP and SDP) are available as before
  - CFM/Y.1731 tools are supported. UP and Down MEP is supported on the SAPs and the SDPs configured in the Epipe service.
- The following Redundancy mechanisms available in Epipe service are supported when using MPLS SDP:
  - Epipe PW redundancy
  - MC-LAG based protection for access SAPs using the new service type (along with use PW redundancy)

Example: vlan-vc-tag value configured to match Q1.Q2 SAP innner tag

The following example shows output of a **vlan-vc-tag** value configured to match the inner tag specified in the Q1.Q2 SAP configured in the service.

```
*A:7210SAS>config>service# info
----------------------------------------------
epipe 10 svc-sap-type qinq-inner-tag-preserve customer 1 create
       sap 1/1/3:10.45 create
    exit
    spoke-sdp 111:69 vc-type vlan create
         vlan-vc-tag 45
    exit
    no shutdown
----------------------------------------------
```

Example: Epipe service with QinQ SAP and dot1q SAP

The following example shows an Epipe service with QinQ SAP and dot1q SAP. In the following example, note that the dot1q SAP (1/1/4:45) VLAN value of 45 matches the inner tag VLAN value specified with QinQ SAP (1/1/3:10.45).

```
*A:7210>config>service# info
----------------------------------------------
epipe 10 svc-sap-type qinq-inner-tag-preserve customer 1 create
       sap 1/1/3:10.45 create
no shutdown
    exit
    sap 1/1/4:45 create
         no shutdown
    exit
    no shutdown
exit
----------------------------------------------
```

Example: Epipe service with 2 QinQ SAPs

The following example shows an Epipe service with 2 QinQ SAPs. In the following sample, note that the inner tag of both QinQ SAPs matches and is set to a value of '45'.

```
*A:7210>config>service# info
----------------------------------------------------------------------------------------
epipe 10 svc-sap-type qinq-inner-tag-preserve customer 1 create
sap 1/1/3:10.45 create
no shutdown
exit
sap 1/1/4:200.45 create
no shutdown
exit
no shutdown
exit
----------------------------------------------------------------------------------------
```

3.2 Epipe oper state decoupling

An Epipe service transitions to an operational state of down when only a single entity SAP or binding is active and the operation state of the mate is down or displays an equivalent state. The default behavior does not allow you to validate the connectivity and measure performance metrics. With this feature an option is provided to allow you to validate the connectivity and measure performance metrics of an Epipe service.

You can also maintain performance and continuity measurement across the customer network regardless of the connectivity between the terminating node and the customer. If the SAP between the operator and the customer enters a Oper Down state, the Epipe remains operationally up, so the results can continue to be collected uninterrupted. The operator receives applicable port or SAP alerts/alarms. This option is available only for the customer facing SAP failures. If a network facing SAP or spoke-SDP fails, the operational state of the Epipe service is set to 'Down'. That is, there is no option to hold the service in an UP state, if a network component fails.

The following functionality is supported:

- Configuration under SAP is required to change the default behavior of the Epipe service in response to the SAP failure.
- The user can create a SAP on a LAG where the LAG has no port members. In this case, the operator configures the **ignore-oper-state** on the SAP and the service remains operational. However, as there are no ports existing in the LAG member group, there is no extraction function that can be created. This feature protects against an established working configuration with full forwarding capabilities from failing to collect PM data. The user should shutdown their equipment and place the Epipe SAP in an operationally down state.
- The SAP connecting the provider equipment to the customer is configured to hold the Epipe service status UP when the customer facing SAP enters any failed state. Only one SAP per Epipe is allowed to be configured.
- Any failure of the network entity (network SAP or SDP-Binding) still cause the Epipe service to transition to OPER=DOWN.
- As the service remains operationally up, all bindings should remain operationally up and should be able to receive and transmit data. The PW status represents the failed SAP in the LDP status message, but this does not prevent the data from using the PW as a transport, in or out. This is the same as LDP status messaging.
- The SAP failure continues to trigger normal reactions, except the operational state of the service.
- ETH-CFM PM measurement tools (DMM/SLM) can be used with the UP MEP on the failed SAP to collect performance metric. Additionally, CFM troubleshooting tools and connectivity (LBM, LTM, AIS, CCM) can be used and function as usual.
- ETH-CFM CCM processing and fault propagation does not change. Even when a SAP fails with the hold service UP configuration, CCM sets the Interface Status TLV to "Down".
- VPLS services remain operationally UP until the final entity in the service enters a failed operational state. There are no changes to VPLS services and the change is specific to Epipe.

3.3 Pseudowire switching

Note:
The 7210 SAS platforms as described in this document can be configured as S-PE nodes.

The pseudowire switching feature provides the user with the ability to create a VLL service by cross-connecting two spoke SDPs. This feature allows the scaling of VLL and VPLS services in a large network in which the otherwise full mesh of PE devices would require thousands of Targeted LDP (T-LDP) sessions per PE node.

Services with one SAP and one spoke-SDP are created on the PE; however, the target destination of the SDP is the pseudowire switching node instead of the remote PE.

The pseudowire switching node acts in a passive role with respect to signaling of the pseudowires. It waits until one or both of the PEs sends the label mapping message before relaying it to the other PE. This is because it needs to pass the Interface Parameters of each PE to the other.

A pseudowire switching point TLV is inserted by the switching pseudowire to record its system address when relaying the label mapping message. This TLV is useful in a few situations:

- It allows for troubleshooting of the path of the pseudowire especially if multiple pseudowire switching points exist between the two PEs.

- It helps in loop detection of the T-LDP signaling messages where a switching point would receive back a label mapping message it had already relayed.
- The switching point TLV is inserted in pseudowire status notification messages when they are sent end-to-end or from a pseudowire switching node toward a destination PE.

Pseudowire OAM is supported for the manual switching pseudowires and allows the pseudowire switching node to relay end-to-end pseudowire status notification messages between the two PEs. The pseudowire switching node can generate a pseudowire status and to send it to one or both of the PEs by including its system address in the pseudowire switching point TLV. This allows a PE to identify the origin of the pseudowire status notification message.

Example: Pseudowire service switching node

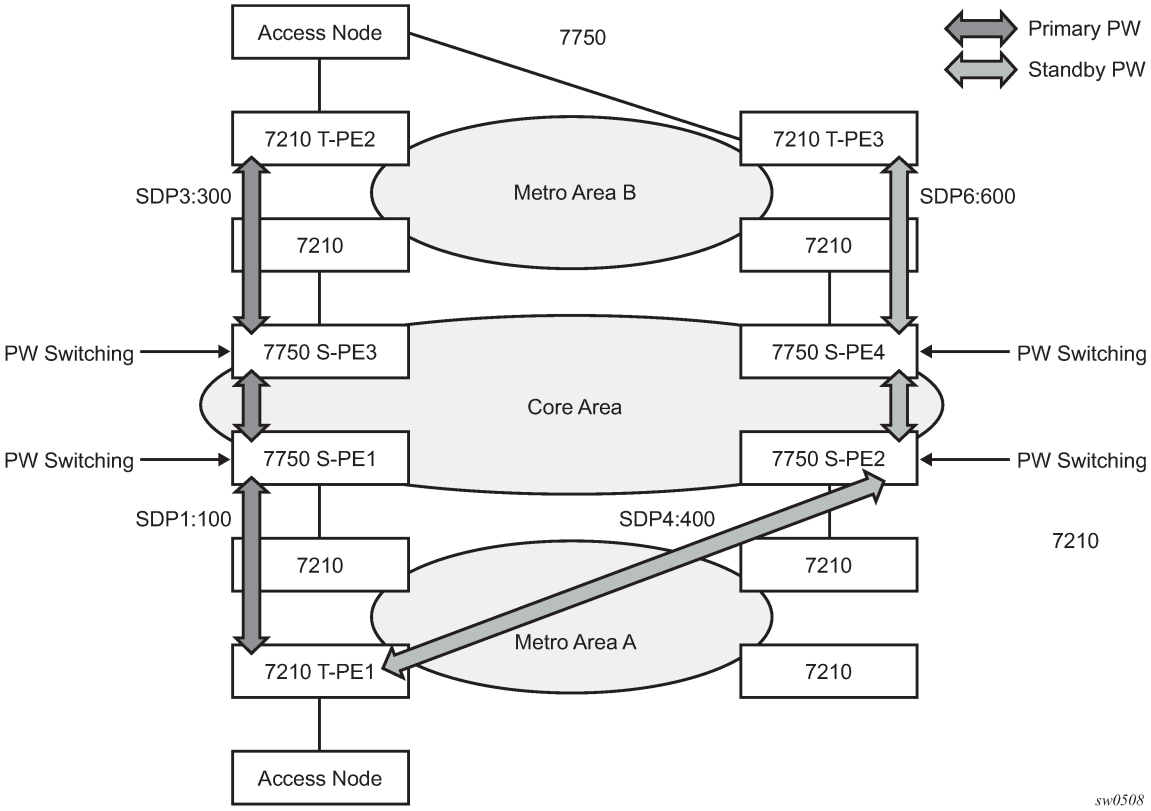
In the following example, the user configures a regular Epipe VLL service PE1 and PE2. These services consist each of a SAP and a spoke SPD. However, the target destination of the SDP is actually not the remote PE but the pseudowire switching node. In addition, the user configures an Epipe VLL service on the pseudowire switching node using the two SDPs.

| PE1 (Epipe)|---sdp 2:10---| PW SW (Epipe)|---sdp 7:15---| PE2 (Epipe)|

3.3.1 Pseudowire switching with protection

Pseudowire switching scales VLL and VPLS services over a multi-area network by removing the need for a full mesh of targeted LDP sessions between PE nodes. The following figure shows the use of pseudowire redundancy to provide a scalable and resilient VLL service across multiple IGP areas in a provider network.

Figure 15: VLL resilience with pseudowire redundancy and switching



In the network in the preceding figure, PE nodes act as leading nodes and pseudowire switching nodes act as followers for the purpose of pseudowire signaling. A switching node needs to pass the SAP Interface Parameters of each PE to the other.T-PE1 sends a label mapping message for the Layer 2 FEC to the peer pseudowire switching node" for example, S-PE1. It includes the SAP interface parameters, such as MTU, in the label mapping message. S-PE1 checks the FEC against the local information and if a match exists, it appends the optional pseudowire switching point TLV to the FEC TLV in which it records its system address. T-PE1 then relays the label mapping message to S-PE2. S-PE2 performs similar operations and forwards a label mapping message to T-PE2. The same procedures are followed for the label mapping message in the reverse direction, for example, from T-PE2 to T-PE1. S-PE1 and S-PE2 affect the spoke-SDP cross-connect only when both directions of the pseudowire have been signaled and matched.

The pseudowire switching TLV is useful in a few situations. First, it allows for troubleshooting of the path of the pseudowire especially if multiple pseudowire switching points exist between the two T-PE nodes. Secondly, it helps in loop detection of the T-LDP signaling messages where a switching point receives back a label mapping message it already relayed. Finally, it can be inserted in pseudowire status messages when they are sent from a pseudowire switching node toward a destination PE.

Pseudowire status messages can be generated by the T-PE nodes. Pseudowire status messages received by a switching node are processed and then passed on to the next hop. An S-PE node appends the optional pseudowire switching TLV, with its system address added to it, to the FEC in the pseudowire status notification message only if it originated the message or the message was received with the TLV in it. Otherwise, it means the message was originated by a T-PE node and the S-PE should process and pass the message without changes except for the VCID value in the FEC TLV.

3.3.2 Pseudowire switching behavior

In the network in Figure 15: VLL resilience with pseudowire redundancy and switching, PE nodes act as leading nodes and pseudowire switching nodes act as followers for the purpose of pseudowire signaling. This is because a switching node needs to pass the SAP interface parameters of each PE to the other.T-PE1 sends a label mapping message for the Layer 2 FEC to the peer pseudowire switching node, for example, S-PE1. It includes the SAP interface parameters, such as MTU, in the label mapping message. S-PE1 checks the FEC against the local information and if a match exists, it appends the optional pseudowire switching point TLV to the FEC TLV in which it records its system address. T-PE1 then relays the label mapping message to S-PE2. S-PE2 performs similar operation and forwards a label mapping message to T-PE2. The same procedures are followed for the label mapping message in the reverse direction, for example, from T-PE2 to T-PE1. S-PE1 and S-PE2 affect the spoke-SDP cross-connect only when both directions of the pseudowire have been signaled and matched.

The merging of the received T-LDP status notification message and the local status for the spoke SDPs from the service manager at a PE complies with the following rules:

- When the local status for both spokes is up, the S-PE passes any received SAP or SDP-binding generated status notification message unchanged, for example, the status notification TLV is unchanged but the VC-ID in the FEC TLV is set to value of the pseudowire segment to the next hop.
- When the local operational status for any of the spokes is down, the S-PE always sends SDP-binding down status bits regardless if the received status bits from the remote node indicated SAP up/down or SDP-binding up/down.

3.3.2.1 Pseudowire switching TLV

The format of the pseudowire switching TLV is as follows:

```
 0                   1                   2                   3
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|1|0|     pw sw TLV  (0x096D)   |     pseudowire sw TLV  Length         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |    Length     |    Variable Length Value      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         Variable Length Value                 |
|                             "                                 |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

- **PW sw TLV Length**

  Specifies the total length of all the following pseudowire switching point TLV fields in octets.

- **Type**

  Encodes how the Value field is to be interpreted.

- **Length**

  Specifies the length of the Value field in octets.

- **Value**

Octet string of Length octets that encodes information to be interpreted as specified by the Type field.

Pseudowire Switching Point Sub-TLVs

The following are details specific to pseudowire switching point sub-TLVs:

- **pseudowire ID of last pseudowire segment traversed**

  This sub-TLV type contains a pseudowire ID in the format of the pseudowire ID
- **pseudowire switching point description string**

  An optional description string of text up to 80 characters
- IP address of pseudowire switching point
- The IP V4 or V6 address of the pseudowire switching point. This is an optional sub-TLV
- MH VCCV capability indication

3.3.2.2 Static-to-dynamic pseudowire switching

When one segment of the pseudowire cross-connect at the S-PE is static while the other is signaled using T-LDP, the S-PE operates much like a T-PE from a signaling perspective and as an S-PE from a data plane perspective.

The S-PE signals a label mapping message as soon as the local configuration is complete. The control word C-bit field in the pseudowire FEC is set to the value configured on the static spoke-SDP.

When the label mapping for the egress direction is also received from the T-LDP peer, and the information in the FEC matches that of the local configuration, the static-to-dynamic cross-connection is effected.

End nodes of a static pseudowire segment can be misconfigured. In this case, an S-PE or T-PE node may be receiving packets with the wrong encapsulation, and it is possible that an invalid payload is forwarded over the pseudowire or the SAP respectively. Also, if the S-PE or T-PE node is expecting the control word in the packet encapsulation and the received packet comes with no control word but the first nibble below the label stack is 0x0001, the packet may be mistaken for a VCCV OAM packet and may be forwarded to the CPM. In that case, the CPM performs a check of the IP header fields such as version, IP header length, and checksum. If any of this fails the VCCV packet is discarded.

3.3.3 Pseudowire redundancy

Pseudowire redundancy provides the ability to protect a pseudowire with a preprovisioned pseudowire and to switch traffic over to the secondary standby pseudowire in case of a SAP or network failure condition. Pseudowires are redundant by the virtue of the SDP redundancy mechanism. For instance, if the SDP is an RSVP LSP and is protected by a secondary standby path, Fast-Reroute paths, or both, the pseudowire is also protected. However, there are a couple of applications in which SDP redundancy does not protect the end-to-end pseudowire path:

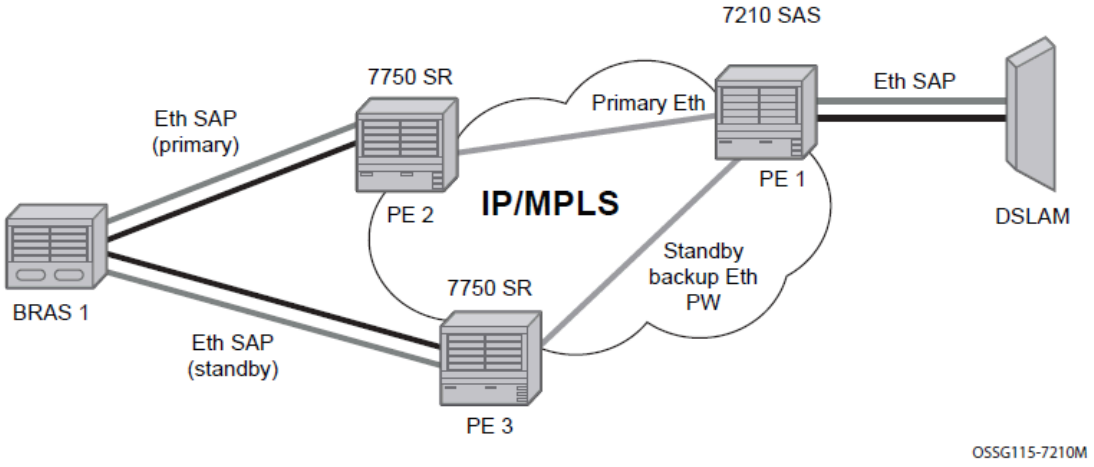
- There are two different destination PE nodes for the same VLL service. The main use case is the provision of dual-homing of a CPE or access node to two PE nodes located in different POPs. The other use case is the provision of a pair of active and standby BRAS nodes, or active and standby links to the same BRAS node, to provide service resiliency to broadband service subscribers.
- The pseudowire path is switched in the middle of the network and the 7210 SAS pseudowire switching node fails.

Pseudowire and VPLS link redundancy extends link-level resiliency for pseudowires and VPLS to protect critical network paths against physical link or node failures. These innovations enable the virtualization of redundant paths across the metro or core IP network to provide seamless and transparent fail-over for point-to-point and multi-point connections and services. When deployed with multi-chassis LAG, the path for return traffic is maintained through the pseudowire or VPLS switchover, which enables carriers to deliver “always on” services across their IP/MPLS networks.

3.3.3.1 VLL resilience with two destination PE nodes

The following figure shows the application of pseudowire redundancy to provide Ethernet VLL service resilience for broadband service subscribers accessing the broadband service on the service provider BRAS.

Figure 16: VLL resilience



If the Ethernet SAP on PE2 fails, PE2 notifies PE1 of the failure by either withdrawing the primary pseudowire label it advertised or by sending a pseudowire status notification with the code set to indicate a SAP defect. PE1 receives it and immediately switches its local SAP to forward over the secondary standby spoke-SDP. To avoid black holing of in-flight packets during the switching of the path, PE1 accepts packets received from PE2 on the primary pseudowire while transmitting over the backup pseudowire.

When the SAP at PE2 is restored, PE2 updates the new status of the SAP by sending a new label mapping message for the same pseudowire FEC or by sending pseudowire status notification message indicating that the SAP is back up. PE1 then starts a timer and reverts to the primary at the expiry of the timer. By default, the timer is set to 0, which means PE1 reverts immediately. A special value of the timer (infinity) means that PE1 should never revert to the primary pseudowire.

The behavior of the pseudowire redundancy feature is the same if PE1 detects or is notified of a network failure that brought the spoke-SDP operational status to DOWN. The following are the events which cause PE1 to trigger a switchover to the secondary standby pseudowire:

1. T-LDP peer (remote PE) node withdrew the pseudowire label.
2. T-LDP peer signaled a FEC status indicating a pseudowire failure or a remote SAP failure.
3. T-LDP session to peer node times out.

4. SDP binding and VLL service went down as a result of network failure condition such as the SDP to peer node going operationally down.

The Nokia routers support the ability to configure multiple secondary standby pseudowire paths. For example, PE1 uses the value of the user configurable precedence parameter associated with each spoke-SDP to select the next available pseudowire path after the failure of the current active pseudowire (whether it is the primary or one of the secondary pseudowires). The revertive operation always switches the path of the VLL back to the primary pseudowire though. There is no revertive operation between secondary paths meaning that the path of the VLL does not switch back to a secondary pseudowire of higher precedence when the latter comes back up again.

The Nokia routers support the ability for a user-initiated manual switchover of the VLL path to the primary or any of the secondary be supported to divert user traffic in case of a planned outage such as in node upgrade procedures.

3.3.4 Dynamic Multi-Segment Pseudowire Routing

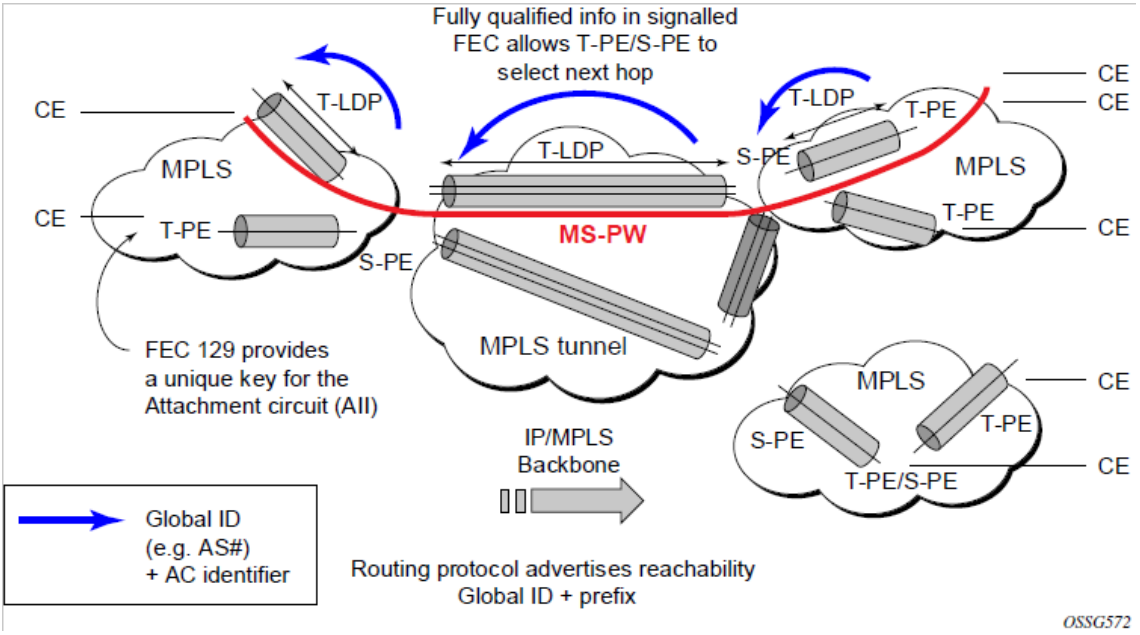
3.3.4.1 Overview

The following sections describe the end-to-end solution with BGP PW-routing, assuming appropriate platforms are used for various functions.

Dynamic Multi-Segment Pseudowire Routing (Dynamic MS-PWs) enable a complete multi-segment pseudowire to be established, while only requiring per-pseudowire configuration on the T-PEs. No per-pseudowire configuration is required on the S-PEs. End-to-end signaling of the MS-PW is achieved using T-LDP, while multi-protocol BGP is used to advertise the T-PEs, so allowing dynamic routing of the MS-PW through the intervening network of S-PEs. Dynamic multi-segment pseudowires are described in the IETF in *draft-ietf-pwe3-dynamic-ms-pw-13.txt*.

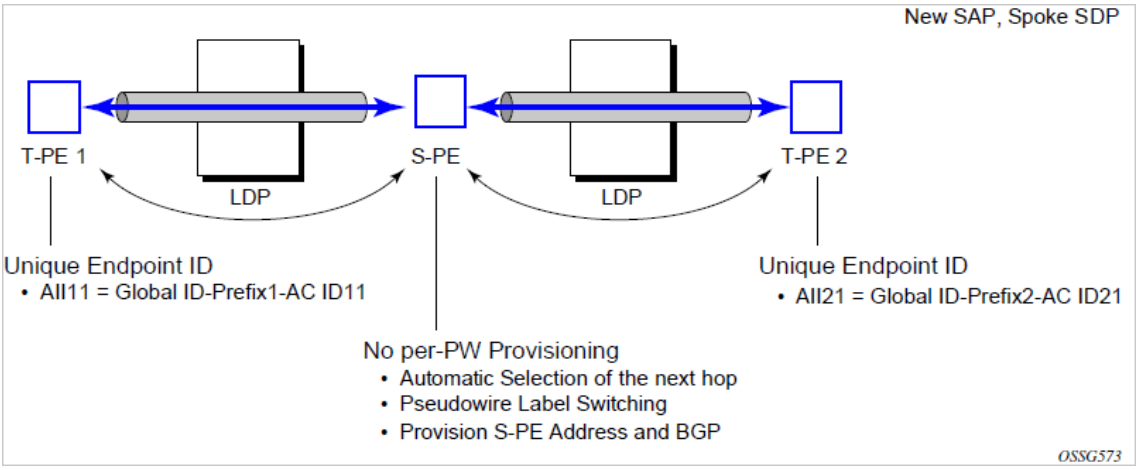
The following figure shows the operation of dynamic MS-PWs.

Figure 17: Dynamic MS-PW overview



The FEC 129 AII Type 2 structure shown in the following figure is used to identify each individual pseudowire endpoint:

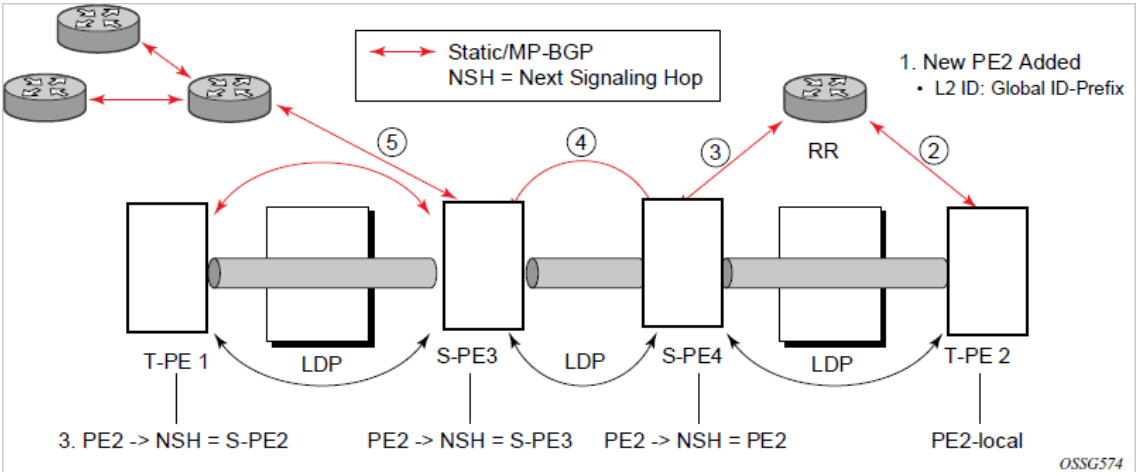
Figure 18: MS-PW addressing using FEC129 AII Type 2



A 4-byte global ID followed by a 4 byte prefix and a 4 byte attachment circuit ID are used to provide for hierarchical, independent allocation of addresses on a per service provider network basis. The first 8 bytes (Global ID + Prefix) may be used to identify each individual T-PE or S-PE as a loopback Layer 2 Address.

This new AII type is mapped into the MS-PW BGP NLRI (a new BGP AFI of L2VPN, and SAFI for network layer reachability information for dynamic MS-PWs. As soon as a new T- PE is configured with a local prefix address of global id:prefix, pseudowire routing proceeds to advertise this new address to all the other T- PEs and S-PEs in the network, as shown in the following figure.

Figure 19: Advertisement of PE addresses by PW routing



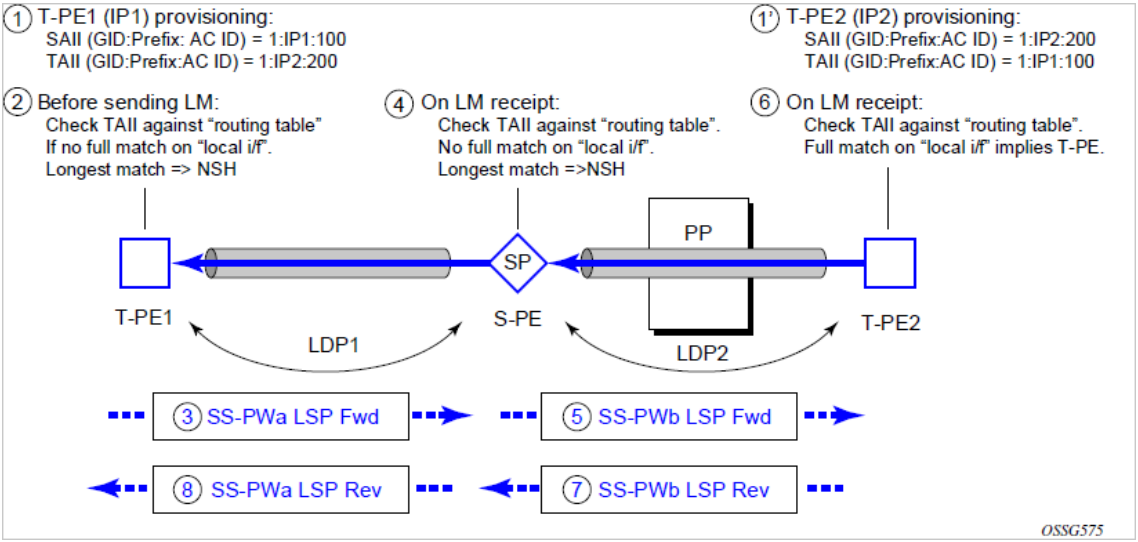
In step 1 a new T-PE (T-PE2) is configured with a local prefix.

Next, in steps 2-5, MP-BGP uses the NLRI for the MS-PW routing SAFI to advertise the location of the new T-PE to all the other PEs in the network. Alternatively, static routes may be configured on a per T-PE/S-PE basis to accommodate non-BGP PEs in the solution.

As a result, pseudowire routing tables for all the S-PEs and remote T-PEs are populated with the next hop to be used to reach T-PE2.

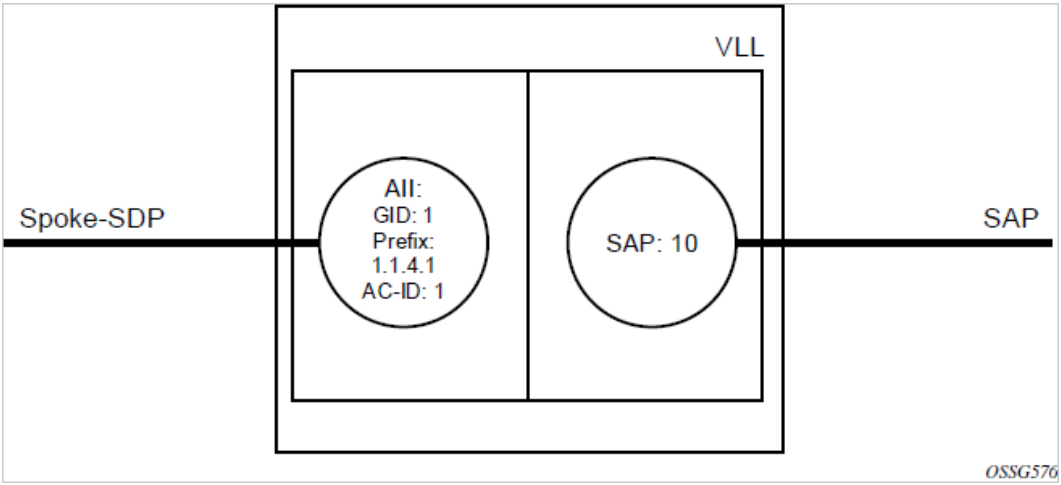
VLL services can then be established, as shown in the following figure.

Figure 20: Signaling of dynamic MS-PWs using T-LDP



In step 1 and 1' the T-PEs are configured with the local and remote endpoint information, Source AII (SAII), Target AII (TAII). On the 7210, the AIIs are locally configured for each spoke-SDP, according to the model shown in the following figure. The 7210 therefore provides for a flexible mapping of AII to SAP. That is, the values used for the AII are through local configuration, and it is the context of the spoke-SDP that binds it to a specific SAP.

Figure 21: Mapping of AII to SAP



Before T-LDP signaling starts, the two T-PEs decide on an active and passive relationship using the highest AII (comparing the configured SAII and TAII) or the configured precedence. Next, the active T-PE (in the IETF draft this is referred to as the source T-PE or ST-PE) checks the PW Routing Table to determine the next signaling hop for the configured TAII using the longest match between the TAII and the entries in the PW routing table

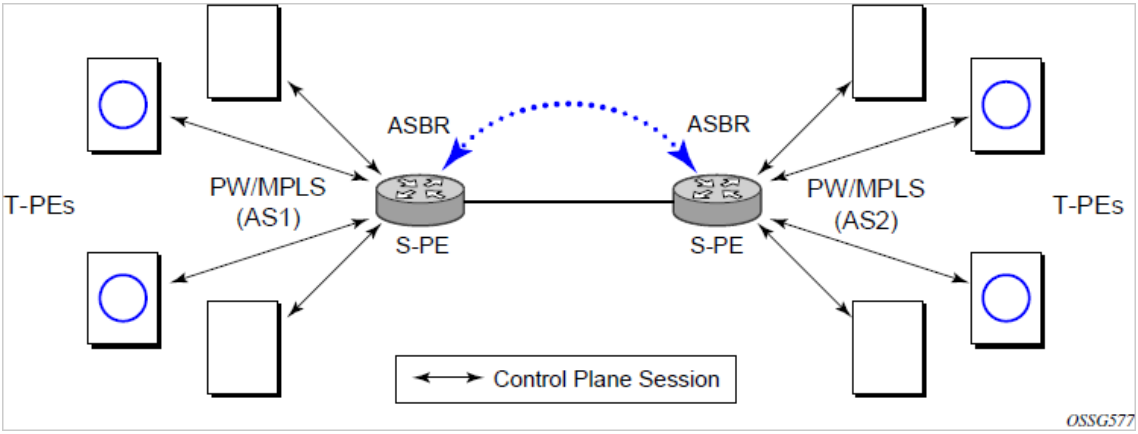
This signaling hop is then used to choose the T-LDP session to the chosen next-hop S-PE. Signaling proceeds through each subsequent S-PE using similar matching procedures to determine the next signaling hop. Otherwise, if a subsequent S-PE does not support dynamic MS-PW routing and therefore uses a statically configured PW segment, the signaling of individual segments follows the procedures already implemented in the PW Switching feature.

Note: BGP can install a PW AII route in the PW routing table with ECMP next-hops. However, when LDP needs to signal a PW with matching TAII, it chooses only one next-hop from the available ECMP next-hops. PW routing supports up to 4 ECMP paths for each destination.

The signaling of the forward path ends when the PE matches the TAII in the label mapping message with the SAII of a spoke-SDP bound to a local SAP. The signaling in the reverse direction can now be initiated, which follows the entries installed in the forward path. The PW Routing tables are not consulted for the reverse path. This ensures that the reverse direction of the PW follows exactly the same set of S-PEs as the forward direction.

This solution can be used in either a MAN-WAN environment or in an Inter-AS/Inter-Provider environment as shown in the following figure.

Figure 22: VLL using dynamic MS-PWs, Inter-AS scenario



Note: Data plane forwarding at the S-PEs uses pseudowire service label switching, as per the pseudowire switching feature.

3.3.4.2 Pseudowire routing

Note: The platforms as described in this document can be configured as S-PE nodes.

The following sections describe the end-to-end solution with BGP PW-routing, assuming appropriate platforms are used for various functions.

Each S-PE and T-PE has a pseudowire routing table that contains a reference to the T-LDP session to use to signal to a set of next hop S-PEs to reach a specific T-PE (or the T-PE if that is the next hop). For VLLs, this table contains aggregated All Type 2 FECs and may be populated with routes that are learned through MP-BGP or that are statically configured.

MP-BGP is used to automatically distribute T-PE prefixes using the new MS-PW NLRI, or static routes can be used. The MS-PW NLRI is composed of a Length, an 8-byte RD, a 4-byte Global-ID, a 4-byte local prefix, and (optionally) a 4-byte AC-ID. Support for the MS-PW address family is configured in CLI under **config>router>bgp>family ms-pw**.

MS-PW routing parameters are configured in the **config>service>pw-routing** context.

To enable support for dynamic MS-PWs on a 7210 node to be used as a T-PE or S-PE, a single, globally unique, S-PE ID, known as the S-PE Address, is first configured under **config>service>pw-routing** on each 7210 to be used as a T-PE or S-PE. The S-PE Address has the format global-id:prefix. It is not possible to configure any local prefixes used for pseudowire routing or to configure spoke SPDs using dynamic MS-PWs at a T-PE unless an S-PE address has already been configured. The S-PE address is used as the address of a node used to populate the switching point TLV in the LDP label mapping message and the pseudowire status notification sent for faults at an S-PE.

Each T-PE is also be configured with the following parameters:

1. **Global ID**

   This is a 4 byte identifier that uniquely identifies an operator or the local network.

2. **Local Prefix**

One or more local (Layer 2) prefixes (up to a maximum of 16), which are formatted in the style of a 4-octet IPv4 address. A local prefix identifies a T-PE or S-PE in the PW routing domain.

3. For each local prefix, at least one 8-byte route distinguisher can be configured. It is also possible to configure an optional BGP community attribute.

For each local prefix, BGP then advertises each global ID/prefix tuple and unique RD and community pseudowire using the MS-PW NLRI, based on the aggregated FEC129 AII Type 2 and the Layer 2 VPN/PW routing AFI/SAFI 25/6, to each T-PE/S-PE that is a T-LDP neighbor, subject to local BGP policies.

The dynamic advertisement of each of these pseudowire routes is enabled for each prefix and RD using the **advertise-bgp** command.

Example: Exporting MS-PW routes in MP-BGP

An export policy is also required to export MS-PW routes in MP-BGP. This can be done using a default policy, such as the following.

```
*A:lin-123>config>router>policy-options# info
----------------------------------------------
            policy-statement "ms-pw"
                default-action accept
                exit
            exit
----------------------------------------------
```

However, this would export all routes. A recommended choice is to enable filtering per family, as follows.

```
*A:lin-123>config>router>policy-options# info
----------------------------------------------
            policy-statement "to-mspw"
                entry 1
                    from
                        family ms-pw
                    exit
                    action accept
                    exit
                exit
            exit
----------------------------------------------
```

The following command is then added in the **config>router>bgp** context.

```
export "to-mspw"
```

Local preference for iBGP and BGP communities can be configured under such a policy.

3.3.4.2.1 Static routing

In addition to support for BGP routing, static MS-PW routes may also be configured using the config>services>pw-routing>static-route command. Each static route comprises the target T-PE Global-ID and prefix, and the IP address of the T-LDP session to the next hop S-PE or T-PE that should be used.

If a static route is set to 0, then this represents the default route. If a static route exists to a specific T-PE, then this is used in preference to any BGP route that may exist.

3.3.4.2.2 Explicit paths

A set of default explicit routes to a remote T-PE or S-PE prefix may be configured on a T-PE under **config>services>pw-routing** using the path name command. Explicit paths are used to populate the explicit route TLV used by MS-PW T-LDP signaling. Only strict (fully qualified) explicit paths are supported.

Note: It is possible to configure explicit paths independently of the configuration of BGP or static routing.

3.3.4.3 Configuring VLLs using dynamic MS-PWs

One or more spoke SDPs may be configured for distributed Epipe VLL services. Dynamic MS-PWs use FEC129 (also known as the Generalized ID FEC) with Attachment Individual Identifier (AII) Type 2 to identify the pseudowire, as opposed to FEC128 (also known as the PW ID FEC) used for traditional single segment pseudowires and for pseudowire switching. FEC129 spoke SDPs are configured under the **spoke-sdp-fec** command in the CLI.

FEC129 AII Type 2 uses a Source Attachment Individual Identifier (SAII) and a Target Attachment Individual Identifier (TAII) to identify the end of a pseudowire at the T-PE. The SAII identifies the local end, while the TAII identifies the remote end. The SAII and TAII are each structured as follows:

- **Global-ID**

  This is a 4 byte identifier that uniquely identifies an operator or the local network.

- **Prefix**

  A 4-byte prefix, which should correspond to one of the local prefixes assigned under **pw-routing**.

- **AC-ID**

  A 4-byte identifier for this end of the pseudowire. This should be locally unique within the scope of the global-id:prefix.

3.3.4.3.1 Active/passive T-PE selection

Dynamic MS-PWs use single-sided signaling procedures with double-sided configuration, a fully qualified FEC must be configured at both endpoints. That is, one T-PE (the source T-PE, ST-PE) of the MS-PW initiates signaling for the MS-PW, while the other end (the terminating T-PE, TT-PE) passively waits for the label mapping message from the far-end and only responds with a label mapping message to set up the opposite direction of the MS-PW when it receives the label mapping from the ST-PE. By default, the 7210 SAS determines which T-PE is the ST-PE (the active T-PE) and which is the TT-PE (the passive T-PE) automatically, based on comparing the SAII with the TAII as unsigned integers. The T-PE with SAII>TAII assumes the active role. However, it is possible to override this behavior using the **signaling** {**master** | **auto**} command under the **spoke-sdp-fec**. If master is selected at a specific T-PE, it assumes the active role. If a T-PE is at the endpoint of a spoke-SDP that is bound to an VLL SAP and single sided auto-configuration is used (as follows), then that endpoint is always passive. Therefore, signaling master should only be used when it is known that the far end assumes a passive behavior.

3.3.4.3.2 Automatic endpoint configuration

Automatic endpoint configuration allows the configuration of an endpoint without specifying the TAII associated with that **spoke-sdp-fec**. It allows a single-sided provisioning model where an incoming label mapping message with a TAII that matches the SAII of that spoke-SDP to be automatically bound to that endpoint. This is useful in scenarios where a service provider needs to separate service configuration from the service activation phase.

Automatic endpoint configuration is supported required for Epipe VLL **spoke-sdp-fec** endpoints bound to a VLL SAP. It is configured using the **spoke-sdp-fec>auto-config** command, and excluding the TAII from the configuration. When auto-configuration is used, the node assumed passive behavior from a point of view of T-LDP signaling. Therefore, the far-end T-PE must be configured for signaling master for that **spoke-sdp-fec**.

3.3.4.3.3 Selecting a path for an MS-PW

Path selection for signaling occurs in the outbound direction (ST-PE to TT-PE) for an MS-PW. In the TT-PE to ST-PE direction, a label mapping message follows the reverse of the path already taken by the outgoing label mapping.

A node can use explicit paths, static routes, or BGP routes to select the next hop S-PE or T-PE. The order of preference used in selecting these routes is:

1. Explicit Path
2. Static route
3. BGP route

To use an explicit path for an MS-PW, an explicit path must have been configured in the **config>services>pw-routing>path** *path-name* context. The user must then configure the corresponding **path** *path-name* under **spoke-sdp-fec**.

If an explicit path name is not configured, the TT-PE or S-PE performs a longest match lookup for a route (static if it exists, and BGP if not) to the next hop S-PE or T-PE to reach the TAII.

Pseudowire routing chooses the MS-PW path in terms of the sequence of S-PEs to use to reach a specific T-PE. It does not select the SDP to use on each hop, which is instead determined at signaling time. When a label mapping is sent for a specific pseudowire segment, an LDP SDP is used to reach the next-hop S-PE/T-PE if such an SDP exists. If not, and a RFC 3107 labeled BGP SDP is available, then that is used. Otherwise, the label mapping fails and a label release is sent.

3.3.4.3.4 Pseudowire templates

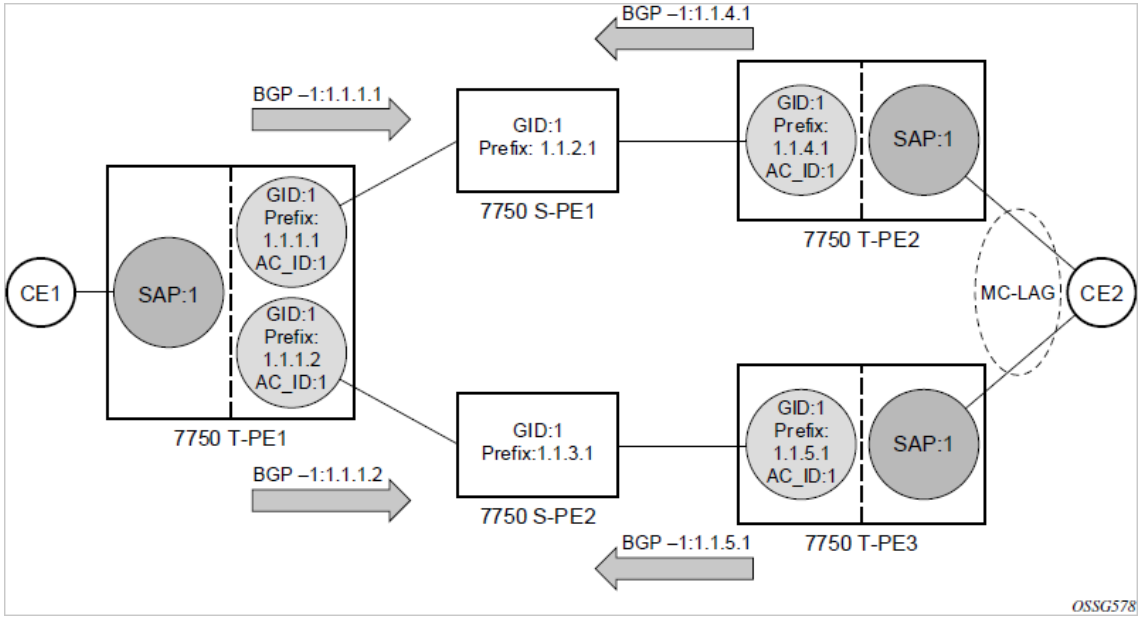
Dynamic MS-PWs support the use of the pseudowire template for specifying generic pseudowire parameters at the T-PE. The pseudowire template to use is configured in the **spoke-sdp-fec>pw-template-bind** *policy-id* context. Dynamic MS-PWs do not support the provisioned SDPs specified in the pseudowire template.

3.3.4.4 Pseudowire redundancy

Pseudowire redundancy is supported on dynamic MS-PWs used for VLLs. It is configured in a similar manner to pseudowire redundancy on VLLs using FEC128, whereby each **spoke-sdp-fec** within an endpoint is configured with a unique SAII/TAII.

The following figure shows the use of pseudowire redundancy.

Figure 23: Pseudowire redundancy



The following is a summary of the key points to consider in using pseudowire redundancy with dynamic MS-PWs:

- Each MS-PW in the redundant set must have a unique SAII/TAII set and is signaled separately. The primary pseudowire is configured in the **spoke-sdp-fec>primary** context.
- Each MS-PW in the redundant set should use a diverse path (from the point of view of the S-PEs traversed) from every other MS-PW in that set if path diversity is possible in a specific network topology. There are a number of possible ways to achieve this:
  - Configure an explicit path for each MS-PW.
  - Allow BGP routing to automatically determine diverse paths using BGP policies applied to different local prefixes assigned to the primary and standby MS-PWs.
  - Path diversity can be further provided for each primary pseudowire through the use of a BGP route distinguisher.

If the primary MS-PW fails, a fail-over to a standby MS-PW occurs, as per the normal pseudowire redundancy procedures. A configurable retry timer for the failed primary MS-PW is then started. When the timer expires, attempt to reestablish the primary MS-PW using its original path, up to a maximum number of attempts as per the retry count parameter. The T-PE may then optionally revert to the primary MS-PW on successful reestablishment.

Note that because the SDP ID is determined dynamically at signaling time, it cannot be used as a tie breaker to choose the primary MS-PW between multiple MS-PWs of the same precedence. The user should therefore explicitly configure the precedence values to determine which MS-PW is active in the final selection.

3.3.4.5 VCCV OAM for dynamic MS-PWs

The primary difference between dynamic MS-PWs and those using FEC128 is support for FEC129 AII type 2. As in PW Switching, VCCV on dynamic MS-PWs requires the use of the VCCV control word on the pseudowire. Both the **vccv-ping** and **vccv-trace** commands support dynamic MS-PWs.

3.3.4.6 VCCV-ping on dynamic MS-PWs

VCCV-ping supports the use of FEC129 AII type 2 in the target FEC stack of the ping echo request message. The FEC to use in the echo request message is derived in one of two ways: Either the user can specify only the spoke-sdp-fec-id of the MS-PW in the vccv-ping command, or the user can explicitly specify the SAII and TAII to use.

If the SAII:TAII is entered by the user in the **vccv-ping** command, then those values are be used for the VCCV ping echo request, but their order is be reversed before being sent so that they match the order for the downstream FEC element for an S-PE, or the locally configured SAII:TAII for a remote T-PE of that MS-PW. If SAII:TAII is entered in addition to the spoke-sdp-fec-id, the system verifies the entered values against the values stored in the context for that spoke-sdp-fec-id.

Otherwise, if the SAII:TAII to use in the target FEC stack of the VCCV ping message is not entered by the user, and if a switching point TLV was previously received in the initial label mapping message for the reverse direction of the MS-PW (with respect to the sending PE), then the SAII:TAII to use in the target FEC stack of the VCCV ping echo request message is derived by parsing that switching point TLV based on the user-specified TTL (or a TTL of 255 if none is specified). In this case, the order of the SAII:TAII in the switching point TLV is maintained for the VCCV ping echo request message.

If no pseudowire switching point TLV was received, then the SAII:TAII values to use for the VCCV ping echo request are derived from the MS-PW context, but their order is reversed before being sent so that they match the order for the downstream FEC element for an S-PE, or the locally configured SAII:TAII for a remote T-PE of that MS-PW. Note that the use of spoke-sdp-fec-id in vccv-ping is only applicable at T-PE nodes, because it is not configured for a specific MS-PW at S-PE nodes.

3.3.4.7 VCCV-trace on dynamic MS-PWs

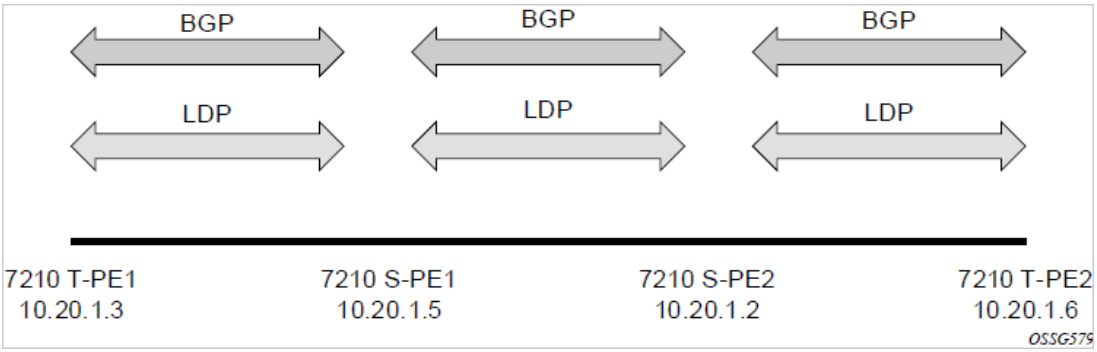
The 7210 SAS supports the MS-PW path trace mode of operation for VCCV trace, as per pseudowire switching, but using FEC129 AII type 2. As in the case of VCCV ping, the SAII:TAII used in the VCCV echo request message sent from the T-PE or S-PE from which the VCCV trace command is executed is specified by the user or derived from the context of the MS-PW.

Note: The use of spoke-sdp-fec-id in vccv-trace is only applicable at T-PE nodes because it is not configured for a specific MS-PW at S-PE nodes.

3.3.5 Example dynamic MS-PW configuration

This section presents an example of how to configure Dynamic MS-PWs for a VLL service between a set of 7210 nodes. The network consists of two 7210 T-PEs and two 7210 playing the role of S-PEs, as shown in the following figure. Each 7210 peers with its neighbor using LDP and BGP.

Figure 24: Dynamic MS-PW example



The example uses BGP to route dynamic MS-PWs and T-LDP to signal them. Therefore each node must be configured to support the MS-PW address family under BGP, and BGP and LDP peerings must be established between the T-PEs/S-PEs. The appropriate BGP export policies must also be configured.

Next, pseudowire routing must be configured on each node. This includes an S-PE address for every participating node, and one or more local prefixes on the T-PEs. MS-PW paths and static routes may also be configured. When this routing and signaling infrastructure is established, spoke-SDP FECs can be configured on each of the T-PEs.

Example: T-PE-1 configuration

```
config
   router
      ldp
         targeted-session
            peer 10.20.1.5
            exit
         exit
      policy-options
         begin
         policy-statement "exportMsPw"
            entry 10
               from
                  family ms-pw
               exit
               action accept
               exit
            exit
         exit
         commit
      exit
      bgp
         family ms-pw
         connect-retry 1
         min-route-advertisement 1
         export "exportMsPw"
         rapid-withdrawal
```

```
         group "ebgp"
            neighbor 10.20.1.5
               multihop 255
               peer-as 200
            exit
         exit
     exit
config
   service
      pw-routing
         spe-address 3:10.20.1.3
         local-prefix 3:10.20.1.3 create
         exit
         path "path1_to_F" create
            hop 1 10.20.1.5
            hop 2 10.20.1.2
            no shutdown
        exit
     exit
     epipe 1 customer 1 vpn 1 create
        description "Default epipe
             description for service id 1"
        service-mtu 1400
        service-name "XYZ Epipe 1"
        sap 2/1/1:1 create
        exit
        spoke-sdp-fec 1 fec 129 aii-type 2 create
           retry-timer 10
           retry-count 10
           saii-type2 3:10.20.1.3:1
           taii-type2 6:10.20.1.6:1
           no shutdown
```

Example: T-PE-2 configuration

```
config
   router
      ldp
         targeted-session
            peer 10.20.1.2
            exit
         exit
         …
      policy-options
         begin
         policy-statement "exportMsPw"
            entry 10
               from
                  family ms-pw
               exit
               action accept
               exit
            exit
         exit
         commit
      exit

      bgp
         family ms-pw
         connect-retry 1
         min-route-advertisement 1
         export "exportMsPw"
         rapid-withdrawal
```

```
         group "ebgp"
            neighbor 10.20.1.2
               multihop 255
               peer-as 300
            exit
         exit
     exit
config
   service
      pw-routing
         spe-address 6:10.20.1.6
         local-prefix 6:10.20.1.6 create
         exit
         path "path1_to_F" create
            hop 1 10.20.1.2
            hop 2 10.20.1.5
            no shutdown
        exit
     exit
     epipe 1 customer 1 vpn 1 create
        description "Default epipe
             description for service id 1"
service-mtu 1400
        service-name "XYZ Epipe 1"
        sap 1/1/3:1 create
        exit
        spoke-sdp-fec 1 fec 129 aii-type 2 create
           retry-timer 10
           retry-count 10
           saii-type2 6:10.20.1.6:1
           taii-type2 3:10.20.1.3:1
           no shutdown
        exit
        no shutdown
     exit
```

3.4 Master-slave operation

This section describes a mechanism in which one end on a pseudowire (the "master") dictates the active PW selection, which is followed by the other end of the PW (the "slave"). This mechanism and associated terminology is specified in RFC 6870.

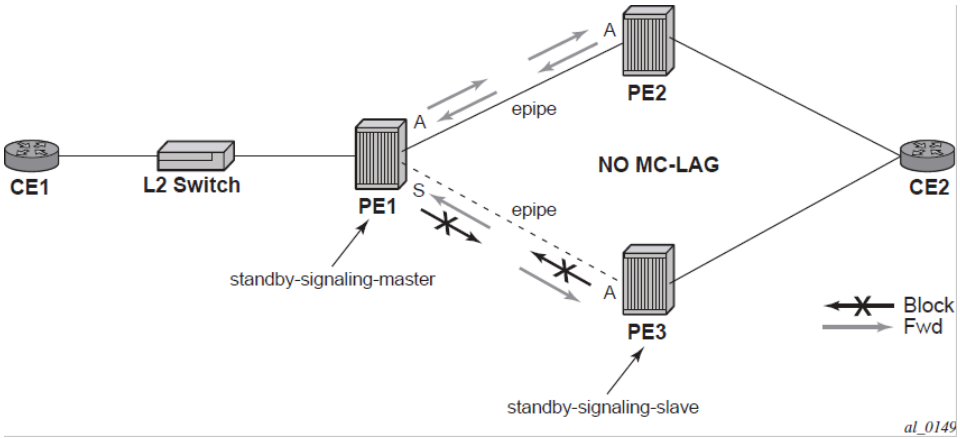
7210 SAS devices support only the standby-signaling-master option. 7210 does not support the CLI command standby-signaling-slave. In the following discussion, reference to standby-signaling-slave command is only used to describe the solution. 7210 device can be used only where standby-signaling-master is used in the following example.

Master-Slave pseudowire redundancy is discussed in this section. It adds the ability for the remote peer to react to the pseudowire standby status notification, even if only one spoke-SDP terminates on the VLL endpoint on the remote peer, by blocking the transmit (Tx) direction of a VLL spoke-SDP when the far-end PE signals standby. This solution enables the blocking of the Tx direction of a VLL spoke-SDP at both master and slave endpoints when standby is signaled by the master endpoint. This approach satisfies a majority of deployments where bidirectional blocking of the forwarding on a standby spoke-SDP is required.

The following figure shows the operation of master-slave pseudowire redundancy. In this scenario, an Epipe service is provided between CE1 and CE2. CE2 is dual homed to PE2 and PE3, and therefore PE1 is dual-homed to PE2 and PE3 using Epipe spoke SDPs. The objectives of this feature is to ensure that

only one pseudowire is used for forwarding in both directions by PE1, PE2 and PE3 in the absence of a native dual homing protocol between CE2 and PE2/PE3, such as MC-LAG. In normal operating conditions (the SAPs on PE2 and PE3 toward CE2 are both up and there are no defects on the ACs to CE2), PE2 and PE3 cannot choose which spoke-SDP to forward on based on the status of the AC redundancy protocol.

Figure 25: Master-slave pseudowire redundancy



Master-slave pseudowire redundancy adds the ability for the remote peer to react to the pseudowire standby status notification, even if only one spoke-SDP terminates on the VLL endpoint on the remote peer. When the CLI command standby-signaling-slave is enabled at the spoke-SDP or explicit endpoint level in PE2 and PE3, then any spoke-SDP for which the remote peer signals PW FWD Standby is blocked in the transmit direction.

This is achieved as follows. The standby-signaling-master state is activated on the VLL endpoint in PE1. In this case, a spoke-SDP is blocked in the transmit direction at this master endpoint if it is either in operDown state, or it has lower precedence than the highest precedence spoke-SDP, or the specific peer PE signals one of the following pseudowire status bits:

- Pseudowire not forwarding (0x01)
- SAP (ingress) receive fault (0x02)
- SAP (egress) transmit fault (0x04)
- SDP binding (ingress) receive fault (0x08)
- SDP binding (egress) transmit fault (0x10)

The fact that the specific spoke-SDP is blocked is signaled to LDP peer through the pseudowire status bit (PW FWD Standby (0x20)). This prevents traffic being sent over this spoke-SDP by the remote peer, but obviously only in case that remote peer supports and reacts to pseudowire status notification. Previously, this applied only if the spoke-SDP terminates on an IES, VPRN or VPLS. However, if standby-signaling-slave is enabled at the remote VLL endpoint then the Tx direction of the spoke-SDP is also blocked, according to the rules in Operation of master-slave pseudowire redundancy with existing scenarios.

Although master-slave operation provides bidirectional blocking of a standby spoke-SDP during steady-state conditions, it is possible that the Tx directions of more than one slave endpoint can be active for transient periods during a fail-over operation. This is because of slave endpoints transitioning a spoke-SDP from standby to active receiving or processing a pseudowire preferential forwarding status message before those transitioning a spoke-SDP to standby. This transient condition is most likely when a forced switch-over is performed, or the relative preferences of the spoke SDPs is changed, or the active spoke-SDP is

shutdown at the master endpoint. During this period, loops of unknown traffic may be observed. Fail-overs because of common network faults that can occur during normal operation, a failure of connectivity on the path of the spoke-SDP or the SAP, would not result in such loops in the datapath.

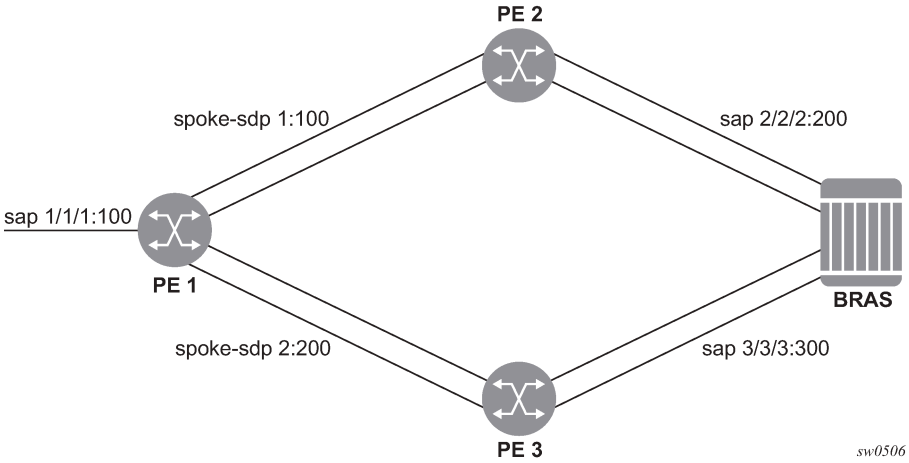
3.4.1 Operation of master-slave pseudowire redundancy with existing scenarios

This section illustrates how master-slave pseudowire redundancy could operate.

3.4.1.1 VLL resilience

The following figure shows a VLL resilience path example. A sample configuration follows.

Figure 26: VLL resilience



A revert-time value of zero (default) means that the VLL path is switched back to the primary immediately after it comes back up.

Example: PE1 configuration

```
configure service epipe 1
endpoint X
exit
endpoint Y
revert-time 0
standby-signaling-master
exit
sap 1/1/1:100 endpoint X
spoke-sdp 1:100 endpoint Y
precedence primary
spoke-sdp 2:200 endpoint Y
precedence 1
```

Example: PE2 configuration

```
configure service epipe 1
endpoint X
exit
sap 2/2/2:200 endpoint X
```

```
spoke-sdp 1:100
standby-signaling-slave
```

Example: PE3 configuration

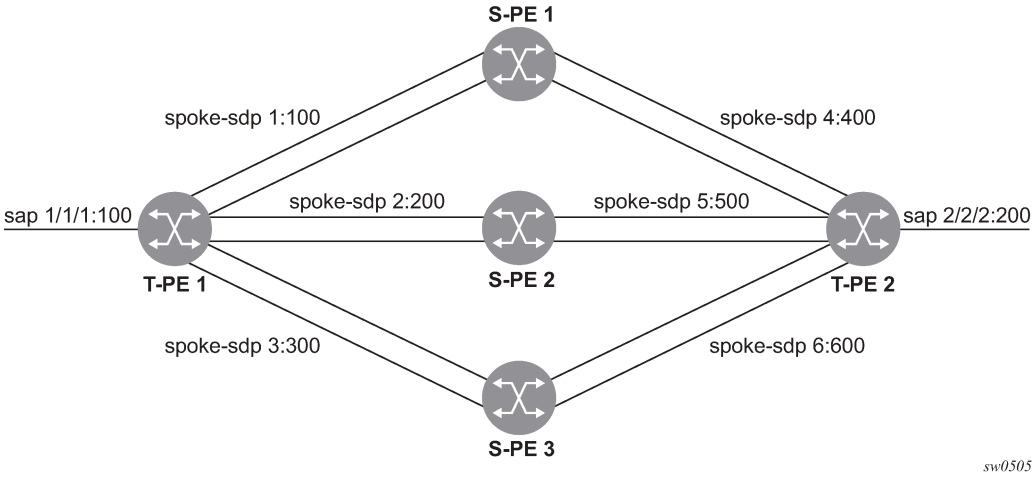
```
configure service epipe 1
endpoint X
exit
sap 3/3/3:300 endpoint X
spoke-sdp 2:200
standby-signaling-slave
```

3.4.1.2 VLL resilience for a switched PW path

Note:
The 7210 SAS platforms as described in this document can be configured as S-PE nodes.

The following figure shows a VLL resilience for a switched pseudowire path example. A sample configuration follows.

Figure 27: VLL resilience with pseudowire switching



Example: T-PE1 configuration

```
configure service epipe 1
endpoint X
exit
endpoint Y
revert-time 100
standby-signaling-master
exit
sap 1/1/1:100 endpoint X
spoke-sdp 1:100 endpoint Y
precedence primary
spoke-sdp 2:200 endpoint Y
precedence 1
spoke-sdp 3:300 endpoint Y
precedence 1
```

Example: T-PE2 configuration

```
configure service epipe 1
endpoint X
exit
endpoint Y
revert-time 100
standby-signaling-slave
exit
sap 2/2/2:200 endpoint X
spoke-sdp 4:400 endpoint Y
precedence primary
spoke-sdp 5:500 endpoint Y
precedence 1
spoke-sdp 6:600 endpoint Y
precedence 1
```

Example: S-PE1 configuration

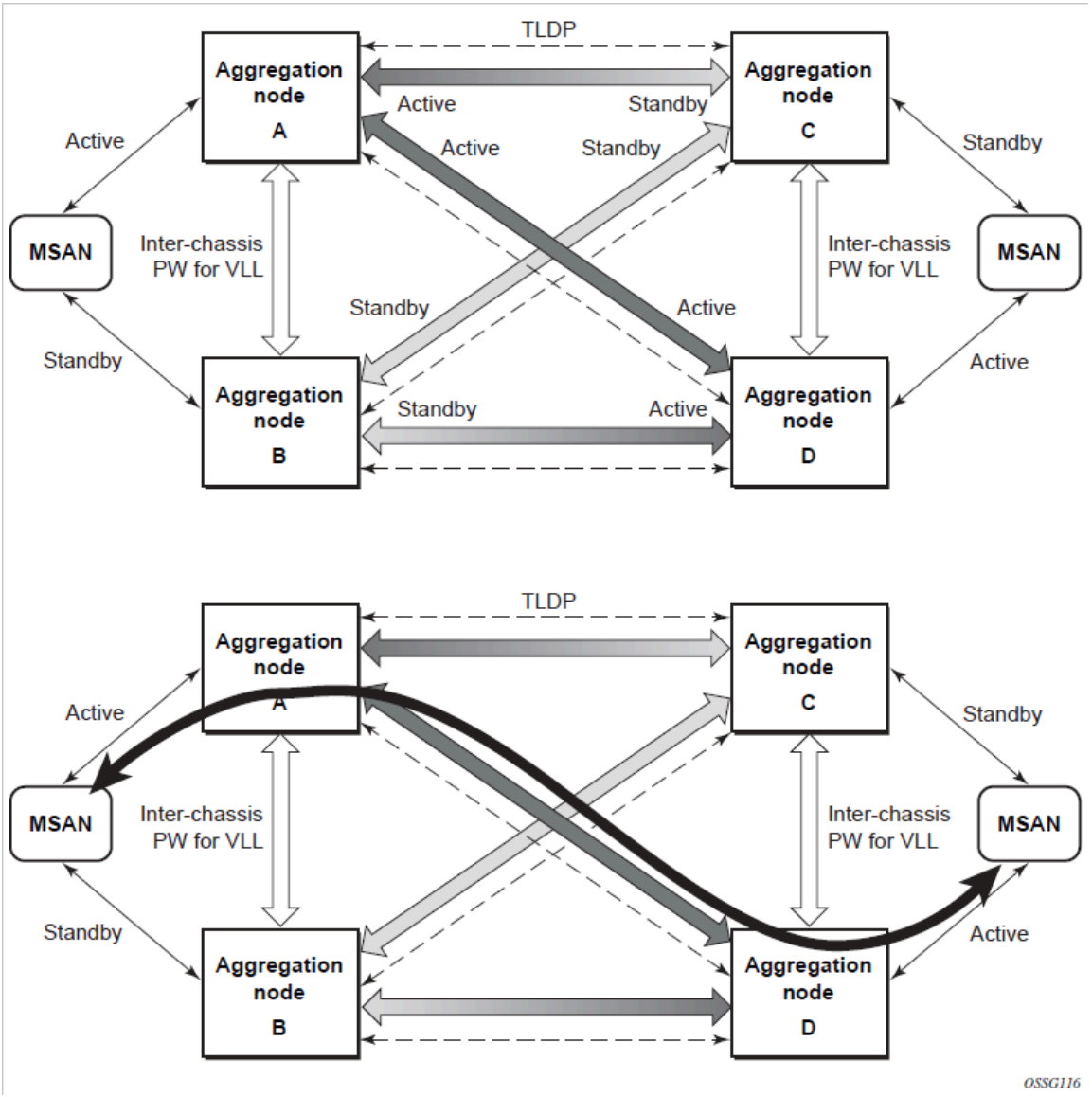
VC switching indicates a VC cross-connect so that the service manager does not signal the VC label mapping immediately but put this into passive mode.

```
configure service epipe 1 vc-switching
spoke-sdp 1:100
spoke-sdp 4:400
```

3.4.2 Access node resilience using MC-LAG and pseudowire redundancy

The following figure shows the use of both Multi-Chassis Link Aggregation (MC-LAG) in the access network and pseudowire redundancy in the core network to provide a resilient end-to-end VLL service to the customers.

Figure 28: Access node resilience



In this application, a new pseudowire status bit of active or standby indicates the status of the SAP in the MC-LAG instance in the 7210 SAS aggregation node. All spoke SDPs are of secondary type and there is no use of a primary pseudowire type for this mode of operation. Node A is in the active state according to its local MC-LAG instance and therefore advertises active status notification messages to both its peer pseudowire nodes, for example, nodes C and D. Node D performs the same operation. Node B is in the standby state according to the status of the SAP in its local MC-LAG instance and therefore advertises standby status notification messages to both nodes C and D. Node C performs the same operation.

7210 SAS node selects a pseudowire as the active path for forwarding packets when both the local pseudowire status and the received remote pseudowire status indicate active status. However, a 7210 SAS device in standby status according to the SAP in its local MC-LAG instance is capable of processing packets for a VLL service received over any of the pseudowires which are up. This is to avoid black holing of user traffic during transitions. The 7210 SAS standby node forwards these packets to the active node

bye the Inter-Chassis Backup pseudowire (ICB pseudowire) for this VLL service. An ICB is a spoke-SDP used by a MC-LAG node to backup a MC-LAG SAP during transitions. The same ICB can also be used by the peer MC-LAG node to protect against network failures causing the active pseudowire to go down.

Note that at configuration time, the user specifies a precedence parameter for each of the pseudowires which are part of the redundancy set as described in the application. A 7210 SAS node uses this to select which pseudowire to forward packet to in case both pseudowires show active/active for the local/remote status during transitions.

Only VLL service of type Epipe is supported in this application. Also, ICB spoke-SDP can only be added to the SAP side of the VLL cross-connect if the SAP is configured on a MC-LAG instance.

3.4.3 VLL resilience for a switched pseudowire path

The following figures show the use of both pseudowire redundancy and pseudowire switching to provide a resilient VLL service across multiple IGP areas in a provider network.

Figure 29: VLL resilience in a provider network

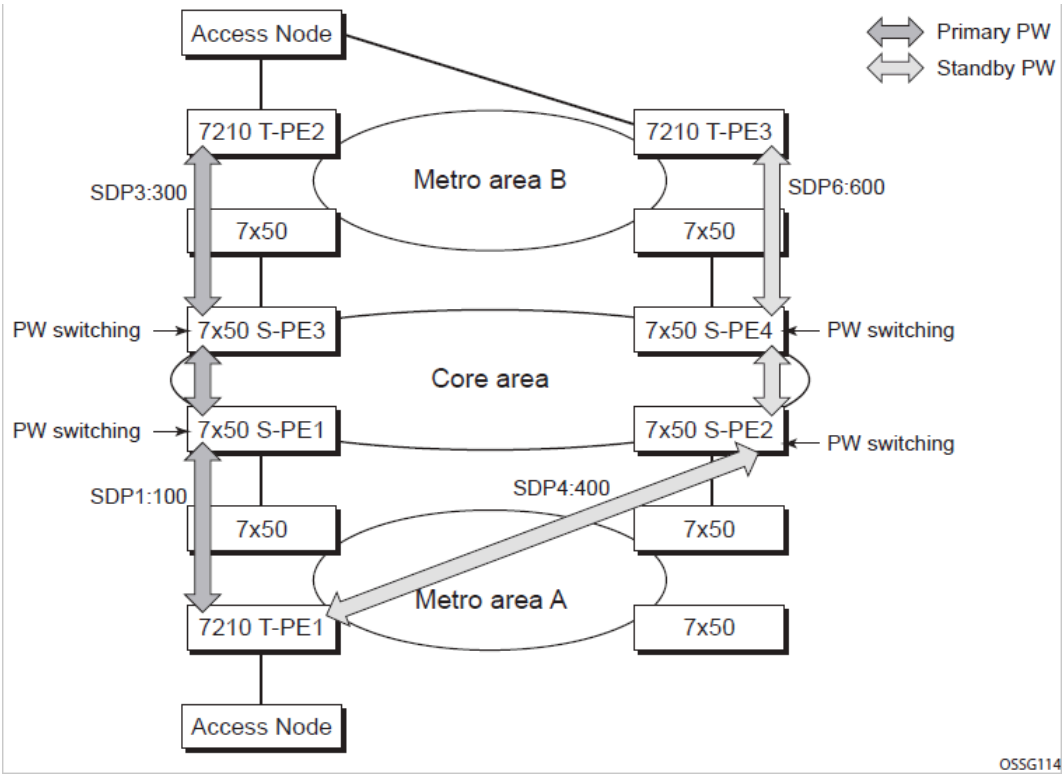
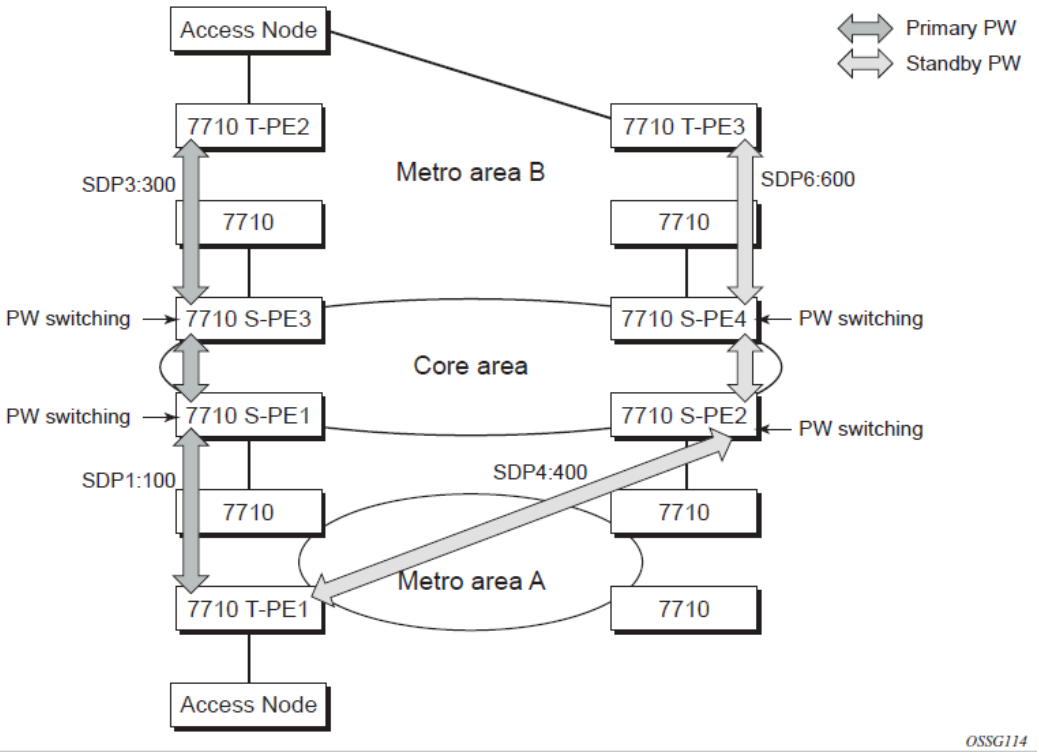


Figure 30: VLL resilience with pseudowire redundancy and switching



Pseudowire switching is a method for scaling a large network of VLL or VPLS services by removing the need for a full mesh of T-LDP sessions between the PE nodes as the number of these nodes grows over time.

Like in the application in VLL resilience with two destination PR nodes, the T-PE1 node switches the path of a VLL to a secondary standby pseudowire in the case of a network side failure causing the VLL binding status to be DOWN or if T-PE2 notified it that the remote SAP went down. This application requires that pseudowire status notification messages generated by either a T-PE node or a S-PE node be processed and relayed by the S-PE nodes.

It is possible that the secondary pseudowire path terminates on the same target PE as the primary, for example, T-PE2. This provides protection against network side failures but not against a remote SAP failure. When the target destination PE for the primary and secondary pseudowires is the same, T-PE1 does not switch the VLL path onto the secondary pseudowire upon receipt of a pseudowire status notification indicating the remote SAP is down because the status notification is sent over both the primary and secondary pseudowires.

However, the status notification on the primary pseudowire may arrive earlier than the one on the secondary pseudowire because of the differential delay between the paths. This causes T-PE1 to switch the path of the VLL to the secondary standby pseudowire and remain there until the status notification is cleared. At that point in time, the VLL path is switched back to the primary pseudowire because of the revertive behavior operation. The path does not switch back to a secondary path when it becomes up even if it has a higher precedence than the currently active secondary path.

3.5 Pseudowire redundancy service models

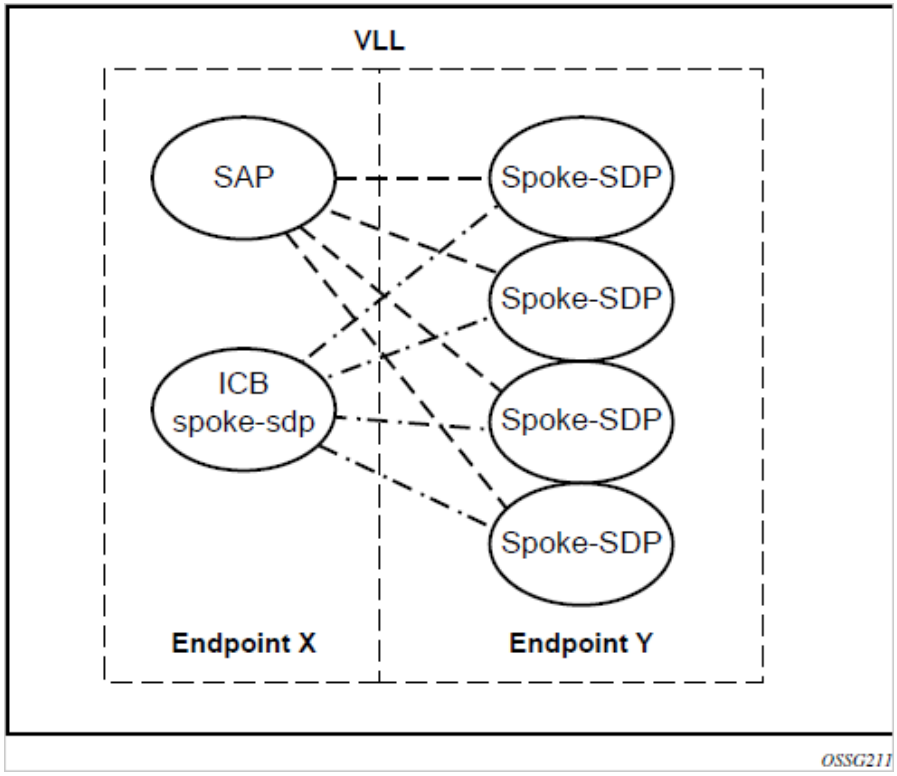
This section describes the various MC-LAG and pseudowire redundancy scenarios as well as the algorithm used to select the active transmit object in a VLL endpoint.

The redundant VLL service model is described in the following section, Redundant VLL service model.

3.5.1 Redundant VLL service model

To implement pseudowire redundancy, a VLL service accommodates more than a single object on the SAP side and on the spoke-SDP side. The following figure shows the model for a redundant VLL service based on the concept of endpoints.

Figure 31: Redundant VLL endpoint objects



A VLL service supports by default two implicit endpoints managed internally by the system. Each endpoint can only have one object, a SAP or a spoke-SDP.

To add more objects, up to two (2) explicitly named endpoints may be created per VLL service. The endpoint name is locally significant to the VLL service. They are referred to as endpoint 'X' and endpoint 'Y' as shown in the preceding figure.

The information in Figure 31: Redundant VLL endpoint objects is merely an example and that the "Y" endpoint can also have a SAP and an ICB spoke-SDP. The following details the four types of endpoint objects supported and the rules used when associating them with an endpoint of a VLL service:

- **SAP**

  There can only be a maximum of one SAP per VLL endpoint.

- **Primary spoke-SDP**

  The VLL service always uses this pseudowire and only switches to a secondary pseudowire when it is down the VLL service switches the path to the primary pseudowire when it is back up. The user can configure a timer to delay reverting back to primary or to never revert. There can only be a maximum of one primary spoke-SDP per VLL endpoint.

- **Secondary spoke-SDP**

  There can be a maximum of four secondary spoke-SDP per endpoint. The user can configure the precedence of a secondary pseudowire to indicate the order in which a secondary pseudowire is activated.

- **Inter-Chassis Backup (ICB) spoke-SDP**

  Special pseudowire used for MC-LAG and pseudowire redundancy application. Forwarding between ICBs is blocked on the same node. The user has to explicitly indicate the spoke-SDP is actually an ICB at creation time. There are however a few scenarios (as follows) where the user can configure the spoke-SDP as ICB or as a regular spoke-SDP on a specific node. The CLI for those cases indicate both options.

A VLL service endpoint can only use a single active object to transmit at any specific time but can receive from all endpoint objects

An explicitly named endpoint can have a maximum of one SAP and one ICB. When a SAP is added to the endpoint, only one more object of type ICB spoke-SDP is allowed. The ICB spoke-SDP cannot be added to the endpoint if the SAP is not part of a MC-LAG instance. Conversely, a SAP which is not part of a MC-LAG instance cannot be added to an endpoint which already has an ICB spoke-SDP.

An explicitly named endpoint, which does not have a SAP object, can have a maximum of four spoke SDPs and can include any of the following:

- a single primary spoke-SDP
- one or many secondary spoke SDPs with precedence
- a single ICB spoke-SDP

3.5.2 T-LDP status notification handling rules

Using Figure 31: Redundant VLL endpoint objects as a reference, the following are the rules for generating, processing, and merging T-LDP status notifications in VLL service with endpoints. Note that any allowed combination of objects as specified in Redundant VLL service model can be used on endpoints "X" and "Y". The following sections refer to the specific combination objects in Figure 31: Redundant VLL endpoint objects as an example to describe the more general rules.

3.5.2.1 Processing endpoint SAP active/standby status bits

The advertised admin forwarding status of active/standby reflects the status of the local LAG SAP in MC-LAG application. If the SAP is not part of a MC-LAG instance, the forwarding status of active is always advertised.

When the SAP in endpoint "X" is part of a MC-LAG instance, a node must send T-LDP forwarding status bit of "SAP active/standby" over all "Y" endpoint spoke SDPs, except the ICB spoke-SDP, whenever this status changes. The status bit sent over the ICB is always zero (active by default).

When the SAP in endpoint "X" is not part of a MC-LAG instance, then the forwarding status sent over all "Y" endpoint spoke-SDPs should always be set to zero (active by default).

3.5.2.2 Processing and merging

Endpoint "X" is operationally up if at least one of its objects is operationally up. It is down if all its objects are operationally down.

If the SAP in endpoint "X" transitions locally to the down state, or received a SAP down notification by SAP-specific OAM signal, the node must send T-LDP SAP down status bits on the "Y" endpoint ICB spoke-SDP only. Ethernet SAP does not support SAP OAM protocol. All other SAP types cannot exist on the same endpoint as an ICB spoke-SDP because non Ethernet SAP cannot be part of a MC-LAG instance.

If the ICB spoke-SDP in endpoint "X" transitions locally to down state, the node must send T-LDP SDP-binding down status bits on this spoke-SDP.

If the ICB spoke-SDP in endpoint "X" received T-LDP SDP-binding down status bits or pseudowire not forwarding status bits, the node saves this status and takes no further action. The saved status is used for selecting the active transmit endpoint object.

If all objects in endpoint "X" transition locally to down state, or received a SAP down notification by remote T-LDP status bits or by SAP specific OAM signal, or received status bits of SDP-binding down, or received status bits of pseudowire not forwarding, the node must send status bits of SAP down over all "Y" endpoint spoke SDPs, including the ICB.

Endpoint "Y" is operationally up if at least one of its objects is operationally up. It is down if all its objects are operationally down.

If a spoke-SDP in endpoint "Y", including the ICB spoke-SDP, transitions locally to down state, the node must send T-LDP SDP-binding down status bits on this spoke-SDP.

If a spoke-SDP in endpoint "Y", including the ICB spoke-SDP, received T-LDP SAP down status bits, or received T-LDP SDP-binding down status bits, or received status bits of pseudowire not forwarding, the node saves this status and takes no further action. The saved status is used for selecting the active transmit endpoint object.

If all objects in endpoint "Y", except the ICB spoke-SDP, transition locally to down state, or received T-LDP SAP down status bits, or received T-LDP SDP-binding down status bits, or received status bits of pseudowire not forwarding, the node must send status bits of SDP-binding down over the "X" endpoint ICB spoke-SDP only.

If all objects in endpoint "Y" transition locally to down state, or received T-LDP SAP down status bits, or received T-LDP SDP-binding down status bits, or received status bits of pseudowire not forwarding, the node must send status bits of SDP-binding down over the "X" endpoint ICB spoke-SDP, and must send a SAP down notification on the "X" endpoint SAP by the SAP specific OAM signal if applicable. An Ethernet SAP does not support signaling status notifications.

3.6 Epipe configuration for MPLS-TP

Note: MPLS-TP PWs are supported in Epipe service. MPLS-TP is only supported on 7210 SAS-R6 and 7210 SAS-R12.

The following subsections describe how SDPs and spoke-SDPs are used with MPLS-TP LSPs and static PWs with MPLS-TP OAM.

3.6.1 SDPs

An SDP used for MPLS-TP supports the configuration of an MPLS-TP identifier as the far end address, as an alternative to an IP address. IP addresses are used if IP/MPLS LSPs are used by the SDP, or MPLS-TP tunnels identified by IPv4 source or destination addresses. MPLS-TP node identifiers are used if MPLS-TP tunnels are used.

Example: MPLS-TP options

```
config
    service
        sdp
            no description
            network-domain "default"
            signaling off
            far-end node-id 0.0.0.43 global-id 4294967295
            no mixed-lsp-mode
            no ldp
            no bgp-tunnel
            lsp "unnumberedLSP"
            no vlan-vc-etype
            no pbb-etype
            no path-mtu
            no adv-mtu-override
            keep-alive
                shutdown
                hello-time 10
                hold-down-time 10
                max-drop-count 3
                timeout 5
                no message-length
            exit
            no metric
            no collect-stats
            no accounting-policy
            binding
                no port
            exit
            no shutdown
-------------------------------------------
*A:7210SAS>config>service>sdp#
```

The **far-end node-id** *ip-address* **global-id** *global-id* command is used to associate an SDP far end with an MPLS-TP tunnel whose far end address is an MPLS-TP node ID. If the SDP is associated with an RSVP-TE LSP, then the far-end must be a routable IPv4 address.

The system accepts the **node-id** being entered as either 4-octet IP address format <a.b.c.d> or unsigned integer format.

The SDP far-end refers to an MPLS-TP **node-id** or **global-id** only if:

- delivery type is MPLS
- signaling is off
- keep-alive is disabled
- mixed-lsp-mode is disabled
- adv-mtu-override is disabled

An LSP is allowed to be configured only if the far-end info matches the LSP far-end info (whether MPLS-TP or RSVP):

- Only one LSP is allowed if the far-end is an MPLS-TP node-id or global-id.
- MPLS-TP or RSVP-TE LSPs are supported. However, note that LDP and BGP LSPs are not blocked in CLI.

Signaling TLDP or BGP is blocked if:

- far-end node-id/global-id configured
- control-channel-status enabled on any spoke (or mate vc-switched spoke)
- PW-path-id configured on any spoke (or mate vc-switched spoke)

The following commands are blocked if a far-end node-id or global-id is configured:

- **class-forwarding**
- **tunnel-far-end**
- **mixed-lsp-mode**
- **keep-alive**
- **ldp-tunnel** or **bgp-tunnel**
- **adv-mtu-override**

3.6.2 VLL spoke-SDP configuration

7210 SAS-R6 and 7210 SAS-R12 can be S-PE or T-PE and 7210 SAS-T can only be a T-PE. MPLS-TP OAM related commands are applicable to spoke SDPs configured under all services supported by MPLS-TP pseudowires. All commands and functions that are applicable to spoke SDPs in the current implementation are supported, except for those that explicitly depend on an LDP session on the SDP or stated as follows. Likewise, all existing functions on a specific service SAP are supported if the spoke-sdp that it is matched to is MPLS-TP.

The following describes how to configure MPLS-TP on an Epipe VLL. However, similar configuration applies to other VLL types.

A spoke-SDP bound to an SDP with the **mpls-tp** keyword cannot be enabled unless the ingress label, the egress label, the control word, and the **pw-path-id** are configured.

Example: VLL spoke-SDP configuration

```
*7210SAS>config>service>epipe# info
----------------------------------------------
            sap 1/1/10:1.111 create
            exit
            spoke-sdp 1:111 create
```

```
                [no] hash-label  ingress
                     vc-label 2111
                 exit
                 egress
                     vc-label 2111
                 exit
                 control-word
                 pw-path-id
                        agi 0:111
                        saii-type2 4294967295:0.0.0.42:111
                        taii-type2 4294967295:0.0.0.43:111
                 exit
                 no shutdown
            exit
            no shutdown
----------------------------------------------
*7210SAS>config>service>epipe#
```

The **pw-path-id** context is used to configure the end-to-end identifiers for a MS-PW. These may not coincide with those for the local node if the configuration is at an S-PE. The saii and taii are consistent with the source and destination of a label mapping message for a signaled PW.

The control-channel-status command enables static PW status signaling. This is valid for any spoke-SDP where signaling none is configured on the SDP (for example, where T-LDP signaling is not in use). The refresh timer is specified in seconds, from 10-65535, with a default of 0 (off). This value can only be changed if control-channel-status is shutdown. Commands that rely on PW status signaling are allowed if control-channel-status is configured for a spoke-SDP bound to an SDP with signaling off, but the system uses control channel status signaling instead of T-LDP status signaling. The ability to configure control channel status signaling on a specific spoke-SDP is determined by the credit-based algorithm described as follows. Control-channel-status for a particular PW only counts against the credit based algorithm if it is in a no shutdown state and has a non-zero refresh timer.

Note: A shutdown of a service results in the static PW status bits for the corresponding PW being set.

The spoke-SDP is held down unless the pw-path-id is complete.

The system accepts the node ID of the pw-path-id saii or taii being entered as either a 4-octet IP address format <a.b.c.d> or an unsigned integer format.

The control word must be enabled to use MPLS-TP on a spoke-SDP.

The pw-path-id only configurable if all of the following is true:

- network mode D
- SDP signaling is off
- control word enabled (control-word is disabled by default)
- service type Epipe or VPLS
- mate SDP signaling is off for VC-switched services
- an MPLS-TP node ID/global ID is configured under the **config>router>mpls>mpls-tp** context. This is required for OAM to provide a reply address.

In the VC switching case, if configured on a mate spoke-SDP, then the TAII of the spoke-SDP must match the SAII of its mate, and SAII of spoke-SDP has to match the TAII of its mate.

A **control-channel-status no shutdown** is allowed only if all of the following is true:

- Network-mode D

- SDP signaling is off
- Control-ord enabled (control-word by default is disabled)
- the service type is Epipe or VPLS interface
- Mate SDP signaling is off (in VC-switched services)
- PW status signaling is enabled (as follows)
- PW path ID is configured for this spoke

The hash-label option is only configurable if SDP far-end is not node-id or global-id.

The control channel status request mechanism is enabled when the **request-timer** *timer* parameter is non-zero. When enabled, this overrides the normal RFC-compliant refresh timer behavior. The refresh timer value in the status packet defined in RFC 6478 is always set to zero.

The refresh-timer in the sending node is taken from the request-timer. The two mechanisms are not compatible with each other. One node sends a request timer while the other is configured for refresh timer. In a specific node, the request timer can only be configured with both acknowledgment and refresh timers disabled.

When configured, the following procedures are used instead of the RFC 6478 procedures when a PW status changes.

The following commands are used to configure control channel status requests.

```
[no] control-channel-status
[no] refresh-timer <value> //0,10-65535, default:0
[no] request-timer
[timeout-multiplier <value>]
[no] shutdown
exit
request-timer <timer1>: 0, 10-65535, defaults: 0.
```

- This parameter determines the interval at which PW status messages, including a reliable delivery TLV, with the "request" bit set (as follows) are sent. This cannot be enabled if refresh-timer not equal to zero (0). retry-timer : 3-60s
- This parameter determines the timeout interval if no response to a PW status is received. This defaults to zero (0) when no retry-timer. timeout-multiplier <value> - 3-15.
- If a requesting node does not hear back after retry-timer times multiplier, then it must assume that the peer is down. This defaults to zero (0) when no retry-timer.

3.6.3 Credit-based algorithm

To constrain the CPU resources consumed processing control channel status messages, the system should implement a credit-based mechanism. If a user enables control channel status on a PW[n], then a number of credits c_n are consumed from a CPM-wide pool of max_credit credits. The number of credits consumed is inversely proportional to the configured refresh timer (the first three messages at 1 second interval do not count against the credit). If the current_credit <= 0, then control channel status signaling cannot be configured on a PW (but the PW can still be configured and enabled).

The following is an example algorithm:

If refresh timer > 0, c_n = 65535 / refresh_timer

Else c_n = 0.

For n=1, current_credit[n] = max-credits – c_n

Else current_credit [n] = current_credit [n-1] – c_n

If a PE with a non-zero refresh timer configured does not receive control channel status refresh messages for 3.5 time the specified timer value, then by default it times out and assumes a PW status of zero. A proprietary optional extension to the [RFC6478] protocol should be implemented to enable a node to resolve such a stale PW status condition by requesting the status from the far end node in such cases.

3.7 VLAN range for SAPs in an Epipe service

7210 SAS VLAN ranges provide a mechanism to group a range of VLAN IDs as a single service entity. This allows the operator to provide the service treatment (forwarding, ACL, QoS, Accounting, and others) to the group of VLAN IDs as a whole.

Note: Grouping a range of VLAN IDs to a SAP is supported only for Virtual Leased Lines (VLL) Ethernet services.

3.7.1 VLAN range SAPs feature support and restrictions

The following information describes VLAN range SAPs feature support and restrictions:

- The access SAPs that specify VLAN range values (using connection-profile) are allowed only in Epipe service. The system allows only one range SAP in an Epipe service. Any attempt to configure more than one range SAP in an Epipe service fails. Range SAP can be configured only on access ports.
- In network mode, the dot1q range sap is allowed to be configured in a service with **svc-sap-type** set to **any**.
- The access SAPs using VLAN range values are allowed only for dot1q encapsulation port or LAG. A connection profile is used to specify either range of VLAN IDs or individual VLANs to be grouped together in a single SAP.
- A "connection profile" is used to specify either range of VLAN IDs or individual VLANs to be grouped together in a single SAP.
- Multiple "connection-profile" can be used per port or Lag as long as the VLAN value specified by each of them does not overlap. The number of VLAN ranges available per port/LAG is limited. The available number must be shared among all the SAPs on the port/LAG.
- "Connection-profile", associated with a SAP cannot be modified. To modify a connection profile, it must be removed from all SAPs that are using it.

3.7.2 Processing behavior for SAPs using VLAN ranges in network mode

The access SAPs that specifies VLAN range values (using connection-profile) is allowed only in an Epipe service. The system allows only one range SAP in an Epipe service. Any attempt to configure more than one range SAP in an Epipe service fails. Range SAP can be configured only on access ports. The other endpoint in the Epipe service has to be a Q.* access SAP or a spoke-sdp (PW) in network mode.

The Spoke-SDP processing and forwarding behavior for packets received on range SAPs are listed as follows: No VLAN tags are removed/stripped on ingress of the access dot1q SAPs using VLAN range connection profile. When the other endpoint in the service is configured to be an Q1.* access SAP, 7210

adds another tag to the packet and forwards it out of that SAP. If the other endpoint in the service is configured to be a spoke-SDP whose **vc-type** is set to **vc-ether**, 7210 SAS adds the appropriate MPLS PW and LSP encapsulations and forwards it out of the SDP.

In the reverse direction, when the other endpoint is a Q1.* SAP and a packet is received on it, 7210 SAS removes the outermost VLAN tag and forwards the packet out of the access dot1q SAP using VLAN ranges. When the other endpoint is a spoke-SDP (whose **vc-type** is set to **vc-ether**), 7210 SAS removes the MPLS PW and LSP encapsulation and forwards the packet out of the access dot1q SAP using VLAN ranges. The system does not check if the VLAN in the packet matches the VLAN IDs of the dot1q access SAPs configured in the service:

- **ACL support**

  Filter policies are supported on SAP ingress. For more information about ACL on range SAPs, see the *7210 SAS-Mxp, R6, R12, S, Sx, T Router Configuration Guide*.

- **QoS**

  For ingress classification and metering with hierarchical metering support for SAP ingress, SAP ingress classification criteria available for use with VLAN range SAPs is similar to that available for other SAPs supported in an Epipe service. Dot1p based ingress classification uses the dot1p bits in the outermost VLAN tag for matching. On access egress, dot1p received from the SDP (on a network port) from another access port is preserved.

- The amount of hardware resources (such as CAM entries used for matching in QoS classification and ACL match, meters used in SAP ingress policy, and others.) consumed by a single range SAP is equivalent to the amount of resources consumed by a single SAP that specifies a single VLAN ID for service identification. That is, the hardware has the ability to match a range of VLAN values and therefore uses 'X' resources for a SAP using a VLAN range instead of X * n, where 'n' is the number of VLANs specified in the range and X is the amount of QoS or ACL resources needed.
- Ingress accounting support is similar to the support available for other SAPs in an Epipe service. Count of packets or octets received from individual VLANs configured in the connection profile is not available. No support for Egress SAP statistics and accounting is available.
- Mirroring is supported. In network mode, the use of service resiliency mechanisms such as MC-LAG and Epipe PW redundancy is supported.

3.8 VLL service considerations

This section describes various of the general service features and any special capabilities or considerations as they relate to VLL services.

3.8.1 SDPs

The most basic SDPs must have the following:

- a locally unique SDP identification (ID) number
- the system IP address of the originating and far-end routers
- an SDP encapsulation type, MPLS

3.8.1.1 SAP encapsulations

The Epipe service is designed to carry Ethernet frame payloads, so it can provide connectivity between any two SAPs that pass Ethernet frames. The following SAP encapsulations are supported on the Epipe service:

- Ethernet null
- Ethernet dot1q
- QinQ

While different encapsulation types can be used, encapsulation mismatch can occur if the encapsulation behavior is not understood by connecting devices and are unable to send and receive the expected traffic. For example, if the encapsulation type on one side of the Epipe is dot1q and the other is null, tagged traffic received on the null SAP can potentially be double tagged when it is transmitted out of the dot1q SAP.

3.8.1.2 QoS policies

Traffic Management - Traffic management of Ethernet VLLs is achieved through the application of ingress QoS policies to SAPs and access egress QoS policies applied to the port. All traffic management is forwarding-class aware and the SAP ingress QoS policy identifies the forwarding class based on the rules configured to isolate and match the traffic ingressing on the SAP. Forwarding classes are determined based on the Layer 2 (Dot1p, MAC) or Layer 3 (IP, DSCP) fields of contained packets and this association of forwarding class at the ingress determines both the queuing and the Dot1P bit setting of packets on the Ethernet VLL on the egress.

SAP ingress classification and Policing - The traffic at the SAP ingress is classified and metered according to the SLA parameters. All the traffic ingressing on the SAP is classified to a particular forwarding class. All the forwarding class is metered through and marked in-profile or put-profile based on the Meter parameters.

When applied to Epipe services, service ingress QoS policies only create the unicast defined in the policy. The multipoint are not created on the service. Note that both Layer 2 or Layer 3 criteria can be used in the QoS policies for traffic classification in a service.

Egress Network DOT1P Marking - Marking of IEEE DOT1P bits in VLAN tag is as per the FC-to-Dot1p map. For details see the default network QoS policy in the *7210 SAS-Mxp, R6, R12, S, Sx, T Quality of Service Guide*. This marking is applied at the port level on access ports and access uplink ports.

Ingress Network Classification - Ingress network classification is based on the Dot1p bits in the outer VLAN tag received on the access uplink port. Dot1p-to-FC mapping is based on the network ingress QoS policy.

3.8.1.3 Filter policies

7210 SAS Epipe services can have a single filter policy associated on both ingress and egress. Both MAC and IP filter policies can be used on Epipe services.

3.8.1.4 MAC resources

Epipe services are point-to-point Layer 2 VPNs capable of carrying any Ethernet payloads. Although an Epipe is a Layer 2 service, the 7210 SAS-R6 and 7210 SAS-R12 Epipe implementation does not perform MAC learning on the service, so Epipe services do not consume any MAC hardware resources.

3.9 Configuring a VLL service with CLI

This section provides information to configure Virtual Leased Line (VLL) services using the command line interface.

3.9.1 Basic configurations

3.9.2 Common configuration tasks

This section provides a brief overview of the tasks that must be performed to configure the VLL services and provides the CLI commands:

- Associate the service with a customer ID.
- Define SAP parameters:
  - Optional - select ingress QoS policies (configured in the **config>qos** context)
  - Optional - select accounting policy (configured in the **config>log** context)
- Define spoke-SDP parameters.
- Enable the service.

3.9.3 Configuring VLL components

This section provides VLL configuration examples for the VLL services.

3.9.3.1 Creating an Epipe service

Use the following syntax to create an Epipe service.

```
config>service#
    epipe service-id [customer customer-id] [create] [vpn vpn-id]
    description description-string
    no shutdown
```

For 7210 SAS-R6 and 7210 SAS-R12 devices:

```
config>service#
    epipe service-id [customer customer-id] [create] [vpn vpn-id][vc-switching] [svc-sap-type
 {any | qinq-inner-tag-preserve}]
    description description-string
```

```
    no shutdown
```

Example: Epipe configuration

The following example shows Epipe configuration output.

```
A:ALA-1>config>service# info
epipe 1 customer 1 vpn 1 vc-switching create
            description "Default epipe description for service id 1"
            spoke-sdp 1:1 vc-type vlan create
                description "Description for Sdp Bind 1 for Svc ID 1"
A:ALA-1>config>service# info
```

3.9.3.1.1 Configuring Epipe SAP parameters

A default QoS policy is applied to each ingress SAP. Additional QoS policies can be configured in the **config>qos** context. Filter policies are configured in the **config>filter** context and explicitly applied to a SAP. There are no default filter policies.

```
config>service# epipe service-id [customer customer-id]
    sap sap-id
    accounting-policy policy-id
    collect-stats
    description description-string
    no shutdown
    egress
        filter {ip ip-filter-name | mac mac-filter-name}
    ingress
        filter {ip ip-filter-name | mac mac-filter-name}
        qos policy-id
```

3.9.3.1.1.1 Local Epipe SAPs

To configure a basic local Epipe service, enter the **sap** *sap-id* command twice with different port IDs in the same service configuration.

By default, QoS policy ID 1 is applied to ingress service SAPS. Existing filter policies or other existing QoS policies can be associated with service SAPs on ingress and egress ports.

Ingress and Egress SAP parameters can be applied to local and distributed Epipe service SAPs.

Example: SAP configurations for a local Epipe service

This example displays the SAP configurations for local Epipe service 500 on SAP 1/1/2 and SAP 1/1/3 on ALA-1.

```
A:ALA-1>config>service# epipe 500 customer 5 create
config>service>epipe$ description "Local epipe service
config>service>epipe# sap 1/1/2 create
config>service>epipe>sap? ingress
config>service>epipe>sap>ingress# qos 20
config>service>epipe>sap>ingress# filter ip 1
config>service>epipe>sap>ingress# exit
config>service>epipe>sap# egress
config>service>epipe# sap 1/1/3 create
config>service>epipe>sap# ingress
```

```
config>service>epipe>sap>ingress# qos 555
config>service>epipe>sap>ingress# filter ip 1
config>service>epipe>sap>ingress# exit
config>service>epipe>sap# no shutdown
config>service>epipe>sap# exit

A:ALA-1>config>service# info
----------------------------------------------
...
        epipe 500 customer 5 create
            description "Local epipe service"
            sap 1/1/2 create
                ingress
                    qos 20
                    filter ip 1
                exit
            exit
            sap 1/1/3 create
                ingress
                    qos 555
                    filter ip 1
                exit
            exit
            no shutdown
        exit
```

3.9.4 Using spoke-SDP control words

The control word command provides the option to add a control word as part of the packet encapsulation for PW types for which the control word is optional. On 7210 SAS, an option is provided to enable it for Ethernet PW (Epipe). The control word may be needed because when ECMP is enabled on the network, packets of a specific PW may be spread over multiple ECMP paths if the hashing router mistakes the PW packet payload for an IPv4 or IPv6 packet. This occurs when the first nibble following the service label corresponds to a value of 4 or 6.

The control word negotiation procedures described in Section 6.2 of RFC 4447 are not supported and therefore the service only comes up if the same C bit value is signaled in both directions. If a spoke-SDP is configured to use the control word but the node receives a label mapping message with a C-bit clear, the node releases the label with an "Illegal C-bit" status code per Section 6.1 of RFC 4447. As soon as the user enables control of the remote peer, the remote peer withdraws its original label and sends a label mapping with the C-bit set to 1 and the VLL service is up in both nodes.

When the control word is enabled, VCCV packets also include the VCCV control word. In that case, the VCCV CC type 1 (OAM CW) is signaled in the VCCV parameter in the FEC. If the control word is disabled on the spoke-SDP, then the Router Alert label is used. In that case, VCCV CC type 2 is signaled. Note that for a multi-segment PW (MS-PW), the CC type 1 is the only supported and therefore the control word must be enabled on the spoke-SDP to be able to use VCCV ping and VCCV trace.

Example: Spoke-SDP control word configuration

The following example shows spoke-SDP control word configuration output.

```
-Dut-B>config>service>epipe# info
----------------------------------------------
description "Default epipe description for service id 2100"
sap 1/2/7:4 create
description "Default sap description for service id 2100"
exit
```

```
spoke-sdp 1:2001 create
control-word
exit
no shutdown
-----------------------------------------------
*A:ALA-Dut-B>config>service>epipe#
To disable the control word on spoke-sdp 1:2001:
*A:ALA-Dut-B>config>service>epipe# info
-----------------------------------------------
description "Default epipe description for service id 2100"
sap 1/2/7:4 create
description "Default sap description for service id 2100"
exit
spoke-sdp 1:2001 create
exit
no shutdown
-----------------------------------------------
*A:ALA-Dut-B>config>service>epipe#
```

3.9.5 Pseudowire configuration notes

The **vc-switching** parameter must be specified at the time the VLL service is created.

Note: When the **vc-switching** parameter is specified, you are configuring an S-PE. This is a pseudowire switching point (switching from one pseudowire to another). Therefore, you cannot add a SAP to the configuration.

Example: Error generated when adding a SAP to a pseudowire

The following example show the configuration when a SAP is added to a pseudowire. The CLI generates an error response if you attempt to create a SAP. VC switching is only needed on the pseudowire at the S-PE.

```
*A:ALA-701>config>service# epipe 28 customer 1 create vc-switching
*A:ALA-701>config>service>epipe$ sap 1/1/3 create
MINOR: SVCMGR #1311 SAP is not allowed under PW switching service
*A:ALA-701>config>service>epipe$
```

Use the following syntax to create pseudowire switching VLL services.

```
config>service# epipe service-id [customer customer-id][vpn vpn-id] [vc-
switching]
description description-string
spoke-sdp sdp-id:vc-id
```

Example: Configuring VLL pseudowiare switching services

The following example shows command usage to configure VLL pseudowire switching services.

```
*A:7210SAS>config>service# info
.............
epipe 1 customer 1 vpn 1 vc-switching create
            description "Default epipe description for service id 1"
            spoke-sdp 1:1 vc-type vlan create
                description "Description for Sdp Bind 1 for Svc ID 1"
                ingress
                    vc-label 4501
                exit
```

```
                egress
                    vc-label 4501
                exit
                control-word
                pw-path-id
                        agi 1:1
                        saii-type2 1:0.0.0.2:1
                        taii-type2 1:0.0.0.1:1
                exit
                control-channel-status
                    refresh-timer 10
                    no shutdown
                exit
                no shutdown
            exit
            spoke-sdp 1001:1 vc-type vlan create
                description "Description for Sdp Bind 1001 for Svc ID 1"
                ingress
                    vc-label 5501
                exit
                egress
                    vc-label 5501
                exit
                control-word
                pw-path-id
                        agi 1:1
                        saii-type2 1:0.0.0.1:1
                        taii-type2 1:0.0.0.2:1
                exit
                control-channel-status
                    refresh-timer 10
                    no shutdown
                exit
                no shutdown
            exit
            no shutdown
        exit
-------------------------------------------
*A:7210SAS>config>service#
```

Example: S-PE1 configuration

Note: Note that specifying the **vc-switching** parameter enables a VC cross-connect so the service manager does not signal the VC label mapping immediately but puts this into passive mode.

The following example shows configuration output for S-PE1.

```
*A:ALA-S-PE1>config>service>epipe# info
-------------------------------------------
...
spoke-sdp 2:200 create
exit
spoke-sdp 3:300 create
exit
no shutdown
-------------------------------------------
*A:ALA-S-PE1>config>service>epipe#
```

Example: S-PE2 configuration

Note: Note that specifying the **vc-switching** parameter enables a VC cross-connect so the service manager does not signal the VC label mapping immediately but puts this into passive mode.

The following example shows configuration output for S-PE2.

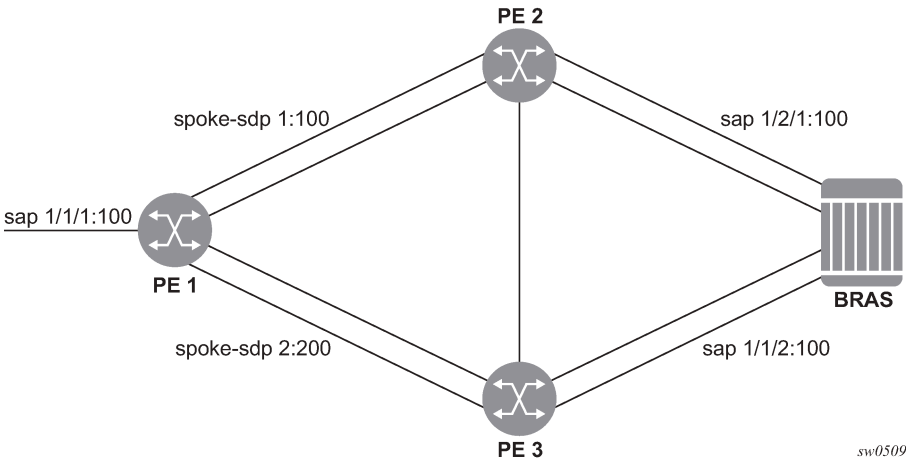
```
*A:ALA-S-PE2>config>service>epipe# info
----------------------------------------------
...
spoke-sdp 2:200 create
exit
spoke-sdp 3:300 create
exit
no shutdown
----------------------------------------------
*A:ALA-S-PE2>config>service>epipe#
```

3.9.6 Configuring VLL resilience

The following figure shows an example to create VLL resilience.

Note: The zero revert-time value means that the VLL path switches back to the primary immediately after it comes back up.

Figure 32: VLL resilience



Example: PE1 configuration output

The following example shows configuration output on PE1.

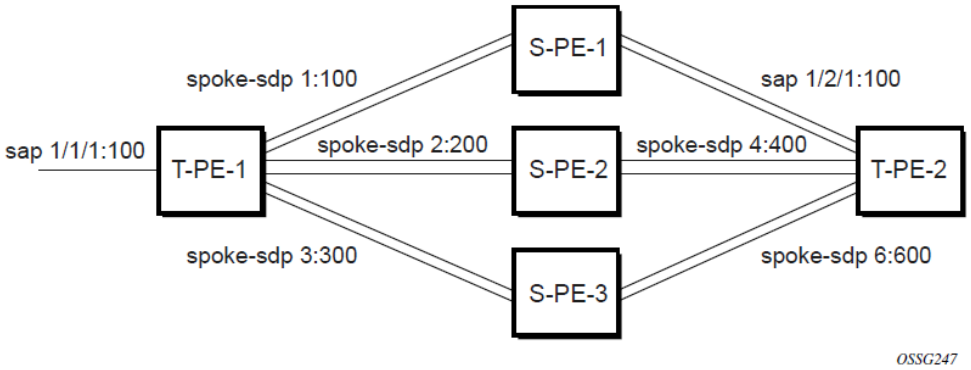
```
*A:ALA-48>config>service>epipe# info
----------------------------------------------
            endpoint "x" create
            exit
            endpoint "y" create
            exit
            spoke-sdp 1:100 endpoint "y" create
```

```
                precedence primary
            exit
            spoke-sdp 2:200 endpoint "y" create
                precedence 1
            exit
            no shutdown
----------------------------------------------
*A:ALA-48>config>service>epipe#
```

3.9.7 Configuring VLL resilience for a switched pseudowire path

The following figure shows an example to create VLL resilience with pseudowire switching.

Figure 33: VLL resilience with pseudowire switching



Example: T-PE1 configuration output

The following example shows configuration output on TPE1.

```
*A:ALA-48>config>service>epipe# info
----------------------------------------------
            endpoint "x" create
            exit
            endpoint "y" create
            exit
            sap 1/1/1:100 endpoint "x" create
            exit
            spoke-sdp 1:100 endpoint "y" create
                precedence primary
            exit
            spoke-sdp 2:200 endpoint "y" create
                precedence 1
            exit
            spoke-sdp 3:300 endpoint "y" create
                precedence 1
            exit
            no shutdown
----------------------------------------------
*A:ALA-48>config>service>epipe#
```

Example: T-PE2 configuration output

The following example shows configuration output on TPE2.

```
*A:ALA-49>config>service>epipe# info
----------------------------------------------
            endpoint "x" create
            exit
            endpoint "y" create
                revert-time 100
            exit
            spoke-sdp 4:400 endpoint "y" create
                precedence primary
            exit
            spoke-sdp 5:500 endpoint "y" create
                precedence 1
            exit
            spoke-sdp 6:600 endpoint "y" create
                precedence 1
            exit
            no shutdown
----------------------------------------------
*A:ALA-49>config>service>epipe#
```

Example: S-PE1 configuration output

The following example shows configuration output on S-PE1.

```
*A:ALA-50>config>service>epipe# info
----------------------------------------------
...
            spoke-sdp 1:100 create
            exit
            spoke-sdp 4:400 create
            exit
            no shutdown
----------------------------------------------
*A:ALA-49>config>service>epipe#
```

3.9.8 Service management tasks

This section describes the Epipe service management tasks.

3.9.8.1 Modifying Epipe service parameters

Example: Adding an accounting policy to an existing SAP

The following example shows adding an accounting policy to an existing SAP.

```
config>service# epipe 2
config>service>epipe# sap
config>service>epipe>sap# accounting-policy 14
config>service>epipe>sap# exit
```

Example: SAP configuration output

The following example shows SAP configuration output.

```
ALA-1>config>service# info
----------------------------------------------
epipe 2 customer 6 vpn 2 create
            description "Distributed Epipe service to east coast"
            sap 1/1/3:21 create
accounting-policy 14
            exit
            no shutdown
        exit
----------------------------------------------
ALA-1>config>service#
```

3.9.8.2 Disabling an Epipe service

Use the following syntax to shut down an Epipe service without deleting the service parameters.

```
config>service# epipe service-id
    shutdown
```

Example: Disabling an Epipe service

```
config>service# epipe 2
config>service>epipe# shutdown
config>service>epipe# exit
```

3.9.8.3 Re-enabling an Epipe service

Use the following syntax to re-enable an Epipe service that was shut down.

```
config>service# epipe service-id
    no shutdown
```

Example: Re-enabling an Epipe service

```
config>service# epipe 2
config>service>epipe# no shutdown
config>service>epipe# exit
```

3.9.8.4 Deleting an Epipe service

Perform the following steps before deleting an Epipe service:

1. Shut down the SAP.
2. Delete the SAP.
3. Shut down the service.

Use the following syntax to delete an Epipe service.

```
config>service
    [no] epipe service-id
    shutdown
    [no] sap sap-id
        shutdown
```

Example: Deleting an Epipe service

```
config>service# epipe 2
config>service>epipe# sap
config>service>epipe>sap# shutdown
config>service>epipe>sap# exit
config>service>epipe# no sap
config>service>epipe# epipe 2
config>service>epipe# shutdown
config>service>epipe# exit
config>service# no epipe 2
```

3.10 VLL services command reference

- Command hierarchies
- Command descriptions

3.10.1 Command hierarchies

- Epipe service configuration commands
- Connection profile commands
- Show commands
- Clear commands
- Debug commands

3.10.1.1 Epipe service configuration commands

- Epipe global commands in network mode
- Epipe SAP configuration commands
- Epipe SAP meter override commands
- Epipe SAP statistics commands
- Epipe spoke-SDP configuration commands
- Epipe SAP filter and QoS configuration commands

3.10.1.1.1 Epipe global commands in network mode

```
config
    - service
        - [no] epipe service-id [customer customer-id] [create] [vpn vpn-id] [vc-switching]
 [svc-sap-type {any | qinq-inner-tag-preserve}]
        - no epipe service-id
            - description description-string
            - no description
            - [no] endpoint endpoint-name [create]
                - active-hold-delay active-endpoint-delay
                - no active-hold-delay
                - revert-time [revert-time | infinite]
                - no revert-time
                - standby-signaling-master
                - [no] standby-signaling-master
            - sap sap-id [create]
            - no sap sap-id
            - service-mtu octetsno service-mtu
            - [no] service-mtu-check[no] shutdown
            - spoke-sdp sdp-id[:vc-id] [vc-type {ether | vlan}] [create] [no-endpoint]
            - spoke-sdp sdp-id[:vc-id] [vc-type {ether | vlan}] [create] endpoint
            - no spoke-sdp sdp-id[:vc-id]
            - spoke-sdp-fec spoke-sdp-fec-id [fec fec-type] [aii-type aii-type] [create]
            - spoke-sdp-fec spoke-sdp-fec-id no-endpoint
            - spoke-sdp-fec spoke-sdp-fec-id [fec fec-type] [aii-type aii-type] [create]
 endpoint name [icb]
            - no spoke-sdp-fec spoke-sdp-fec-id
```

3.10.1.1.2 Epipe SAP configuration commands

```
config
    - service
        - [no] epipe service-id [customer customer-id] [create] [vpn vpn-id] [vc-switching]
 [svc-sap-type {any | qinq-inner-tag-preserve}]
        - no epipe service-id
            - sap sap-id [no-endpoint] [create]
            - sap sap-id [endpoint endpoint-name] [create]
            - no sap sap-id
                - accounting-policy acct-policy-id
                - no accounting-policy acct-policy-id
                - [no] collect-stats
                - description description-string
                - no description
                - eth-cfm
                    - [no] ais-enable
                    - [no] mep mep-id domain md-index association ma-index [direction {up |
 down}] primary-vlan-enable
                        - [no] ais-enable
                            - [no] client-meg-level [[level [level ...]]
                            - [no] interval {1 | 60}
                            - [no] priority priority-value
                        - [no] ccm-enable
                        - [no] ccm-ltm-priority priority
                        - [no] description
                        - [no] eth-test-enable
                            - [no] test-pattern {all-zeros | all-ones} [crc-enable]
                        - [no] fault-propagation-enable {use-if-tlv | suspendccm}
                        - [no] mac-address mac-address
```

```
                        - [no] one-way-delay-threshold seconds
                    - mip [mac mac address]
                    - mip default-mac
                    - no mip
                    - mep
                        - [no] ccm-enable
                        - ccm-ltm-priority priority
                        - no ccm-ltm-priority
                        - [no] eth-test-enable
                            - test-pattern {all-zeros | all-ones} [crc-enable]
                            - no test-pattern
                        - low-priority-defect {allDef | macRemErrXcon | remErrXcon | errXcon |
 xcon | noXcon}
                        - mac-address mac-address
                        - no mac-address
                        - [no] shutdown
                - ethernet
                    - [no] llf
                - [no] ignore-oper-down
                - [no] shutdown
```

3.10.1.1.3 Epipe SAP meter override commands

```
config
    - service
        - [no] epipe service-id [customer customer-id] [create] [vpn vpn-id] [vc-switching]
 [svc-sap-type {any | qinq-inner-tag-preserve}]
        - no epipe service-id
            - no sap sap-id
                - ingress
                    - meter-override
                        - meter meter-id [create]
                        - no meter meter-id
                            - adaptation-rule  [pir adaptation-rule] [cir adaptation-rule]
                            -  cbs size [kbits | bytes | kbytes]
                            - no cbs
                            - mbs size [kbits | bytes | kbytes]
                            - no mbs
                            - mode mode
                            - no mode
                            - rate cir cir-rate [pir pir-rate]
                            - no rate
```

3.10.1.1.4 Epipe SAP statistics commands

```
config
    - service
        - [no] epipe service-id [customer customer-id] [create] [vpn vpn-id] [vc-switching]
 [svc-sap-type {any | qinq-inner-tag-preserve}]
        - no epipe service-id
            - no sap sap-id
                - statistics
                    - ingress
                        - counter-mode {in-out-profile-count | forward-drop-count}
                        - [no] drop-count-extra-vlan-tag-pkts
                        - [no] shutdown
```

3.10.1.1.5 Epipe spoke-SDP configuration commands

```
config
    - service
        - [no] epipe service-id [customer customer-id] [create] [vpn vpn-id] [vc-switching]
 [svc-sap-type {any | qinq-inner-tag-preserve}]
        - no epipe service-id
            - spoke-sdp sdp-id[:vc-id] [vc-type {ether | vlan}] [create] [no-endpoint]
            - spoke-sdp sdp-id[:vc-id] [vc-type {ether | vlan}] [create]  endpoint
            - no spoke-sdp sdp-id[:vc-id]
                - accounting-policy acct-policy-id
                - no accounting-policy
                - [no] collect-stats
                - [no] control-word
                - control-channel-status
                    - acknowledgment
                    - no acknowledgment
                    - refresh-timer seconds
                    - no refresh-timer
                    - request-timer request-timer request-timer-secs retry-timer retry-timer-
secs timeout-multiplier multiplier
                - [no] description
                - [no] egress
                    - [no] vc-label egress-vc-label
                - eth-cfm
                    - [no] ais-enable
                    - [no] mep mep-id domain md-index association ma-index [direction {up |
 down}]
                        - [no] ais-enable
                            - [no] client-meg-level [[level [level ...]]
                            - [no] interval {1 | 60}
                            - [no] priority priority-value
                        - [no] ccm-enable
                        - [no] ccm-ltm-priority priority
                        - [no] description
                        - [no] eth-test-enable
                            - [no] test-pattern {all-zeros | all-ones} [crc-enable]
                        - [no] fault-propagation-enable {use-if-tlv | suspendccm}
                        - low-priority-defect {allDef | macRemErrXcon | remErrXcon | errXcon |
 xcon | noXcon}
                        - [no] mac-address mac-address
                        - [no] one-way-delay-threshold seconds
                        - [no] shutdown
                    - mip [mac mac address]
                    - mip default-mac
                    - no mip
                - [no] force-vlan-vc-forwarding
                - hash-label
                - hash-label [signal-capability]
                - no hash-label
                - [no] ingress
                    - [no] vc-label egress-vc-label
                - precedence [precedence-value| primary]
                - no precedence
                - [no] pw-path-id
                    - agi attachment-group-identifier
                    - no agi
                    - no saii-type2
                    - saii-type2 global-id:node-id:ac-id
                    - no taii-type2
                    - taii-type2 global-id:node-id:ac-id
                - no pw-status-signaling
```

```
                - pw-status-signaling
                - [no] shutdown
                - vlan-vc-tag vlan-id
                - no vlan-vc-tag [vlan-id]
            - spoke-sdp-fec spoke-sdp-fec-id [fec fec-type] [aii-type aii-type] [create]
            - spoke-sdp-fec spoke-sdp-fec-id no-endpoint
            - spoke-sdp-fec spoke-sdp-fec-id [fec fec-type] [aii-type aii-type] [create]
endpoint name [icb]
            - no spoke-sdp-fec spoke-sdp-fec-id
                - [no] auto-config
                - path name
                - no path
                - precedence prec-value
                - precedence primary
                - no precedence
                - pw-template-bind policy-id
                - no pw-template-bind
                - retry-count retry-count
                - no retry-count
                - retry-timer retry-timer
                - no retry-timer
                - saii-type2 global-id:prefix:ac-id
                - no saii-type2
                - [no] shutdown
                - signaling signaling
                - [no] standby-signaling-slave
                - taii-type2 global-id:prefix:ac-id
                - no taii-type2
```

3.10.1.1.6 Epipe SAP filter and QoS configuration commands

```
config
    - service
        - [no] epipe service-id [customer customer-id] [create] [vpn vpn-id] [vc-switching]
[svc-sap-type {any | qinq-inner-tag-preserve}]
        - no epipe service-id
            - no sap sap-id
                - egress
                    - agg-rate-limit [cir cir-rate] [pir pir-rate]
                    - no agg-rate-limit
                    - aggregate-meter-rate rate-in-kbps [burst burst-in-kbits] [enable-stats]
                    - no aggregate-meter-rate
                    - filter [ip ip-filter-id]
                    - filter  [ipv6 ipv6 -filter-id]
                    - filter [mac mac-filter-id] (app
                    - no filter [ip ip-filter-id] [ ipv6 ipv6 -filter-id] [mac mac-filter-id]
                    - qos  policy-id
                    - no qos
                - ingress
                    - aggregate-meter-rate rate-in-kbps [burst burst-in-kbits]
                    - no aggregate-meter-rate
                    - filter [ip ip-filter-id]
                    - filter [ ipv6 ipv6-filter-id]
                    - filter [mac mac-filter-id]
                    - no filter [ip ip-filter-id] [ ipv6 ipv6-filter-id] [mac mac-filter-id]
                    - qos  policy-id [enable-table-classification]
                    - no qos
```

3.10.1.2 Connection profile commands

```
config
    - connection-profile conn-prof-id [create]
    - no connection-profile conn-prof-id
        - description description-string
        - no description
        - ethernet
            - no ranges
        - ranges  vlan ranges [vlan ranges...(up to 32 max)]
```

3.10.1.3 Show commands

```
show
    - service
        - id service-id
            - all
            - base
            - endpoint [endpoint-name]
            - labels
            - sap sap-id  [detail]
            - stp [sap-id] [detail]]
        - sap-using [sap sap-id]
        - sap-using [ingress | egress] filter filter-id
        - sap-using [ingress] qos-policy qos-policy-id
        - sap-using authentication-policy policy-name
        - service-using [epipe] [vpls] [mirror] [customer customer-id]
```

```
show
    - connection-profile [conn-prof-id] [associations]
```

3.10.1.4 Clear commands

```
clear
    - service
        - id service-id
        - statistics
            -  id service-id
            - counters
            - sap sap-id {all | counters | stp| l2pt}
```

3.10.1.5 Debug commands

```
debug
    - service
        - id service-id
            - sap sap-id
            - event-type {arp | config-change | oper-status-change}
            - sdp sdp-id:vc-id
```

3.10.2 Command descriptions

- Configuration commands
- Show commands
- Clear commands
- Debug commands

3.10.2.1 Configuration commands

3.10.2.1.1 Generic commands

shutdown

Syntax

[**no**] **shutdown**

Context

config>service>epipe

config>service>epipe>sap

config>service>epipe>sap>eth-cfm>mep

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

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

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

Services are created in the administratively down (**shutdown**) state. When a **no shutdown** command is entered, the service becomes administratively up and then tries to enter the operationally up state.

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

description

Syntax

description *description-string*

no description

Context

config>service>epipe

config>service>epipe>sap

config>service>epipe>spoke-sdp

config>connection-profile

Platforms

Supported on all 7210 SAS platforms as described in this document

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 identify the content in the configuration file.

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

Parameters

string

Specifies the description character string. Allowed values are any string up to 80 characters composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

eth-cfm

Syntax

eth-cfm

Context

config>service>vpls

config>service>vpls>mesh-sdp

config>service>vpls>spoke-sdp

config>service>epipe>sap

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

Commands in this context configure ETH-CFM parameters.

mep

Syntax

mep *mep-id* **domain** *md-index* **association** *ma-index* [**direction** {**up** | **down**}] **primary-vlan-enable**

no mep *mep-id* **domain** *md-index* **association** *ma-index*

Context

config>service>epipe>sap>eth-cfm

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the Maintenance Endpoint (MEP).

The **no** form of this command reverts to the default values.

For more information about ETH-CFM support for different services, see the *7210 SAS-Mxp, R6, R12, S, Sx, T OAM and Diagnostics Guide*.

Parameters

mep-id

Specifies the MEP identifier.

Values 1 to 8191

md-index

Specifies the maintenance domain (MD) index value.

Values 1 to 4294967295

ma-index

Specifies the MA index value.

Values 1 to 4294967295

direction up | down

Indicates the direction in which the MEP faces on the bridge port. Direction is not supported when a MEP is created directly under the **vpls>eth-cfm** context (vMEP).

down — Keyword that sends ETH-CFM messages away from the MAC relay entity.

up — Keyword that sends ETH-CFM messages toward the MAC relay entity.

primary-vlan-enable

Provides a method for linking with the primary VLAN configured under the bridge-identifier for the MA. This is only allowed if the mhf-creation method is static. MIPs cannot be changed from or to primary VLAN functions without first being deleted.

This must be configured as part of the creation step and can be changed only by deleting the MEP and recreating it. Primary VLANs are supported only under Ethernet SAPs.

3.10.2.1.2 VLL global commands

epipe

Syntax

epipe *service-id* [**customer** *customer-id*] [**create**] [**vpn** *vpn-id*] [**vc-switching**] [**svc-sap-type** {**any** | **qinq-inner-tag-preserve**}]

no epipe *service-id*

Context

config>service

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures a point-to-point Epipe service instance. An Epipe connects two endpoints, defined as Service Access Points (SAPs). In a local service, the SAPs can be defined in one 7210 SAS node, and in a distributed service, the SAPs can be defined on two different 7210 SAS nodes.

Note:

- 7210 SAS platforms as described in this document support local SAP-to-SAP service.
- 7210 SAS platforms as described in this document support both local and distributed services.

MAC learning and filtering are not supported on an Epipe service.

When a service is created, the **customer** keyword and *customer-id* parameter must be specified to associate 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 has been created with a customer association, it is not possible to edit the customer association. The service must be deleted and recreated with a new customer association.

When a service is created, the use of the **customer** *customer-id* command is optional for navigating into the service configuration context. Edit a service with the incorrect *customer-id* value specified results in an error.

By default, no Epipe services exist until they are explicitly created with this command.

The **no** form of this command deletes the Epipe service instance with the specified *service-id*. The service cannot be deleted until the service has been shut down and all instances of SAPs, mesh SDPs, or spoke SDPs have been deleted from the service.

Parameters

service-id

Specifies the unique service identification number or string identifying the service in the service domain. This ID must be unique to this service and may not be used for any other service of any type. The *service-id* must be the same number used for every 7210 SAS on which this service is defined.

Values *service-id*: 1 to 2147483647 *svc-name*: 64 characters maximum

customer *customer-id*

Specifies the customer ID number to be associated with the service. This parameter is required on service creation and is optional for service editing or deletion.

Values 1 to 2147483647

vpn vpn-id

Specifies the VPN ID number, which allows you to identify virtual private networks (VPNs). If this parameter is not specified, the VPN ID uses the same number as the service ID.

Values 1 to 2147483647

Default null (0)

vc-switching

Specifies whether pseudowire switching signaling is used for the spoke-SDPs configured in the service.

svc-sap-type

Specifies the type of service and allowed SAPs in the service.

Values **any** — Specifies that, for network mode, all supported SAPs are allowed in the service. See QinQ SAP configuration restrictions for 7210 SAS in network mode only for information about restrictions related to QinQ SAPs.

qinq-inner-tag-preserve — Specifies that an Epipe service processes and forwards packets received with 3 or more tags on a QinQ SAP. See Support for processing of packets received with more than 2 tags on a QinQ SAP in Epipe service (only on 7210 SAS devices configured in network mode) for more information about available support and restrictions.

create

Keyword used to create the service instance. The **create** keyword requirement can be enabled or disabled in the **environment>create** context.

endpoint

Syntax

[**no**] **endpoint** *endpoint-name* [**create**]

Context

config>service>epipe

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures a service endpoint.

Parameters

endpoint-name

Specifies an endpoint name.

create

Mandatory keyword to create a service endpoint name.

active-hold-delay

Syntax

active-hold-delay *active-hold-delay*

no active-hold-delay

Context

config>service>epipe>endpoint

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command specifies that the node delays sending the change in the T-LDP status bits for the VLL endpoint when the MC-LAG transitions the LAG subgroup that hosts the SAP for this VLL endpoint from **active** to **standby** or when any object in the endpoint. For example, SAP, ICB, or regular spoke-SDP, transitions from up to down operational state.

By default, when the MC-LAG transitioned the LAG subgroup that hosts the SAP for this VLL endpoint from **active** to **standby**, the node immediately sends new T-LDP status bits indicating the new value of "standby" over the spoke SDPs that are on the mate-endpoint of the VLL. The same applies when an object in the endpoint changes an operational state from up to down.

A value of zero means that when the MC-LAG transitioned the LAG subgroup which hosts the SAP for this VLL endpoint from **active** to **standby**, the node sends immediately new T-LDP status bits indicating the new value of **standby** over the spoke SDPs which are on the mate-endpoint of the VLL. The same applies when any object in the endpoint changes an operational state from up to down.

There is no delay applied to the VLL endpoint status bit advertisement when the MC-LAG transitions the LAG subgroup that hosts the SAP from "standby" to "active" or when an object in the endpoint transitions to an operationally up state.

Default

0

Parameters

active-hold-delay

Specifies the active hold delay in 100s of milliseconds.

Values 0 to 60

revert-time

Syntax

revert-time [*revert-time* | **infinite**]

no revert-time

Context

config>service>epipe>endpoint

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the time to wait before reverting back to the primary spoke-SDP defined on this service endpoint, after having failed over to a backup spoke-SDP.

Parameters

revert-time

Specifies the time, in seconds, to wait before reverting to the primary SDP.

Values 0 to 600

infinite

Keyword that causes the endpoint to be non-revertive.

standby-signaling-master

Syntax

[**no**] **standby-signaling-master**

Context

config>service>vll>endpoint

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

When this command is enabled, the pseudowire standby bit (value 0x00000020) is sent to T-LDP peer for each spoke SDP of the endpoint that is selected as a standby.

This command cannot be used with a VLL mate SAP created on an MC-LAG or ICB. This command and the **vc-switching** parameter are mutually exclusive.

Default

no standby-signaling-master

service-mtu

Syntax

service-mtu *octets*

no service-mtu

Context

config>service>epipe

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the service payload (Maximum Transmission Unit – MTU), in bytes, for the service. This MTU value overrides the service-type default MTU. The service MTU defines the payload capabilities of the service. It is used by the system to validate the SAP and the SDP binding operational state within the service.

The service MTU and a SAP service delineation encapsulation overhead (that is, 4 bytes for a dot1q tag) is used to derive the required MTU of the physical port or channel on which the SAP was created. If the required payload is larger than the port or channel MTU, the SAP is placed in an inoperative state. If the required MTU is equal to or less than the port or channel MTU, the SAP can transition to the operative state.

If a service MTU, port or channel MTU, or path MTU is dynamically or administratively modified, all associated SAP and SDP binding operational states are automatically reevaluated.

To disable service MTU check, execute the command **no service-mtu-check**. Disabling service MTU check allows the packets to pass to the egress if the packet length is less than or equal to the MTU configured on the port.

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

Default

VPLS: 1514

Parameters

octets

Specifies the size of the MTU in octets, expressed as a decimal integer. The following table lists MTU values for specific VC types.

Table 24: MTU values for VC types

VC-type	Example service MTU	Advertised MTU
Ethernet	1514	1500
Ethernet (with preserved dot1q)	1518	1504
VPLS	1514	1500
VPLS (with preserved dot1q)	1518	1504
VLAN (dot1p transparent to MTU value)	1514	1500
VLAN (QinQ with preserved bottom Qtag)	1518	1504

Values 1 to 9194

service-mtu-check

Syntax

[**no**] **service-mtu-check**

Context

config>service>epipe

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

Disabling service MTU check allows the packets to pass to the egress if the packet length is less than or equal to the MTU configured on the port. The length of the packet sent from a SAP is limited only by the access port MTU. In case of a pseudowire, the length of a packet is limited by the network port MTU (including the MPLS encapsulation).

The **no** form of this command disables the service MTU check.

Note:
If TLDP is used for signaling, the configured value for **service-mtu** is used during pseudowire set up.

Default

enabled

3.10.2.1.3 VLL SAP commands

sap

Syntax

sap *sap-id* [**no-endpoint**] [**create**]

sap *sap-id* **endpoint** *endpoint-name* [**create**]

no sap *sap-id*

Context

config>service>epipe

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command creates a SAP within a service. A SAP is a combination of port and encapsulation parameters that identify the SAP on the interface and within the service. 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 does not exist on that object.

Enter an existing SAP without the **create** keyword to edit SAP parameters.

For ports in network mode, multiple SAPs on the same port can belong to the same service.

If a port is shut down, all SAPs on that port become operationally down. When a service is shut down, SAPs for the service are not displayed as operationally down, although all traffic traversing the service is discarded.

The operational state of a SAP is relative to the operational state of the port on which the SAP is defined.

The following encapsulations are supported:

- Ethernet access SAPs support null, dot1q
- Ethernet access-uplink SAPs support only QinQ encapsulation.

The **no** form of this command deletes the SAP with the specified port. When a SAP is deleted, all configuration parameters for the SAP are also deleted.

Special Cases

Default SAPs

A default SAP has the following format: port-id:*. This type of SAP is supported only on Ethernet MDAs, and its creation is allowed only in the scope of Layer 2 services (Epipe and VPLS).

Parameters

sap-id

Specifies the physical port identifier portion of the SAP. See Common CLI command descriptions for command syntax.

endpoint

Keyword that adds a SAP endpoint association.

no endpoint

Keyword that removes the association of a SAP with an explicit endpoint name.

create

Keyword used to create a SAP instance. The **create** keyword requirement can be enabled or disabled in the **environment>create** context.

tod-suite

Syntax

tod-suite *tod-suite-name*

no tod-suite

Context

config>service>epipe>sap

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

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

Default

no tod-suite

Parameters

tod-suite-name

Specifies a collection of policies (ACLs, QoS) including time-ranges that define the full or partial behavior of a SAP. The suite can be applied to more than one SAP.

accounting-policy

Syntax

accounting-policy *acct-policy-id*

no accounting-policy

Context

config>service>epipe>sap

config>service>epipe>spoke-sdp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command creates the accounting policy context that can be applied to a SAP or spoke-SDP.

An accounting policy must be defined before it can be associated with a SAP or spoke-SDP. If the *policy-id* does not exist, an error message is generated.

A maximum of one accounting policy can be associated with a SAP or spoke-SDP at one time. Accounting policies are configured in the **config>log** context.

The **no** form of this command removes the accounting policy association from the SAP or spoke-SDP, and the accounting policy reverts to the default.

Parameters

acct-policy-id

Specifies the accounting *policy-id*, as configured in the **config>log>accounting-policy** context.

Values 1 to 99

collect-stats

Syntax

[**no**] **collect-stats**

Context

config>service>epipe>sap

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables accounting and statistical data collection for either the SAP, network port, or IP interface. When applying accounting policies, by default the data is collected in the appropriate records and written to the designated billing file.

When the **no collect-stats** command is issued, the statistics are still accumulated by the cards. However, the CPU does not obtain the results and write them to the billing file. If a subsequent **collect-stats** command is issued, the counters written to the billing file include all the traffic while the **no collect-stats** command was in effect.

Default

no collect-stats

ethernet

Syntax

ethernet

Context

config>service>epipe>sap

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures Ethernet properties in this SAP.

llf

Syntax

[**no**] **llf**

Context

config>service>epipe>sap>ethernet

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables Link Loss Forwarding (LLF) on an Ethernet port. It provides an end-to-end OAM fault notification for Ethernet VLL service.

LLF on an Ethernet port brings down the port when there is a local fault on the pseudowire or service, or a remote fault on the SAP or pseudowire, signaled with label withdrawal or TLDP status bits. LLF stops signaling when the fault disappears.

The Ethernet port must be configured for null encapsulation.

The **no** form of this command disables LLF.

ignore-oper-down

Syntax

[**no**] **ignore-oper-down**

Context

config>service>epipe>sap

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This optional command configures a specific SAP to ignore the transition of the operational state to down when a SAP fails. Only a single SAP in an Epipe may use this option.

Default

no ignore-oper-down

mip

Syntax

mip [**mac** *mac-address*]

mip default-mac

no mip

Context

config>service>epipe>sap>eth-cfm

config>service>epipe>spoke-sdp>eth-cfm

config>service>vpls>sap>eth-cfm

config>service>vpls>spoke-sdp>eth-cfm

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables Maintenance Intermediate Points (MIPs) to be created if mhf-creation for the MA is configured using the default option.

The **no** form of this command deletes the MIP.

Default

no mip

Parameters

mac-address

Specifies the MAC address of the MIP.

Values 6-byte mac-address in the form of xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx of the MIP. The MAC must be unicast. Using the all zeros address is equivalent to the no form of this command.

default-mac

Keyword to change the MAC back to the default MAC without having to delete the MIP and reconfigure it.

3.10.2.1.4 Service filter and QoS policy commands

egress

Syntax

egress

Context

config>service>epipe>sap

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

Commands in this context configure egress SAP parameters.

agg-rate-limit

Syntax

agg-rate-limit [**cir** *cir-rate*] [**pir** *pir-rate*]

no agg-rate-limit

Context

config>service>epipe>sap>egress

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command defines a maximum total rate for all egress queues on a service SAP.

The SAP aggregate rate can be used only if SAP based-scheduling mode is configured at the port level. It is not supported in FC-based scheduling mode.

When configured in SAP-based scheduling mode, the egress port scheduler distributes the available bandwidth to all the SAPs configured on the port, up to the configured aggregate rate for the SAP.

The **no** form of this command removes the aggregate rate limit from the SAP.

Parameters

cir-rate

Specifies the CIR in kilobits per second. This parameter is supported only on the 7210 SAS-R6 and 7210 SAS-R12.

Values 0 to 10000000

pir-rate

Specifies the PIR in kilobits per second. This parameter is supported only on the 7210 SAS-R6 and 7210 SAS-R12.

Values 1 to 10000000, max

aggregate-meter-rate

Syntax

aggregate-meter-rate *rate-in-kbps* [**burst** *burst-in-kbits*] [**enable-stats**]

no aggregate-meter-rate

Context

config>service>epipe>sap>egress

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command associates a set of two counters to count total forwarded packets and octets and total dropped packets and octets. When enabled, the amount of resources required increases by twice the amount of resources taken up when counter is not used. If the **enable-stats** keyword is specified during the creation of the meter, the counter is allocated by the software, if available. To free up the counter and relinquish its use, use the **no aggregate-meter-rate** command, and then recreate the meter using the **aggregate-meter-rate** command.

If egress Frame-based accounting is used, the SAP egress aggregate meter rate accounts for the Ethernet frame overhead. The system accounts for 12 bytes of IFG and 8 bytes of start delimiter. Frame-based counting does not affect the count of octets maintained by the counter, if in use.

Note:

- Before enabling this command for a SAP, resources must be allocated to this feature from the egress internal TCAM resource pool using the **configure system resource-profile egress-**

internal-tcam egress-sap-aggregate-meter command. See the *7210 SAS-Mxp, R6, R12, S, Sx, T Basic System Configuration Guide* for more information.

- The egress aggregate meter is not FC aware. The forward and drop decisions are made based on the order the packets are sent out of the SAP by the egress port scheduler.

The **no** form of this command removes the egress aggregate policer from use.

Default

no aggregate-meter-rate

Parameters

rate-in-kbps

Specifies the rate in kilobits per second.

Values 1 to 100000000 | max

Default max

burst-in-kbits

Specifies the burst size for the policer in kilobits. The burst size cannot be configured without configuring the rate.

Values 4 to 2146959 | default

Default 512

enable-stats

Specifies that the counter is allocated by the software, if available.

filter

Syntax

filter [**ip** *ip-filter-id*]

filter [**ipv6** *ipv6-filter-id*]

filter [**mac** *mac-filter-id*]

no filter [**ip** *ip-filter-id*]

no filter [**ipv6** *ipv6-filter-id*]

no filter [**mac** *mac-filter-id*]

Context

config>service>epipe>sap>egress

config>service>epipe>sap>ingress

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command associates an IP filter policy with an ingress or egress SAP or IP interface.

Filter policies control the forwarding and dropping of packets based on IP matching criteria. Only one filter can be applied to a SAP at a time.

The **filter** command is used to associate a filter policy with a specified *filter-id* with an ingress or egress SAP. The *filter-id* must already be defined before the **filter** command is executed. If the filter policy does not exist, the operation fails and an error message is returned.

IP filters apply only to RFC 2427-routed IP packets. Frames that do not contain IP packets are not subject to the filter and are always passed, even if the default action of the filter is to drop.

Note:
For filter support available on different 7210 SAS platforms, see the *7210 SAS-Mxp, R6, R12, S, Sx, T Router Configuration Guide*.

The **no** form of this command removes any configured filter ID association with the SAP or IP interface. The filter ID is not removed from the system.

Special Cases

Epipe

Both MAC and IP filters are supported on an Epipe service SAP.

Parameters

ip *ip-filter-id*

Specifies the IP filter policy. The filter ID must already exist within the created IP filters.

Values 1 to 65535

ipv6 *ipv6-filter-id*

Specifies the IPv6 filter policy. The filter ID must already exist within the created IPv6 filters.

Values 1 to 65535

mac *mac-filter-id*

Specifies the MAC filter policy. The specified filter ID must already exist within the created MAC filters. The filter policy must already exist within the created MAC filters.

Values 1 to 65535

qos

Syntax

qos *policy-id*

qos *policy-id* [**enable-table-classification**]

no qos

Context

config>service>epipe>sap>egress

config>service>epipe>sap>ingress

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command associates a Quality of Service (QoS) policy with an ingress SAP.

QoS ingress policies are important for the enforcement of SLA agreements. The policy ID must be defined before associating the policy with a SAP or IP interface. If the *policy-id* does not exist, an error is returned.

The **qos** command is used to associate both ingress and egress QoS policies. The **qos** command allows ingress policies to be associated only on SAP or IP interface ingress, and allows egress policies only on SAP or IP interface egress. Attempts to associate a QoS policy of the wrong type returns an error.

Only one ingress QoS policy can be associated with a SAP or IP interface at one time. Attempts to associate a second policy of same or different type replaces the earlier one with the new policy.

On the 7210 SAS-R6 and 7210 SAS-R12 (ingress), using the **enable-table-classification** keyword enables the use of IP DSCP tables to assign FC and profile on a per-SAP ingress basis. The match-criteria configured from the service ingress policy, which require CAM resources, are ignored. Only meters from the service ingress policy are used (and the meters still require CAM resources). The IP DSCP classification policy configured in the SAP ingress policy is used to assign FC and profile. The default FC is assigned from the SAP ingress policy.

By default, if no specific QoS policy is associated with the SAP for ingress or egress, the default QoS policy is used.

The **no** form of this command removes the QoS policy association from the SAP, and the QoS policy reverts to the default.

Parameters

policy-id

Specifies the ingress or egress policy ID to associate with SAP on ingress or egress. The policy ID must already exist.

Values 1 to 65535

enable-table-classification

Keyword to enable the use of table-based classification instead of CAM-based classification at SAP ingress. The FC and profile are taken from the IP DSCP classification policy configured in the ingress policy, along with the meters from the SAP ingress policy. Match-criteria entries in the SAP ingress policy are ignored.

ingress

Syntax

ingress

Context

config>service>epipe>sap

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

Commands in this context configure ingress SAP QoS policies.

If no SAP ingress QoS policy is defined, the system default SAP ingress QoS policy is used for ingress processing.

aggregate-meter-rate

Syntax

aggregate-meter-rate *rate-in-kbps* [**burst** *burst-in-kbits*]

no aggregate-meter-rate

Context

config>service>epipe>sap>ingress

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the SAP ingress aggregate policer. The rate of the SAP ingress aggregate policer must be specified by the user. The user can optionally specify the burst size for the SAP aggregate policer. The aggregate policer monitors the ingress traffic on different FCs and determines the final disposition of the packet. The packet is either forwarded to an identified profile or dropped.

Note:
The sum of CIR of the individual FCs configured under the SAP cannot exceed the PIR rate configured for the SAP. The 7210 SAS software does not block this configuration, however it is not recommended.

When the SAP aggregate policer is configured, per FC policer can be configured only in "trtcm2" mode (RFC 4115).

Note:
The meter modes "srtcm" and "trtcm1" are used in the absence of an aggregate meter.

The SAP ingress meter counters increment the packet or octet counts based on the final disposition of the packet.

If ingress Frame-based accounting is used, the SAP aggregate meter rate accounts for the Ethernet frame overhead. The system accounts for 12 bytes of IFG and 8 bytes of start delimiter.

The **no** form of this command removes the aggregate policer from use.

Default

no aggregate-meter-rate

Parameters

rate-in-kbps

Specifies the rate in kilobits per second.

Values 1 to 100000000 | max

Default max

burst-in-kbits

Specifies the burst size for the policer in kilobits. The burst size cannot be configured without configuring the rate.

Values 4 to 2146959 | default

Default 512

The following table lists the final disposition of the packet based on the operating rate of the per-FC policer and the per-SAP aggregate policer or meter.

Table 25: Final disposition of packet

Per FC meter operating rate	Per FC assigned color	SAP aggregate meter operating rate	SAP aggregate meter color	Final packet color
Within CIR	Green	Within PIR	Green	Green or In-profile
Within CIR[12]	Green	Above PIR	Red	Green or In-profile
Above CIR, Within PIR	Yellow	Within PIR	Green	Yellow or Out-of-Profile
Above CIR, Within PIR	Yellow	Above PIR	Red	Red or Dropped
Above PIR	Red	Within PIR	Green	Red or Dropped
Above PIR	Red	Above PIR	Red	Red or

[12] This row is not recommended for use. For more information, see the Note in the aggregate-meter-rate command description.

Per FC meter operating rate	Per FC assigned color	SAP aggregate meter operating rate	SAP aggregate meter color	Final packet color
				Dropped

meter-override

Syntax

[**no**] **meter-override**

Context

config>service>epipe>sap>ingress

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures specific overrides to one or more meters created on the SAP through the sap-ingress QoS policies.

The **no** form of this command is used to remove existing meter overrides.

Default

no meter-override

meter

Syntax

meter *meter-id* [**create**]

no meter *meter-id*

Context

config>service>epipe>sap>ingress>meter-override

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables the context for specific overrides to a specific meter created on the SAP through a SAP ingress QoS policies.

The **no** form of this command is used to remove existing overrides for the specified *meter-id*.

Parameters

meter-id

This parameter is required when executing the **meter** command within the **meter-overrides** context. The specified *meter-id* must exist within the SAP ingress QoS policy applied to the SAP. If the meter is not currently used by any forwarding class or forwarding type mappings, the meter does not exist on the SAP. This does not preclude creating an override context for the *meter-id*.

create

Keyword that is required when a **meter** *meter-id* override node is being created and the system is configured to expect explicit confirmation that a new object is being created. When the system is not configured to expect explicit confirmation, the **create** keyword is not required.

adaptation-rule

Syntax

adaptation-rule [**pir** *adaptation-rule*] [**cir** *adaptation-rule*]

no adaptation-rule

Context

config>service>epipe>sap>ingress>meter-override>meter

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the override of specific attributes of the specified meter adaptation rule parameters. The adaptation rule controls the method used by the system to derive the operational CIR and PIR settings when the meter is provisioned in hardware. For the CIR and PIR parameters individually, the system attempts to find the best operational rate, depending on the defined constraint.

The **no** form of this command removes explicitly defined constraints used to derive the operational CIR and PIR created by the application of the policy. When a specific **adaptation-rule** is removed, the default constraints for **rate** and **cir** apply.

Default

no adaptation-rule

Parameters

pir

Specifies the constraints enforced when adapting the PIR rate defined within the **meter-override meter** *meter-id* command. The **pir** parameter requires a qualifier that defines

the constraint used when deriving the operational PIR for the queue. When the **meter-override** command is not specified, the default applies.

When the meter mode in use is "trtcm2," this parameter is interpreted as EIR value. See the description and relevant notes for meter modes in the *7210 SAS-Mxp, R6, R12, S, Sx, T Quality of Service Guide* for more information.

cir

Specifies the constraints enforced when adapting the CIR rate defined within the **meter-override meter** *meter-id* command. The **cir** parameter requires a qualifier that defines the constraint used when deriving the operational CIR for the queue. When the **cir** parameter is not specified, the default constraint applies.

adaptation-rule

Specifies the criteria to use to compute the operational CIR and PIR values for this meter, while maintaining a minimum offset.

Values **max** — The **max**, **min**, and **closest** options are mutually exclusive. When **max** (maximum) is defined, the operational PIR for the meter will be equal to or less than the administrative rate specified using the **meter-override** command.

min — The **min**, **max** and **closest** options are mutually exclusive. When **min** (minimum) is defined, the operational PIR for the queue will be equal to or greater than the administrative rate specified using the **meter-override** command.

closest — The **closest**, **min** and **max** options are mutually exclusive. When **closest** is defined, the operational PIR for the meter will be the rate closest to the rate specified using the **meter-override** command.

cbs

Syntax

cbs *size* [**kbits** | **bytes** | **kbytes**]

no cbs

Context

config>service>epipe>sap>ingress>meter-override>meter

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the override of the default CBS for the meter. The committed burst size parameter specifies the maximum burst size that can be transmitted by the source while still complying with the CIR. If the transmitted burst is lower than the CBS value, the packets are marked as in-profile by the meter to indicate that the traffic is complying with meter configured parameters.

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

Default

32 kbits

Parameters

size

Specifies the value in kilobits, bytes, or kilobytes.

Values kbits: 4 to 2146959 | default
bytes: 512 to 274810752
kbytes: 1 to 268369

mbs

Syntax

mbs *size* [**kbits** | **bytes** | **kbytes**]

no mbs

Context

config>service>epipe>sap>ingress>meter-override>meter

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures a mechanism to override the default MBS for the meter. The maximum burst size parameter specifies the maximum burst size that can be transmitted by the source while still complying with the CIR. If the transmitted burst is lower than the MBS value then the packets are marked as in-profile by the meter to indicate that the traffic is complying with meter configured parameters.

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

Default

512kbits

Parameters

size

Specifies the value in kilobits, bytes, or kilobytes.

Values kbits: 4 to 2146959 | default
bytes: 512 to 274810752
kbytes: 1 to 268369

mode

Syntax

mode *mode*

no mode

Context

config>service>epipe>sap>ingress>meter-override>meter

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command overrides the SAP ingress QoS policy configured mode parameters for the specified meter-id.

The **no** form of this command restores the policy defined metering and profiling mode to a meter.

Parameters

mode

Specifies the rate mode of the meter-override.

Values trtcm1, trtcm2, srtcm

rate

Syntax

rate cir *cir-rate* [**pir** *pir-rate*]

no rate

Context

config>service>epipe>sap>ingress>meter-override>meter

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command overrides the SAP ingress QoS policy configured rate parameters for the specified meter-id.

The **max** default specifies the amount of bandwidth in kilobits per second (thousand bits per second). The **max** value is mutually exclusive to the *pir-rate* value.

The **no** form of this command reverts the policy defined metering and profiling rate to a meter.

Default

max

Parameters

pir-rate

Defines the administrative PIR rate, in kilobits, for the queue. When the **rate** command is executed, a valid PIR setting must be explicitly defined. When the **rate** command has not been executed, the default PIR of **max** is assumed. Fractional values are not allowed and must be specified as a positive integer.

When the meter mode is set to "trtcm2" the PIR value is interpreted as the EIR value. See the *7210 SAS-Mxp, R6, R12, S, Sx, T Quality of Service Guide* for more information.

The actual PIR rate is dependent on the queue **adaptation-rule** parameters and the hardware where the queue is provisioned.

Values 0 to 20000000 | max

Default max

cir-rate

Specifies to override the default administrative CIR used by the queue. When the **rate** command is executed, a CIR setting is optional. When the **rate** command has not been executed or the **cir** parameter is not explicitly specified, the default CIR (0) is assumed.

Fractional values are not allowed and must be specified as a positive integer.

Values 0 to 20000000 | max

Default 0

statistics

Syntax

statistics

Context

config>service>epipe>sap

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

Commands in this context configure the counters associated with SAP ingress and egress.

ingress

Syntax

ingress

Context

config>service>epipe>sap>statistics

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

Commands in this context configure the ingress SAP statistics counter.

counter-mode

Syntax

counter-mode {**in-out-profile-count**| **forward-drop-count**}

Context

config>service>epipe>sap>statistics>ingress

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command sets the counter mode for the counters associated with SAP ingress meters (also known as policers). A pair of counters is available with each meter. These counters count different events based on the counter mode value.

Note:

- The counter mode can be changed if an accounting policy is associated with a SAP. If the counter mode is changed, the counters associated with the meter are reset and the counts are cleared. If an accounting policy is in use when the counter mode is changed, a new record is written into the current accounting file.
- The configuration information is not saved across a reboot.

Perform the following sequence of commands on the specified SAP to ensure the correct statistics are collected when the counter-mode is changed.

1. Execute the **config service epipe sap no collect-stats** command to disable the writing of accounting records for the SAP.
2. Change the counter-mode to the required option by executing the **config service epipe sap counter-mode** {**in-out-profile-count** | **forward-drop-count**} command.

3. Execute the **config service epipe sap collect-stats** command to enable the writing of accounting records for the SAP.

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

Default

in-out-profile-count

Parameters

forward-drop-count

When this parameter is specified, one counter counts the forwarded packets and octets received on ingress of a SAP and another counts the dropped packets. The forwarded count is the sum of in-profile and out-of-profile packets/octets received on SAP ingress. The dropped count is count of packets/octets dropped by the policer. A packet is determined to be in-profile or out-of-profile based on the meter rate parameters configured. A packet is dropped by the policer if it exceeds the configured PIR rate. The in-profile count and out-of-profile count is not individually available when operating in this mode.

in-out-profile-count

When this parameter is specifies, one counter counts the total in-profile packets and octets received on ingress of a SAP and another counts the total out-of-profile packets and octets received on ingress of a SAP. A packet is determined to be in-profile or out-of-profile based on the meter rate parameters configured. A packet is dropped by the policer if it exceeds the configured PIR rate. Dropped counts are not maintained in hardware when this mode is used. It is obtained by subtracting the sum of in-profile count and out-of-profile count from the total SAP ingress received count and displayed.

drop-count-extra-vlan-tag-pkts

Syntax

[**no**] **drop-count-extra-vlan-tag-pkts**

Context

config>service>epipe>sap>statistics>ingress

config>service>epipe>spoke-sdp>statistics>ingress

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command associates a counter, which enables the counting of extra VLAN-tag dropped packets for the SAP or spoke-SDP. A limited number of such counters are available for use.

The **no** form of this command removes the associated counter.

3.10.2.1.5 VLL SDP commands

spoke-sdp

Syntax

spoke-sdp *sdp-id*[**:***vc-id*] [**no-endpoint**] [**create**]

spoke-sdp *sdp-id*[**:***vc-id*] **endpoint** *endpoint-name*

no spoke-sdp *sdp-id*[**:***vc-id*]

Context

config>service>epipe

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command binds a service to an existing Service Distribution Point (SDP).

The SDP has an operational state, which determines the operational state of the SDP within the service; for example, if the SDP is administratively or operationally down, the SDP for the service is down.

The SDP must already exist in the **config>service>sdp** context before it can be associated with an Epipe or VPL service. If the **sdp** *sdp-id* is not already configured, an error message is generated. If the *sdp-id* exists, a binding between the specific *sdp-id* and the service is created.

SDPs must be explicitly associated and bound to a service to allow far-end 7210 SAS-R6 and 7210 SAS-R12 devices to participate in the service.

The **no** form of this command removes the SDP binding from the service; the SDP configuration is not affected. When the SDP binding is removed, no packets are forwarded to the far-end router.

Special Cases

Epipe

At most, only one *sdp-id* can be bound to an Epipe service. Because an Epipe is a point-to-point service, it can have, at most, two end points. The two end points can be one SAP and one SDP or two SAPs. VC-switching VLLs are an exception. If the VLL is a "vc-switching" VLL, the two endpoints must both be SDPs.

Parameters

sdp-id

Specifies the SDP identifier. Allowed values are integers for existing SDPs.

Values 1 to 17407

vc-id

Specifies the virtual circuit identifier.

Values 1 to 4294967295

no endpoint

Keyword that removes the association of a spoke-SDP with an explicit endpoint name.

endpoint *endpoint-name*

Specifies the name of the service endpoint.

control-word

Syntax

[**no**] **control-word**

Context

config>service>epipe>spoke-sdp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command adds a control word as part of the packet encapsulation for pseudowire types for which the control word is optional. These are Ethernet pseudowires (Epipe).

The configuration for the two directions of the pseudowire must match because the control word negotiation procedures described in Section 6.2 of RFC 4447 are not supported. The C-bit in the pseudowire FEC sent in the label mapping message is set to 1 when the control word is enabled. Otherwise, it is set to 0.

The service only comes up if the same C-bit value is signaled in both directions. If a spoke-sdp is configured to use the control word but the node receives a label mapping message with a C-bit clear, the node releases the label with the an "Illegal C-bit" status code, in accordance with Section 6.1 of RFC 4447. When the user also enables the control on the remote peer, the remote peer withdraws its original label and sends a label mapping with the C-bit set to 1; the VLL service then becomes up in both nodes.

control-channel-status

Syntax

[**no**] **control-channel-status**

Context

config>service>epipe>spoke-sdp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures static pseudowire status signaling on a spoke-SDP for which signaling for its SDP is set to OFF.

A control-channel-status no shutdown is allowed only if all of the following is true:

- SDP signaling is off
- control word is enabled (control word by default is disabled)
- service type is Epipe or VPLS
- mate SDP signaling is off (in VC-switched services)
- **pw-path-id** is configured for this spoke

The **no** form of this command removes control channel status signaling form a spoke-sdp. It can only be removed if control channel status is shutdown.

Default

no control-channel-status

acknowledgment

Syntax

[**no**] **acknowledgment**

Context

config>service>epipe>spoke-sdp>control-channel-status

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the acknowledgment of control channel status messages. By default, no acknowledgment packets are sent.

refresh-timer

Syntax

refresh-timer *value*

no refresh-timer

Context

config>service>epipe>spoke-sdp>control-channel-status

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the refresh timer for control channel status signaling packets. By default, no refresh packets are sent.

Default

no refresh-timer

Parameters

value

Specifies the refresh timer value.

Values 10 to 65535 seconds

Default 0 (off)

request-timer

Syntax

request-timer request-timer *request-timer-secs* **retry-timer** *retry-timer-secs* **timeout-multiplier** *multiplier*

Context

config>service>epipe>spoke-sdp>control-channel-status

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the control channel status request mechanism. When it is configured, control channel status request procedures are used. These augment the procedures for control channel status messaging, in accordance with RFC 6478. This command and a non-zero refresh-timer value are mutually exclusive.

Parameters

request-timer-secs

Specifies the interval at which pseudowire status messages, including a reliable delivery TLV, with the "request" bit set, are sent.

Values 10 to 65535 seconds

retry-timer-secs

Specifies the timeout interval if no response to a pseudowire status request is received. This parameter must be configured. A value of zero (0) disables retries.

Values 0, 3 to 60 seconds

multiplier

Specifies that, if a requesting node does not receive a valid response to a pseudowire status request within this multiplier times the retry timer, it assumes the pseudowire is down. This parameter is optional.

Values 3 to 20 seconds

force-vlan-vc-forwarding

Syntax

[**no**] **force-vlan-vc-forwarding**

Context

config>service>epipe>spoke-sdp

config>service>vpls>spoke-sdp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command forces vc-vlan-type forwarding in the datapath for spokes that have either vc-type. This command is not allowed on vlan-vc-type SDPs.

The **no** version of this command reverts to the default value.

Default

disabled

hash-label

Syntax

hash-label [**signal-capability**]

no hash-label

Context

config>service>epipe>spoke-sdp

Platforms

7210 SAS-R6 IMMv2 and IMM-c cards and 7210 SAS-R12 IMMv2 and IMM-c cards

Description

This command configures the use of the hash label on a VLL or VPLS service bound to LDP or RSVP SDP using the autobind mode with the ldp, rsvp-te, or mpls options. When this feature is enabled, the ingress

datapath is modified such that the result of the hash on the packet header is communicated to the egress datapath for use as the value of the label field of the hash label. The egress datapath appends the hash label at the bottom of the stack (BoS) and sets the S-bit to one (1).

Note:
On 7210 SAS, the hash label is not used on the local node for purpose of ECMP hashing and LAG hashing. It is available for use by LSR nodes through which the traffic flows and that are capable of using the labels for hashing.

Packets generated in CPM and that are forwarded labeled within the context of a service (for example, OAM packets) must also include a hash label at the BoS and set the S-bit accordingly.

The TTL of the hash label is set to a value of 0.

The user enables the signaling of the hash-label capability under a VLL spoke-sdp, a VPLS spoke-sdp, or mesh-sdp interface by adding the signal-capability option. In this case, the decision whether to insert the hash label on the user and control plane packets by the local PE is solely determined by the outcome of the signaling process and can override the local PE configuration. The following rules apply when the hash-label option and the signal-capability option are enabled on the local PE.

- The 7210 SAS local PE inserts the Flow Label Interface Parameters sub-TLV with T=1 and R=1 in the PW ID FEC element in the label mapping message for that spoke-SDP or mesh SDP.
- If the remote PE does not send the Flow Label sub-TLV in the PW ID FEC element, or sends a Flow Label sub-TLV in the PW ID FEC element with T=FALSE and R=FALSE, the local node disables the hash label capability. Therefore, the local PE node does not insert a hash label in user and control plane packets; it forwards on the spoke-SDP or mesh SDP. It also drops user and control plane packets received from the remote PE if they include a hash label. Note that the latter may be caused by a remote 7210 SAS PE that does not support the hash-label option, or that has the hash-label option enabled but does not support the signal-capability option, or does support both options but the user did not enable them because of a misconfiguration.
- If remote PE sends Flow Label sub-TLV in the PW ID FEC element with T=TRUE and R=TRUE, the local PE enables the hash label capability. Therefore, local PE inserts a hash label in user and control plane packets it forwards on the spoke-SDP or mesh SDP. It also accepts user and control plane packets remote PE with or without a hash label.

If the hash-label option was enabled on the local configuration of the spoke-sdp or mesh-sdp at the remote PE, the pseudowire packets received by the local PE include the hash label. These packets must be dropped. The only way to solve this is to disable the signaling capability option on the local node, which results in the insertion of the hash label by both PE nodes.

If the hash-label option is not supported or was not enabled on the local configuration of the spoke-SDP or mesh SDP at the remote PE, the pseudowire received by the local PE does not have the hash label included.

The user can enable or disable the signal-capability option in CLI as needed. When doing so, the router must withdraw the label it sent to its peer and send a new label mapping message with the new value of the F bit in the flow label interface parameters sub-TLV of the PW ID FEC element.

Note:

- This feature is supported only for VLL and VPLS services. It not supported for VPRN services. It is also not supported on multicast packets forwarded using RSVP P2MP LPS or mLDP LSP in both the base router instance and in the multicast VPN (mVPN) instance.
- In 7x50 and possibly other vendor implementations, to allow applications where the egress LER infers the presence of the hash label implicitly from the value of the label, the Most

Significant Bit (MSB) of the result of the hash is set before copying into the Hash Label. Therefore, the value of the hash label is always in the range [524,288 to 1,048,575] and does not overlap with the signaled/static LSP and signaled/static service label ranges. This also guarantees the hash label does not match a value in the reserved label range. This is not supported on 7210 SAS for service traffic (for MPLS OAM traffic the MSB bit is set). That is, 7210 SAS devices do not set the MSB bit in the hash label value for service traffic. If enabled, the user must ensure that both the ends are correctly configured to process hash labels.

The **no** form of this command disables the use of the hash label.

Default

no hash-label

Parameters

signal-capability

Keyword to enable the signaling and negotiation of the use of the hash label between the local and remote PE nodes.

precedence

Syntax

precedence [*precedence-value* | **primary**]

no precedence

Context

config>service>epipe>spoke-sdp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command specifies the precedence of the SDP binding when there are multiple SDP bindings attached to one service endpoint. The value of zero can only be assigned to one SDP bind making it the primary SDP bind. When an SDP binding goes down, the next highest precedence SDP binding begins to forward traffic.

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

Default

4

Parameters

precedence-value

Specifies the spoke-SDP precedence.

Values 1 to 4

primary

Specifies to make this the primary spoke-SDP.

pw-path-id

Syntax

[**no**] **pw-path-id**

Context

config>service>epipe>spoke-sdp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures an MPLS-TP Pseudowire Path Identifier for a spoke-SDP. All elements of the PW path ID must be configured to enable a spoke-SDP with a PW path ID.

For an IES or VPRN spoke-SDP, the PW path ID is only valid for Ethernet spoke SDPs.

This command is configurable only if all the following conditions are true:

- system is using network chassis mode D
- SDP signaling is off
- control-word is enabled (control-word is disabled by default)
- the service type is Epipe or VPLS.
- mate SDP signaling is off for VC-switched services

The **no** form of this command deletes the PW path ID.

Default

no pw-path-id

agi

Syntax

agi *agi*

no agi

Context

config>service>epipe>spoke-sdp>pw-path-id

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the attachment group identifier for an MPLS-TP PW.

Parameters

agi

Specifies the attachment group identifier.

Values 0 to 4294967295

saii-type2

Syntax

saii-type2 *global-id:node-id:ac-id*

no saii-type2

Context

config>service>epipe>spoke-sdp>pw-path-id

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the source individual attachment identifier (SAII) for an MPLS-TP spoke-sdp. If this is configured on a spoke-sdp for which vc-switching is also configured, that is, if it is at an S-PE, the values must match those of the taii-type2 of the mate spoke-sdp.

Parameters

global-id

Specifies the global ID at the source PE or T-PE for the MPLS-TP PW for a spoke-SDP.

Values 0 to 4294967295

node-id

Specifies the node ID at the source PE or T-PE for the MPLS-TP PW for a spoke-SDP.

Values a.b.c.d or 0 to 4294967295

ac-id

Specifies the attachment circuit ID at the source PE or T-PE for the MPLS-TP PW for a spoke-SDP. If this node is the source of the PW, the AC ID must be set to a locally unique value.

Values 1 to 4294967295

taii-type2

Syntax

taii-type2 *global-id:node-id:ac-id*

no taii-type2

Context

config>service>epipe>spoke-sdp>pw-path-id

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the source individual attachment identifier (SAII) for an MPLS-TP spoke-sdp. If this is configured on a spoke-sdp for which vc-switching is also configured, that is, it is at an S-PE, the values must match those of the taii-type2 of the mate spoke-sdp.

Parameters

global-id

Specifies the global ID at the target PE or T-PE for the MPLS-TP PW for a spoke-SDP.

Values 0 to 4294967295

node-id

Specifies the node ID at the target PE or T-PE for the MPLS-TP PW for a spoke-SDP.

Values a.b.c.d or 0 to 4294967295

ac-id

Specifies the attachment circuit ID at the target PE or T-PE for the MPLS-TP PW for a spoke-SDP. If this node is the source of the PW, the AC ID must be set to a locally unique value.

Values 1 to 4294967295

pw-status-signaling

Syntax

[**no**] **pw-status-signaling**

Context

config>service>epipe>spoke-sdp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables pseudowire status signaling for this spoke-SDP binding.

The **no** form of this command disables the status signaling.

Default

pw-status-signaling

vc-label

Syntax

[**no**] **vc-label** *vc-label*

Context

config>service>epipe>spoke-sdp>egress

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the egress VC label.

Parameters

vc-label

Specifies a VC egress value that indicates a specific connection.

Values 16 to 1048575

vc-label

Syntax

[**no**] **vc-label** *vc-label*

Context

config>service>epipe>spoke-sdp>ingress

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the ingress VC label.

Parameters

vc-label

Specifies a VC ingress value that indicates a specific connection.

Values 2048 to 18431

vlan-vc-tag

Syntax

vlan-vc-tag *vlan-id*

no vlan-vc-tag [*vlan-id*]

Context

config>service>epipe>spoke-sdp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command specifies an explicit dot1q value used when encapsulating to the SDP far end. When signaling is enabled between the near and far end, the configured dot1q tag can be overridden by a received TLV specifying the dot1q value expected by the far end. This signaled value must be stored as the remote signaled dot1q value for the binding. The provisioned local dot1q tag must be stored as the administrative dot1q value for the binding.

When the dot1q tag is not defined, the default value of zero is stored as the administrative dot1q value. Setting the value to zero is equivalent to not specifying the value.

The **no** form of this command disables the command.

Default

no vlan-vc-tag

Parameters

vlan-id

Specifies a valid VLAN identifier to bind an 802.1Q VLAN tag ID.

Values 0 to 4094

spoke-sdp-fec

Syntax

spoke-sdp-fec

spoke-sdp-fec *spoke-sdp-fec-id* [**fec** *fec-type*] [**aii-type** *aii-type*] [**create**]

spoke-sdp-fec *spoke-sdp-fec-id* **no-endpoint**

spoke-sdp-fec *spoke-sdp-fec-id* [**fec** *fec-type*] [**aii-type** *aii-type*] [**create**] **endpoint** *name* [**icb**]

Context

config>service>epipe

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command binds a service to an existing Service Distribution Point (SDP), using a dynamic MS-PW.

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

The SDP has an operational state which determines the operational state of the SDP within the service. For example, if the SDP is administratively or operationally down, the SDP for the service is down.

When using dynamic MS-PWs, the particular SDP to bind-to is automatically selected based on the Target Attachment Individual Identifier (TAII) and the path to use, specified under spoke-SDP FEC. The selected SDP terminates on the first hop S-PE of the MS-PW. Therefore, an SDP must already be defined in the **config>service>sdp** context that reaches the first hop 7210 SAS of the MS-PW. The 7210 SAS associates an SDP with a service. If an SDP is not already configured, an error message is generated. If the sdp-id does exist, a binding between that sdp-id and the service is created.

This command differs from the spoke-sdp command in that the spoke-sdp command creates a spoke-SDP binding that uses a PW with the PW ID FEC. However, the spoke-sdp-fec command enables PWs with other FEC types to be used. In Release 9.0, only the Generalised ID FEC (FEC129) may be specified using this command.

The **no** form of this command removes the SDP binding from the service. The SDP configuration is not affected; only the binding of the SDP to a service. When removed, no packets are forwarded to the far-end router.

Parameters

spoke-sdp-fec-id

Specifies an unsigned integer value identifying the spoke-SDP.

Values 1 to 4294967295

fec *fec-type*

Specifies an unsigned integer value for the type of the FEC used by the MS-PW.

Values 129 to 130

aii-type ***aii-type***

Specifies an unsigned integer value for the Attachment Individual Identifier (AII) type used to identify the MS-PW endpoints.

Values 1 to 2

endpoint ***endpoint-name***

Specifies the name of the service endpoint.

no endpoint

Keyword to add or remove a spoke-SDP association.

icb

Keyword to configure the spoke-SDP as an inter-chassis backup SDP binding.

auto-config

Syntax

[**no**] **auto-config**

Context

config>service>epipe>spoke-sdp-fec

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables single-sided automatic endpoint configuration of the spoke-SDP. The 7210 SAS acts as the passive T-PE for signaling this MS-PW.

Automatic Endpoint Configuration allows the configuration of a spoke-SDP endpoint without specifying the TAII associated with that spoke-SDP. It allows a single-sided provisioning model where an incoming label mapping message with a TAII that matches the SAII of that spoke-SDP to be automatically bound to that endpoint. In this mode, the far end T-PE actively initiates MS-PW signaling and sends the initial label mapping message using T-LDP, while the 7210 SAS T-PE for which auto-config is specified acts as the passive T-PE.

The **auto-config** command is blocked in CLI if signaling active has been enabled for this spoke-SDP. It it is only applicable to spoke SDPs configured under the Epipe, IES and VPRN interface context.

The **no** form of this command means that the 7210 SAS T-PE either acts as the active T-PE (if signaling active is configured) or automatically determines which 7210 SAS initiates MS-PW signaling based on the prefix values configured in the SAII and TAII of the spoke-SDP. If the SAII has the greater prefix value, the 7210 SAS initiates MS-PW signaling without waiting for a label mapping message from the far end. However, if the TAII has the greater value prefix, the 7210 SAS assumes that the far end T-PE will initiate MS-PW signaling and will wait for that label mapping message before responding with a T-LDP label mapping message for the MS-PW in the reverse direction.

Default

no auto-config

path

Syntax

path *name*

no path

Context

config>service>epipe>spoke-sdp-fec

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command specifies the explicit path, containing a list of S-PE hops, that should be used for this spoke-SDP. The path-name should correspond to the name of an explicit path configured using the **config>service>pw-routing** context.

If **no** path is configured, each next-hop of the MS-PW used by the spoke-SDP will be chosen locally at each T-PE and S-PE.

Default

no path

Parameters

path-name

Specifies the name of the explicit path to be used, as configured in the **config>service>pw-routing** context.

precedence

Syntax

precedence *prec-value*

precedence primary

no precedence

Context

config>service>epipe>spoke-sdp-fec

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command specifies the precedence of the SDP binding when there are multiple SDP bindings attached to one service endpoint. The value of zero can be assigned to only one SDP bind making it the primary SDP bind. When an SDP binding goes down, the next highest precedence SDP binding begins to forward traffic.

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

Default

42

Parameters

precedence-value

Specifies the spoke-SDP precedence.

Values 1 to 4

primary

Keyword to make this the primary spoke-SDP.

pw-template-bind

Syntax

pw-template-bind *policy-id*

no pw-template-bind

Context

config>service>epipe>spoke-sdp-fec

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command binds the parameters included in a specific PW Template to a spoke-SDP.

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

Parameters

policy-id

Specifies the existing policy ID.

Values 1 to 2147483647

retry-count

Syntax

retry-count *retry-count*

no retry-count

Context

config>service>epipe>spoke-sdp-fec

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This optional command specifies the number of attempts software should make to reestablish the spoke-SDP after it has failed. After each successful attempt, the counter is reset to zero.

When the specified number is reached, no more attempts are made, and the spoke-sdp is put into the shutdown state.

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

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

Default

30

Parameters

retry-count

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

Values 10 to 10000

retry-timer

Syntax

retry-timer *retry-timer*

no retry-timer

Context

config>service>epipe>spoke-sdp-fec

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command specifies a retry-timer for the spoke-SDP. This is a configurable exponential back-off timer that determines the interval between retries to reestablish a spoke-SDP if it fails, a label withdraw message is received with the status code "AII unreachable".

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

Default

30

Parameters

retry-timer

Specifies the initial retry-timer value in seconds.

Values 10 to 480

saii-type2

Syntax

saii-type2 *global-id:prefix:ac-id*

no saii-type2

Context

config>service>epipe>spoke-sdp-fec

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the source attachment individual identifier for the spoke-sdp. This is only applicable to FEC129 AII type 2.

Parameters

global-id

Specifies a global ID for this 7210 SAS T-PE. This value must correspond to one of the global_id values configured for a local-prefix in the **config>service>pw-routing>local-prefix** context.

Values 1 to 4294967295

prefix

Specifies the prefix, expressed as an IPv4-formatted address, on this 7210 SAS T-PE that the spoke-sdp SDP is associated with.This value must correspond to one of the prefixes configured in the **config>service>pw-routing>local-prefix** context.

Values a.b.c.d or 1 to 4294967295

ac-id

Specifies an unsigned integer representing a locally unique identifier for the spoke-SDP.

Values 1 to 4294967295

signaling

Syntax

signaling *signaling*

Context

config>service>epipe>spoke-sdp-fec

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures this 7210 SAS as the active or passive T-PE for signaling this MS-PW, or to automatically select whether this T-PE is active or passive based on the prefix.

In an active role, this endpoint initiates MS-PW signaling without waiting for a T-LDP label mapping message to arrive from the far end T-PE. In a passive role, it waits for the initial label mapping message from the far end before sending a label mapping for this end of the PW. In auto mode, if the SAII has the greater prefix value, the 7210 SAS initiates MS-PW signaling without waiting for a label mapping message from the far end. However, if the TAII has the greater value prefix, the 7210 SAS assumes that the far end T-PE is initiating MS-PW signaling and waits for that label mapping message before responding with a T-LDP label mapping message for the MS-PW in the reverse direction.

The **no** form of this command means that the 7210 SAS T-PE automatically selects the 7210 SAS that will initiate MS-PW signaling based on the prefix values configured in the SAII and TAII of the spoke-SDP, as described previously.

Default

auto

Parameters

signaling

Specifies this 7210 SAS as the active T-PE for signaling this MS-PW.

Values auto, master

standby-signaling-slave

Syntax

[**no**] **standby-signaling-slave**

Context

config>service>epipe>spoke-sdp-fec

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

When this command is enabled, the node blocks the transmit forwarding direction of a spoke-SDP based on the setting of the standby bit received from a T-LDP peer.

This command is present at the endpoint level and spoke-SDP level. If the spoke-sdp is part of an explicit-endpoint, it is not possible to change this setting at the spoke-sdp level. An existing spoke-sdp can be made part of the explicit endpoint only if the settings do not conflict. A newly created spoke-sdp, which is part of a specific explicit-endpoint, inherits this setting from the endpoint configuration. An existing spoke-sdp cannot be moved to an endpoint if the setting of standby-signaling-slave is not the same as at the endpoint level. If the standby-signaling-slave setting is changed at the endpoint level, that change is automatically populated to the member spoke-sdps.This command cannot be configured for an endpoint that is part of an MC-LAG, ICB, and MC endpoint, or for which standby-signaling-master has been enabled.

If this command is disabled, the node assumes the existing Release 5.0 mode of behavior for forwarding on the spoke-SDP.

Default

no standby-signaling-slave

taii-type2

Syntax

taii-type2 *global-id:prefix:ac-id*

no taii-type2

Context

config>service>epipe>spoke-sdp-fec

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the target attachment individual identifier for the spoke-sdp. This is only applicable to FEC129 AII type 2.

This command is blocked in CLI if this end of the spoke-SDP is configured for single-sided auto configuration (using the **auto-config** command).

Parameters

global-id

Specifies the global ID of this 7210 T-PE. This value must correspond to one of the global_id values configured for a local-prefix in the **config>service>pw-routing>local-prefix** context.

Values 1 to 4294967295

prefix

Specifies the prefix, expressed as an IPv4-formatted address, on this 7210 T-PE that the spoke-sdp SDP is associated with.This value must correspond to one of the prefixes configured in the **config>service>pw-routing>local-prefix** context.

Values a.b.c.d or 1 to 4294967295

ac-id

Specifies an unsigned integer representing a locally unique identifier for the spoke-SDP.

Values 1 to 4294967295

3.10.2.2 Connection profile commands

connection-profile

Syntax

connection-profile *conn-prof-id* [**create**]

no connection-profile *conn-prof-id*

Context

config

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command creates a list of VLAN values to be assigned to a dot1q SAP in an Epipe service.

A connection profile can only be assigned to a dot1q SAP that is part of an Epipe Service.

The **no** form of this command deletes the profile from the configuration.

Parameters

noneconn-prof-id

Specifies the profile number.

Values 1 to 8000

ethernet

Syntax

ethernet

Context

config>connprof

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

Commands in this context configure the VLAN ranges values.

ranges

Syntax

no ranges

ranges vlan-ranges [*vlan-ranges...*(upto 32 max)]

Context

config>connprof>ethernet

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command specifies the list of VLAN ranges or individual VLAN ID to be used for mapping the specific VLANs to the Epipe SAP.

The system validates that the values specified are valid VLAN IDs in the range 0 to 4094 (VLAN ID 4095 is reserved). Ranges are specified in the format "a-b," the expression (a < b) should be true. Up to about 32 individual VLAN values or VLAN ranges can be specified. A maximum of 8 VLAN ranges are allowed per connection profile.

Parameters

vlan-ranges

Specifies the list of VLAN ranges or individual VLAN ID to be used for mapping the specific VLANs to the Epipe SAP.

A list of space separated values specified as either a-b or individual VLAN IDs. Both the VLAN IDs and the value used for "a" and "b" must be in the range of 0 to 4094. Additionally, value "a" must be less than value "b."

For example:

ranges 100 to 200 5 6 4000 to 4020

ranges 4 5 6 10 11 12

ranges 250 to 350 500 to 600 1000 to 1023

3.10.2.3 Show commands

sap-using

Syntax

sap-using [**sap** *sap-id*]

sap-using interface [*ip-address* | *ip-int-name*]

sap-using [**ingress**] **filter** *filter-id*

sap-using [**ingress**] **qos-policy** *qos-policy-id*

sap-using encap-type *encap-type*

Context

show>service

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays SAP information.

If no optional parameters are specified, the command displays a summary of all defined SAPs.

The optional parameters restrict output to only SAPs matching the specified properties.

Parameters

ip-addr

Specifies the IP address of the interface for which to display matching SAPs.

Values a.b.c.d

ip-int-name

Specifies the IP interface name for which to display matching SAPs.

ingress

Specifies matching an ingress policy.

egress

Specifies matching an egress policy.

qos-policy *qos-policy-id*

Specifies the ingress QoS Policy ID for which to display matching SAPs.

Values 1 to 65535

filter *filter-id*

Specifies the ingress or egress filter policy ID for which to display matching SAPs.

Values 1 to 65535

sap *sap-id*

Specifies the physical port identifier portion of the SAP definition. See Common CLI command descriptions for command syntax.

encap-type *encap-type*

Displays the CEM encapsulation type.

Values cem

Output

The following output is an example of SAP information, and Table 26: Output fields: service SAP-using describes the output fields.

Sample output

```
*A:DUT-B_sasx>show>service# sap-using

===============================================================================
Service Access Points
===============================================================================
PortId                          SvcId      Ing.  Ing.    Egr.  Egr.   Adm  Opr
                                           QoS   Fltr    QoS   Fltr
-------------------------------------------------------------------------------
1/1/3:1                         1          10    none    1     none   Up   Up
1/1/3:2                         2          1     none    1     none   Up   Up
1/1/3:3                         3          1     none    1     none   Up   Up
1/1/3:4                         4          1     none    1     none   Up   Up
1/1/3:5                         5          1     none    1     none   Up   Up
1/1/3:6                         6          1     none    1     none   Up   Up
1/1/3:7                         7          1     none    1     none   Up   Up
1/1/3:8                         8          1     none    1     none   Up   Up
1/1/3:9                         9          1     none    1     none   Up   Up
1/1/3:10                        10         1     none    1     none   Up   Up
1/1/3:11                        11         1     none    1     none   Up   Up
1/1/3:12                        12         1     none    1     none   Up   Up
1/1/3:13                        13         1     none    1     none   Up   Up
1/1/3:14                        14         1     none    1     none   Up   Up
1/1/3:15                        15         1     none    1     none   Up   Up
1/1/3:16                        16         1     none    1     none   Up   Up
1/1/3:17                        17         1     none    1     none   Up   Up
1/1/3:18                        18         1     none    1     none   Up   Up
1/1/3:19                        19         1     none    1     none   Up   Up
1/1/3:20                        20         1     none    1     none   Up   Up
1/1/3:21                        21         1     none    1     none   Up   Up
1/1/3:22                        22         1     none    1     none   Up   Up
1/1/3:23                        23         1     none    1     none   Up   Up
1/1/3:24                        24         1     none    1     none   Up   Up
1/1/3:25                        25         1     none    1     none   Up   Up
```

```
1/1/3:26                        26          1     none    1     none    Up   Up
1/1/3:27                        27          1     none    1     none    Up   Up
1/1/3:28                        28          1     none    1     none    Up   Up
1/1/3:29                        29          1     none    1     none    Up   Up
1/1/3:30                        30          1     none    1     none    Up   Up
1/1/3:31                        31          1     none    1     none    Up   Up
1/1/3:32                        32          1     none    1     none    Up   Up
1/1/3:33                        33          1     none    1     none    Up   Up
1/1/3:34                        34          1     none    1     none    Up   Up
1/1/3:35                        35          1     none    1     none    Up   Up
1/1/3:36                        36          1     none    1     none    Up   Up
1/1/3:37                        37          1     none    1     none    Up   Up
1/1/3:38                        38          1     none    1     none    Up   Up
1/1/3:39                        39          1     none    1     none    Up   Up
1/1/3:40                        40          1     none    1     none    Up   Up
1/1/3:41                        41          1     none    1     none    Up   Up
1/1/3:42                        42          1     none    1     none    Up   Up
1/1/3:43                        43          1     none    1     none    Up   Up
1/1/3:44                        44          1     none    1     none    Up   Up
1/1/3:45                        45          1     none    1     none    Up   Up
1/1/3:46                        46          1     none    1     none    Up   Up
1/1/3:47                        47          1     none    1     none    Up   Up
1/1/3:48                        48          1     none    1     none    Up   Up
1/1/3:49                        49          1     none    1     none    Up   Up
1/1/3:50                        50          1     none    1     none    Up   Up
1/1/3:51                        51          1     none    1     none    Up   Up
1/1/3:52                        52          1     none    1     none    Up   Up
1/1/3:53                        53          1     none    1     none    Up   Up
1/1/3:54                        54          1     none    1     none    Up   Up
1/1/3:55                        55          1     none    1     none    Up   Up
1/1/3:56                        56          1     none    1     none    Up   Up
1/1/3:57                        57          1     none    1     none    Up   Up
1/1/3:58                        58          1     none    1     none    Up   Up
1/1/3:59                        59          1     none    1     none    Up   Up
1/1/3:60                        60          1     none    1     none    Up   Up
1/1/3:61                        61          1     none    1     none    Up   Up
1/1/3:62                        62          1     none    1     none    Up   Up
1/1/3:63                        63          1     none    1     none    Up   Up
1/1/3:64                        257         1     none    1     none    Up   Up
-------------------------------------------------------------------------------
Number of SAPs : 64
-------------------------------------------------------------------------------
===============================================================================


*A:DUT-B_sasx>show>service# sap-using sap 1/1/3:1

===============================================================================
Service Access Points Using Port 1/1/3:1
===============================================================================
PortId                          SvcId       Ing.  Ing.    Egr.  Egr.   Adm  Opr
                                            QoS   Fltr    QoS   Fltr
-------------------------------------------------------------------------------
1/1/3:1                         1           10    none    1     none    Up   Up
-------------------------------------------------------------------------------
Number of SAPs : 1
-------------------------------------------------------------------------------
===============================================================================
```

Table 26: Output fields: service SAP-using

Label	Description
Port ID	The ID of the access port where the SAP is defined.
Svc ID	The service identifier.
MTU	The port MTU value.
Ing. QoS	The SAP ingress QoS policy number specified on the ingress SAP.
Ing Fltr	The MAC or IP filter policy ID applied to the ingress SAP.
Egr. QoS	The SAP egress QoS policy number specified on the egress SAP.
Egr. Fltr	The MAC or IP filter policy ID applied to the egress SAP.
Adm	The administrative state of the SAP.
Opr	The operational state of the SAP.

sdp

Syntax

sdp [*sdp-id* | **far-end** *ip-address*] [**detail** | **keep-alive-history**]

Context

show>service

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays SDP information.

If no optional parameters are specified, a summary SDP output for all SDPs is displayed.

Parameters

sdp-id

Specifies the SDP ID for which to display information.

Default All SDPs.

Values 1 to 17407

far-end *ip-address*

Displays only SDPs matching with the specified far-end IP address.

Default SDPs with any far-end IP address.

detail

Displays detailed SDP information.

Default SDP summary output.

keep-alive-history

Displays the last fifty SDP keepalive events for the SDP.

Default SDP summary output.

Output

The following output is an example of SDP information, and Table 27: Output fields: service SDP describes the output fields.

Sample output

```
*A:ALA-12# show service sdp
===============================================================================
Services: Service Destination Points
===============================================================================
SdpId    Adm MTU   Opr MTU   IP address       Adm  Opr         Deliver Signal
-------------------------------------------------------------------------------
10       4462      4462      10.20.1.3        Up   Dn NotReady MPLS    TLDP
40       4462      1534      10.20.1.20       Up   Up          MPLS    TLDP
60       4462      1514      10.20.1.21       Up   Up          MPLS TLDP
100      4462      4462      10.0.0.2         Down Down        MPLS TLDP
500      4462      4462      10.20.1.50       Up   Dn NotReady MPLS TLDP
-------------------------------------------------------------------------------
Number of SDPs : 5
===============================================================================
*A:ALA-12#


*A:ALA-12# show service sdp 2 detail
===============================================================================
Service Destination Point (Sdp Id : 2) Details
===============================================================================
Sdp Id 2  -(10.10.10.104)
-------------------------------------------------------------------------------
Description           : MPLS-10.10.10.104
SDP Id                : 2
Admin Path MTU        : 0                    Oper Path MTU      : 0
Far End               : 10.10.10.104         Delivery           : MPLS
Admin State           : Up                   Oper State         : Down
Flags                 : SignalingSessDown TransportTunnDown
Signaling             : TLDP                 VLAN VC Etype      : 0x8100
Last Status Change    : 02/01/2007 09:11:39  Adv. MTU Over.     : No
Last Mgmt Change      : 02/01/2007 09:11:46

KeepAlive Information :
Admin State           : Disabled             Oper State         : Disabled
Hello Time            : 10                   Hello Msg Len      : 0
Hello Timeout         : 5                    Unmatched Replies  : 0
Max Drop Count        : 3                    Hold Down Time     : 10
Tx Hello Msgs         : 0                    Rx Hello Msgs      : 0

Associated LSP LIST :
SDP Delivery Mechanism is not MPLS
```

```
===============================================================================
*A:ALA-12#
*A:ALA-12# show service sdp 8
===============================================================================
Service Destination Point (Sdp Id : 8)
===============================================================================
SdpId    Adm MTU   Opr MTU   IP address       Adm  Opr         Deliver Signal
-------------------------------------------------------------------------------
8        4462      4462      10.10.10.104     Up   Dn NotReady MPLS    TLDP
===============================================================================
*A:ALA-12#


*A:ALA-12# show service sdp 8 detail
===============================================================================
Service Destination Point (Sdp Id : 8) Details
===============================================================================
Sdp Id 8  -(10.10.10.104)
-------------------------------------------------------------------------------
Description           : MPLS-10.10.10.104
SDP Id                : 8
Admin Path MTU        : 0                     Oper Path MTU      : 0
Far End               : 10.10.10.104          Delivery           : MPLS
Admin State           : Up                    Oper State         : Down
Flags                 : SignalingSessDown TransportTunnDown
Signaling             : TLDP                  VLAN VC Etype      : 0x8100
Last Status Change    : 02/01/2007 09:11:39   Adv. MTU Over.     : No
Last Mgmt Change      : 02/01/2007 09:11:46

KeepAlive Information :
Admin State           : Disabled              Oper State         : Disabled
Hello Time            : 10                    Hello Msg Len      : 0
Hello Timeout         : 5                     Unmatched Replies  : 0
Max Drop Count        : 3                     Hold Down Time     : 10
Tx Hello Msgs         : 0                     Rx Hello Msgs      : 0

Associated LSP LIST :
Lsp Name              : to-104
Admin State           : Up                    Oper State         : Down
Time Since Last Tran*: 01d07h36m
===============================================================================
* indicates that the corresponding row element may have been truncated.
*A:ALA-12#
```

Table 27: Output fields: service SDP

Label	Description
SDP Id	The SDP identifier.
Adm MTU	Specifies the configured largest service frame size (in octets) that can be transmitted through this SDP to the far-end router, without requiring the packet to be fragmented.
Opr MTU	Specifies the actual largest service frame size (in octets) that can be transmitted through this SDP to the far-end router, without requiring the packet to be fragmented.
IP address	Specifies the IP address of the remote end of the MPLS tunnel defined by this SDP.

Label	Description
Adm Admin State	Specifies the configured state of the SDP.
Opr Oper State	Specifies the operating state of the SDP.
Deliver Delivery	Specifies the type of delivery used by the SDP: MPLS.
Flags	Specifies all the conditions that affect the operating status of this SDP.
Signal Signaling	Specifies the signaling protocol used to obtain the ingress and egress labels used in frames transmitted and received on the SDP.
Last Status Change	Specifies the time of the most recent operating status change to this SDP.
Last Mgmt Change	Specifies the time of the most recent management-initiated change to this SDP.
Number of SDPs	Specifies the total number of SDPs displayed according to the criteria specified.
Hello Time	Specifies how often the SDP echo request messages are transmitted on this SDP.
Number of SDPs	Specifies the total number of SDPs displayed according to the criteria specified.
Hello Time	Specifies how often the SDP echo request messages are transmitted on this SDP.
Hello Msg Len	Specifies the length of the SDP echo request messages transmitted on this SDP.
Hello Timeout	Specifies the number of seconds to wait for an SDP echo response message before declaring a timeout.
Unmatched Replies	Specifies the number of SDP unmatched message replies.
Max Drop Count	Specifies the maximum number of consecutive SDP echo request messages that can be unacknowledged before the keepalive protocol reports a fault.
Hold Down Time	Specifies the amount of time to wait before the keepalive operating status is eligible to enter the alive state.

Label	Description
TX Hello Msgs	Specifies the number of SDP echo request messages transmitted after the keepalive was administratively enabled or the counter was cleared.
Rx Hello Msgs	Specifies the number of SDP echo request messages received after the keepalive was administratively enabled or the counter was cleared.
Associated LSP List	When the SDP type is MPLS, a list of LSPs used to reach the far-end router displays. All the LSPs in the list must terminate at the IP address specified in the far end field.

sdp-using

Syntax

sdp-using [*sdp-id*[**:***vc-id*] | **far-end** *ip-address*]

Context

show>service

Platforms

Supported on all 7210 SAS platforms as described in this document

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 to 17407

vc-id

Specifies the virtual circuit identifier.

Values 1 to 4294967295

far-end *ip-address*

Displays only services matching the specified far-end IP address.

Default Services with any far-end IP address.

Output

The following output is an example of SDP information, and Table 28: Output fields: service SDP-using describes the output fields.

Sample output

```
*A:ALA-1# show service sdp-using 300
===============================================================================
Service Destination Point (Sdp Id : 300)
===============================================================================
SvcId       SdpId               Type Far End        Opr State I.Label  E.Label
-------------------------------------------------------------------------------
1           300:1               Mesh 10.0.0.13      Up        131071   131071
2           300:2               Spok 10.0.0.13      Up        131070   131070
100         300:100             Mesh 10.0.0.13      Up        131069   131069
101         300:101             Mesh 10.0.0.13      Up        131068   131068
102         300:102             Mesh 10.0.0.13      Up        131067   131067
-------------------------------------------------------------------------------
Number of SDPs : 5
-------------------------------------------------------------------------------
*A:ALA-1#
*A:ces-A# show service sdp-using
===============================================================================
SDP Using
===============================================================================
SvcId       SdpId               Type    Far End        Opr S* I.Label  E.Label
-------------------------------------------------------------------------------
1           12:1                Spok    2.2.2.2        Up     131063   131062
2           12:2                Spok    2.2.2.2        Up     131062   131069
3           122:3               Spok    2.2.2.2        Up     131069   131068
4           12:4                Spok    2.2.2.2        Up     131061   131061
-------------------------------------------------------------------------------
Number of SDPs : 4
-------------------------------------------------------------------------------
===============================================================================
*A:ces-A#
```

Table 28: Output fields: service SDP-using

Label	Description
Svc ID	The service identifier.
Sdp ID	The SDP identifier.
Type	Type of SDP: spoke or mesh.
Far End	The far end address of the SDP.
Oper State	The operational state of the service.
Ingress Label	The label used by the far-end device to send packets to this device in this service by this SDP.
Egress Label	The label used by this device to send packets to the far-end device in this service by this SDP.

service-using

Syntax

service-using [**sdp sdp-id**] [**b-vpls**] [**i-vpls**] [**m-vpls**] [**sdp sdp-id**] [**customer** *customer-id*]

Context

show>service

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays the services matching the specified usage properties.

If no optional parameters are specified, all services defined on the system are displayed.

Parameters

b-vpls

Specifies the B-component instance of the Provider Backbone Bridging (PBB/IEEE 802.1ah) feature. It represents the multi-point tunneling component that multiplexes multiple customer VPNs (ISIDs) together. It is similar to a regular VPLS instance that operates on the backbone MAC addresses.

i-vpls

Specifies the I-component instance of the Provider Backbone Bridging (PBB/IEEE 802.1ah) feature. It identifies the specific VPN entity associated with a customer multipoint (ELAN) service. It is similar to a regular VPLS instance that operates on the customer MAC addresses.

m-vpls

Specifies the M-component (managed VPLS) instance of the Provider Backbone Bridging (PBB/IEEE 802.1ah) feature.

sdp *sdp-id*

Displays only services bound to the specified SDP ID.

Default Services bound to any SDP ID.

Values 1 to 17407

customer *customer-id*

Displays services only associated with the specified customer ID.

Default Services associated with any customer.

Values 1 to 2147483647

Output

The following output is an example of service information, and Table 29: Output fields: service service-using describes the output fields.

Sample output

```
*A:ALA-12# show service service-using customer 10
===============================================================================
Services
===============================================================================
ServiceId    Type      Adm    Opr        CustomerId        Last Mgmt Change
-------------------------------------------------------------------------------
1            VPLS      Up     Up         10                09/05/2006 13:24:15
300          Epipe     Up     Up         10                09/05/2006 13:24:15
-------------------------------------------------------------------------------
Matching Services :
===============================================================================
*A:ALA-12#


*A:ALA-12# show service service-using
===============================================================================
Services
===============================================================================
ServiceId    Type      Adm    Opr        CustomerId        Last Mgmt Change
-------------------------------------------------------------------------------
1            uVPLS     Up     Up         1                 10/26/2006 15:44:57
2            Epipe     Up     Down       1                 10/26/2006 15:44:57
10           mVPLS     Down   Down       1                 10/26/2006 15:44:57
11           mVPLS     Down   Down       1                 10/26/2006 15:44:57
100          mVPLS     Up     Up         1                 10/26/2006 15:44:57
101          mVPLS     Up     Up         1                 10/26/2006 15:44:57
102          mVPLS     Up     Up         1                 10/26/2006 15:44:57
999          uVPLS     Down   Down       1                 10/26/2006 16:14:33
-------------------------------------------------------------------------------
Matching Services : 8
-------------------------------------------------------------------------------
*A:ALA-12#
```

Table 29: Output fields: service service-using

Label	Description
Service Id	The service identifier.
Type	Specifies the service type configured for the service ID.
Adm	The configured state of the service.
Opr	The operating state of the service.
CustomerID	The ID of the customer who owns this service.
Last Mgmt Change	The date and time of the most recent management-initiated change to this service.

id

Syntax

id *service-id* {**all** | **arp** | **base** | **endpoint fdb** | **label** |**sap** | **split-horizon-group** |**stp** | **interface** | **mstp-configuration**}

Context

show>service

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays information for a particular service ID.

Parameters

service-id

Specifies the service identification number that identifies the service in the domain.

Values *service-id*: 1 to 214748364

svc-name: A string up to 64 characters.

all

Displays all information about the service.

arp

Displays ARP entries for the service.

base

Displays basic service information.

endpoint

Displays service endpoint information.

fdb

Displays FDB information.

interface

Displays service interfaces.

labels

Displays labels being used by this service.

mstp-configuration

Display MSTP information.

sap

Displays SAPs associated with the service.

sdp

Displays SDPs associated with the service.

split-horizon-group

Displays split horizon group information.

stp

Displays STP information.

Output

The following output is an example of service ID information.

Sample output

```
*A:ces-A# show service id 1 sap
===============================================================================
SAP(Summary), Service 1
===============================================================================
PortId                          SvcId      Ing.  Ing.    Egr.   Adm  Opr
                                           QoS   Fltr    Fltr
-------------------------------------------------------------------------------
1/2/1.1                         1          1     none    none   Up   Up
-------------------------------------------------------------------------------
Number of SAPs : 1
-------------------------------------------------------------------------------
===============================================================================
```

all

Syntax

all

Context

show>service>id

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays more information for all aspects of the service.

Output

The following outputs are examples of detailed service information, and Table 30: Output fields: service ID All describes the output fields:

- Sample output
- Sample output (split horizon group)
- Sample output (meter-override)
- Sample output (entropy/hash-label)

Sample output

```
*A:Dut-A>show>service>id# all

===============================================================================
Service Detailed Information
===============================================================================
Service Id        : 1501               Vpn Id            : 1501
Service Type      : Epipe
Description       : Default epipe description for service id 1501
Customer Id       : 1
Last Status Change: 02/21/2011 13:07:03
Last Mgmt Change  : 02/21/2011 13:03:58
Admin State       : Up                 Oper State        : Up
MTU               : 1514
MTU Check         : Enabled
Vc Switching      : False
SAP Count         : 1                  SDP Bind Count    : 2
-------------------------------------------------------------------------------
Service Destination Points(SDPs)
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
 Sdp Id 1413:1501  -(10.20.1.4)
-------------------------------------------------------------------------------
Description     : Default sdp description
SDP Id            : 1413:1501               Type              : Spoke
VC Type           : Ether                   VC Tag            : n/a
Admin Path MTU    : 0                       Oper Path MTU     : 9182
Far End           : 10.20.1.4               Delivery          : MPLS

Admin State       : Up                      Oper State        : Up
Acct. Pol         : 14                      Collect Stats     : Enabled
Ingress Label     : 130948                  Egress Label      : 130483
Ing mac Fltr      : n/a                     Egr mac Fltr      : n/a
Ing ip Fltr       : n/a                     Egr ip Fltr       : n/a
Admin ControlWord : Preferred               Oper ControlWord  : True
Admin BW(Kbps)    : 0                       Oper BW(Kbps)     : 0
Last Status Change : 02/21/2011 13:07:12    Signaling         : TLDP
Last Mgmt Change  : 02/21/2011 13:03:58     Force Vlan-Vc     : Disabled
Endpoint          : coreSide                Precedence        : 1
Class Fwding State : Down
Flags             : None
Peer Pw Bits      : None
Peer Fault Ip     : None
Peer Vccv CV Bits : lspPing
Peer Vccv CC Bits : pwe3ControlWord mplsRouterAlertLabel

KeepAlive Information :
Admin State       : Enabled                 Oper State        : Alive
Hello Time        : 10                      Hello Msg Len     : 0
Max Drop Count    : 3                       Hold Down Time    : 10

Statistics          :
I. Fwd. Pkts.     : 48319                   I. Fwd. Octs.     : 5690869
E. Fwd. Pkts.     : 34747                   E. Fwd. Octets    : 4013709
-------------------------------------------------------------------------------
Eth-Cfm Configuration Information
-------------------------------------------------------------------------------
Md-index          : 1000                    Direction         : Down
Ma-index          : 1150114                 Admin             : Enabled
MepId             : 1                       CCM-Enable        : Enabled
LowestDefectPri   : macRemErrXcon           HighestDefect     : none
Defect Flags      : None
Mac Address       : 7c:20:64:ad:04:07       ControlMep        : False
```

```
CcmLtmPriority     : 7
CcmTx              : 11385                    CcmSequenceErr    : 0
Eth-1Dm Threshold  : 3(sec)
Eth-Ais:           : Disabled
Eth-Tst:           : Disabled
LbRxReply          : 0                        LbRxBadOrder      : 0
LbRxBadMsdu        : 0                        LbTxReply         : 0
LbNextSequence     : 1                        LtNextSequence    : 1
LtRxUnexplained    : 0

Associated LSP LIST :
Lsp Name           : A_D_21
Admin State        : Up                       Oper State        : Up
Time Since Last Tr*: 03h49m30s

-------------------------------------------------------------------------------
 Sdp Id 1613:1501  -(10.20.1.6)
-------------------------------------------------------------------------------
Description     : Default sdp description
SDP Id             : 1613:1501                Type              : Spoke
VC Type            : Ether                    VC Tag            : n/a
Admin Path MTU     : 0                        Oper Path MTU     : 9182
Far End            : 10.20.1.6                Delivery          : MPLS

Admin State        : Up                       Oper State        : Up
Acct. Pol          : 14                       Collect Stats     : Enabled
Ingress Label      : 130526                   Egress Label      : 130424
Ing mac Fltr       : n/a                      Egr mac Fltr      : n/a
Ing ip Fltr        : n/a                      Egr ip Fltr       : n/a
Admin ControlWord  : Not Preferred            Oper ControlWord  : False
Admin BW(Kbps)     : 0                        Oper BW(Kbps)     : 0
Last Status Change : 02/21/2011 13:07:03      Signaling         : TLDP
Last Mgmt Change   : 02/21/2011 13:03:58      Force Vlan-Vc     : Disabled
Endpoint           : coreSide                 Precedence        : 2
Class Fwding State : Down
Flags              : None
Peer Pw Bits       : pwFwdingStandby
Peer Fault Ip      : None
Peer Vccv CV Bits  : lspPing
Peer Vccv CC Bits  : mplsRouterAlertLabel

KeepAlive Information :
Admin State        : Enabled                  Oper State        : Alive
Hello Time         : 10                       Hello Msg Len     : 0
Max Drop Count     : 3                        Hold Down Time    : 10

Statistics           :
I. Fwd. Pkts.      : 25                       I. Fwd. Octs.     : 2776
E. Fwd. Pkts.      : 23                       E. Fwd. Octets    : 2557
-------------------------------------------------------------------------------
Eth-Cfm Configuration Information
-------------------------------------------------------------------------------
Md-index           : 1000                     Direction         : Down
Ma-index           : 1150116                  Admin             : Enabled
MepId              : 1                        CCM-Enable        : Enabled
LowestDefectPri    : macRemErrXcon            HighestDefect     : none
Defect Flags       : None
Mac Address        : 7c:20:64:ad:04:07        ControlMep        : False
CcmLtmPriority     : 7
CcmTx              : 11414                    CcmSequenceErr    : 0
Eth-1Dm Threshold  : 3(sec)
Eth-Ais:           : Disabled
Eth-Tst:           : Disabled
LbRxReply          : 0                        LbRxBadOrder      : 0
```

```
LbRxBadMsdu        : 0                        LbTxReply         : 0
LbNextSequence     : 1                        LtNextSequence    : 1
LtRxUnexplained    : 0

Associated LSP LIST :
Lsp Name           : A_F_21
Admin State        : Up                       Oper State        : Up
Time Since Last Tr*: 03h48m45s

-------------------------------------------------------------------------------
Number of SDPs : 2
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
Service Access Points
-------------------------------------------------------------------------------

-------------------------------------------------------------------------------
SAP lag-3:1501.1501
-------------------------------------------------------------------------------
Service Id         : 1501
SAP                : lag-3:1501.1501          Encap             : qinq
QinQ Dot1p         : Default
Description        : (Not Specified)
Admin State        : Up                       Oper State        : Up
Flags              : None
Last Status Change : 02/21/2011 13:06:45
Last Mgmt Change   : 02/21/2011 13:03:58

Admin MTU          : 9212                     Oper MTU          : 9212
Ingr IP Fltr-Id    : n/a                      Egr IP Fltr-Id    : n/a
Ingr Mac Fltr-Id   : 1501                     Egr Mac Fltr-Id   : n/a
tod-suite          : None
Egr Agg Rate Limit : max
Endpoint           : accessSide

Acct. Pol          : Default                  Collect Stats     : Enabled


-------------------------------------------------------------------------------
QOS
-------------------------------------------------------------------------------
Ingress qos-policy : 1500                     Egress qos-policy : 1500
-------------------------------------------------------------------------------
Sap Egress Policy (1500)
-------------------------------------------------------------------------------
Scope              : Template
Remark             : False                    Remark Pol Id     : 2
Accounting         : frame-based
Description    : Sap Egress Policy for svcList 1500
-------------------------------------------------------------------------------
Queue Rates and Rules
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
QueueId        CIR          CIR Adpt Rule        PIR          PIR Adpt Rule
-------------------------------------------------------------------------------
Queue1          10000          max                10000          max
Queue2          10000          max                10000          max
Queue3          10000          max                10000          max
Queue4          10000          max                10000          max
Queue5          10000          max                10000          max
Queue6          10000          max                10000          max
Queue7          10000          max                10000          max
Queue8          10000          max                10000          max
-------------------------------------------------------------------------------
```

```
Parent Details
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
QueueId          Port       CIR Level      PIR Weight
-------------------------------------------------------------------------------
Queue1          True            1            1
Queue2          True            2            2
Queue3          True            3            3
Queue4          True            4            4
Queue5          True            5            5
Queue6          True            6            6
Queue7          True            7            7
Queue8          True            8            8
-------------------------------------------------------------------------------
High Slope
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
QueueId        State      Start-Avg(%)   Max-Avg(%)   Max-Prob(%)
-------------------------------------------------------------------------------
Queue1           Up             50           100            50
Queue2           Up             50           100            50
Queue3           Up             50           100            50
Queue4           Up             50           100            50
Queue5           Up             50           100            50
Queue6           Up             50           100            50
Queue7           Up             50           100            50
Queue8           Up             50           100            50
-------------------------------------------------------------------------------
Low Slope
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
QueueId        State      Start-Avg(%)   Max-Avg(%)   Max-Prob(%)
-------------------------------------------------------------------------------
Queue1           Up             10           50            50
Queue2           Up             10           50            50
Queue3           Up             10           50            50
Queue4           Up             10           50            50
Queue5           Up             10           50            50
Queue6           Up             10           50            50
Queue7           Up             10           50            50
Queue8           Up             10           50            50
-------------------------------------------------------------------------------
Burst Sizes and Time Average Factor
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
QueueId         CBS            MBS       Time Average Factor        Queue-Mgmt
-------------------------------------------------------------------------------
Queue1          200              400             10           qM_1500
Queue2          200              400             10           qM_1500
Queue3          200              400             10           qM_1500
Queue4          200              400             10           qM_1500
Queue5          200              400             10           qM_1500
Queue6          200              400             10           qM_1500
Queue7          200              400             10           qM_1500
Queue8          200              400             10           qM_1500
-------------------------------------------------------------------------------
Aggregate Policer (Available)
-------------------------------------------------------------------------------
rate               : n/a                      burst            : n/a
-------------------------------------------------------------------------------
Ingress QoS Classifier Usage
-------------------------------------------------------------------------------
Classifiers Allocated: 32                  Meters Allocated   : 16
Classifiers Used     : 8                   Meters Used        : 5
```

```
-------------------------------------------------------------------------------
Sap Statistics
-------------------------------------------------------------------------------
                        Packets                 Octets
Ingress Stats:          34659                   3241035
Egress Stats:           48099                   5291928
Extra-Tag Drop Stats:   n/a                     n/a
-------------------------------------------------------------------------------
Sap per Meter stats
-------------------------------------------------------------------------------
                        Packets                 Octets

Ingress Meter 1 (Unicast)
For. InProf           : 7209                    468585
For. OutProf          : 0                       0

Ingress Meter 2 (Unicast)
For. InProf           : 0                       0
For. OutProf          : 0                       0

Ingress Meter 3 (Unicast)
For. InProf           : 0                       0
For. OutProf          : 0                       0

Ingress Meter 4 (Unicast)
For. InProf           : 0                       0
For. OutProf          : 0                       0

Ingress Meter 5 (Unicast)
For. InProf           : 27454                   2772854
For. OutProf          : 0                       0
-------------------------------------------------------------------------------
Sap per Queue stats
-------------------------------------------------------------------------------
                        Packets                 Octets

Egress Queue 1 (be)
Fwd Stats            :  0                       0
Drop InProf          :  0                       0
Drop OutProf         :  0                       0

Egress Queue 2 (l2)
Fwd Stats            :  3                       180
Drop InProf          :  0                       0
Drop OutProf         :  0                       0

Egress Queue 3 (af)
Fwd Stats            :  0                       0
Drop InProf          :  0                       0
Drop OutProf         :  0                       0

Egress Queue 4 (l1)
Fwd Stats            :  0                       0
Drop InProf          :  0                       0
Drop OutProf         :  0                       0

Egress Queue 5 (h2)
Fwd Stats            :  0                       0
Drop InProf          :  0                       0
Drop OutProf         :  0                       0

Egress Queue 6 (ef)
Fwd Stats            :  0                       0
Drop InProf          :  0                       0
```

```
Drop OutProf         :  0                      0

Egress Queue 7 (h1)
Fwd Stats            :  0                      0
Drop InProf          :  0                      0
Drop OutProf         :  0                      0

Egress Queue 8 (nc)
Fwd Stats            :  20842                  1938306
Drop InProf          :  0                      0
Drop OutProf         :  0                      0

-------------------------------------------------------------------------------
Service Endpoints
-------------------------------------------------------------------------------
Endpoint name                : coreSide
Description                  : (Not Specified)
Revert time                  : 0
Act Hold Delay               : 0
Standby Signaling Master     : true
Tx Active                    : 1413:1501
Tx Active Up Time            : 0d 03:48:41
Revert Time Count Down       : N/A
Tx Active Change Count       : 2
Last Tx Active Change        : 02/21/2011 13:07:12
-------------------------------------------------------------------------------
Members
-------------------------------------------------------------------------------
Spoke-sdp: 1413:1501 Prec:1                        Oper Status: Up
Spoke-sdp: 1613:1501 Prec:2                        Oper Status: Up
===============================================================================
Endpoint name                : accessSide
Description                  : (Not Specified)
Revert time                  : 0
Act Hold Delay               : 0
Standby Signaling Master     : false
Tx Active                    : lag-3:1501.1501
Tx Active Up Time            : 0d 03:49:08
Revert Time Count Down       : N/A
Tx Active Change Count       : 1
Last Tx Active Change        : 02/21/2011 13:06:45
-------------------------------------------------------------------------------
Members
-------------------------------------------------------------------------------
SAP      : lag-3:1501.1501                         Oper Status: Up
===============================================================================
===============================================================================


*A:DUT-B_sasx>show>service# id 257 all
===============================================================================
Service Detailed Information
===============================================================================
Service Id        : 257                Vpn Id            : 0
Service Type      : Epipe
Description       : (Not Specified)
Customer Id       : 257
Last Status Change: 05/20/2000 11:03:07
Last Mgmt Change  : 05/20/2000 11:03:07
Admin State       : Up                 Oper State        : Up
MTU               : 1514
MTU Check         : Enabled
Vc Switching      : False
SAP Count         : 1                  SDP Bind Count    : 2
```

```
-------------------------------------------------------------------------------
Service Destination Points(SDPs)
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
 Sdp Id 12:64  -(1.1.1.1)
-------------------------------------------------------------------------------
Description     : (Not Specified)
SDP Id             : 12:64                   Type              : Spoke
VC Type            : Ether                   VC Tag            : n/a
Admin Path MTU     : 0                       Oper Path MTU     : 9186
Far End            : 1.1.1.1                 Delivery          : LDP

Admin State        : Up                      Oper State        : Up
Acct. Pol          : None                    Collect Stats     : Disabled
Ingress Label      : 130940                  Egress Label      : 130747
Ing mac Fltr       : n/a                     Egr mac Fltr      : n/a
Ing ip Fltr        : n/a                     Egr ip Fltr       : n/a
Admin ControlWord  : Not Preferred           Oper ControlWord  : False
Admin BW(Kbps)     : 0                       Oper BW(Kbps)     : 0
Last Status Change : 05/20/2000 12:26:22     Signaling         : TLDP
Last Mgmt Change   : 05/20/2000 11:01:59     Force Vlan-Vc     : Disabled
Endpoint           : y                       Precedence        : 4
Class Fwding State : Down
Flags              : None
Peer Pw Bits       : None
Peer Fault Ip      : None
Peer Vccv CV Bits  : None
Peer Vccv CC Bits  : None

KeepAlive Information :
Admin State        : Enabled                 Oper State        : Alive
Hello Time         : 10                      Hello Msg Len     : 0
Max Drop Count     : 3                       Hold Down Time    : 10

Statistics           :
I. Fwd. Pkts.      : 0                       I. Fwd. Octs.     : 0
E. Fwd. Pkts.      : 1981718                 E. Fwd. Octets    : 3016174796
-------------------------------------------------------------------------------
 Sdp Id 24:64  -(4.4.4.4)
-------------------------------------------------------------------------------
Description     : (Not Specified)
SDP Id             : 24:64                   Type              : Spoke
VC Type            : Ether                   VC Tag            : n/a
Admin Path MTU     : 0                       Oper Path MTU     : 9186
Far End            : 4.4.4.4                 Delivery          : LDP

Admin State        : Up                      Oper State        : Up
Acct. Pol          : None                    Collect Stats     : Disabled
Ingress Label      : 130939                  Egress Label      : 130744
Ing mac Fltr       : n/a                     Egr mac Fltr      : n/a
Ing ip Fltr        : n/a                     Egr ip Fltr       : n/a
Admin ControlWord  : Not Preferred           Oper ControlWord  : False
Admin BW(Kbps)     : 0                       Oper BW(Kbps)     : 0
Last Status Change : 05/20/2000 12:28:58     Signaling         : TLDP
Last Mgmt Change   : 05/20/2000 11:03:07     Force Vlan-Vc     : Disabled
Endpoint           : y                       Precedence        : 4
Class Fwding State : Down
Flags              : None
Peer Pw Bits       : None
Peer Fault Ip      : None
Peer Vccv CV Bits  : None
Peer Vccv CC Bits  : None

KeepAlive Information :
```

```
Admin State        : Enabled                  Oper State        : Alive
Hello Time         : 10                       Hello Msg Len     : 0
Max Drop Count     : 3                        Hold Down Time    : 10

Statistics            :
I. Fwd. Pkts.      : 0                        I. Fwd. Octs.     : 0
E. Fwd. Pkts.      : 2020669                  E. Fwd. Octets    : 3075458218
-------------------------------------------------------------------------------
Number of SDPs : 2
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
Service Access Points
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
SAP 1/1/3:64
-------------------------------------------------------------------------------
Service Id         : 257
SAP                : 1/1/3:64                 Encap             : q-tag
Description        : (Not Specified)
Admin State        : Up                       Oper State        : Up
Flags              : None
Last Status Change : 05/19/2000 12:13:40
Last Mgmt Change   : 05/20/2000 11:00:53
Dot1Q Ethertype    : 0x8100                   QinQ Ethertype    : 0x8100

Admin MTU          : 1518                     Oper MTU          : 1518
Ingr IP Fltr-Id    : n/a                      Egr IP Fltr-Id    : n/a
Ingr Mac Fltr-Id   : n/a                      Egr Mac Fltr-Id   : n/a
tod-suite          : None
Endpoint           : x

Acct. Pol          : None                     Collect Stats     : Disabled
-------------------------------------------------------------------------------
QOS
-------------------------------------------------------------------------------
Ingress qos-policy : 1                        Egress qos-policy : 1
-------------------------------------------------------------------------------
Sap Egress Policy (1)
-------------------------------------------------------------------------------
Scope              : Template
Remark             : False                    Remark Pol Id     : 2
Accounting         : frame-based
Description    : Default SAP egress QoS policy.
-------------------------------------------------------------------------------
Queue Rates and Rules
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
QueueId        CIR          CIR Adpt Rule        PIR          PIR Adpt Rule
-------------------------------------------------------------------------------
Queue1          0             closest            max            closest
Queue2          0             closest            max            closest
Queue3          0             closest            max            closest
Queue4          0             closest            max            closest
Queue5          0             closest            max            closest
Queue6          0             closest            max            closest
Queue7          0             closest            max            closest
Queue8          0             closest            max            closest
-------------------------------------------------------------------------------
Parent Details
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
QueueId          Port       CIR Level      PIR Weight
-------------------------------------------------------------------------------
Queue1          True            1             1
```

```
Queue2          True             1             1
Queue3          True             1             1
Queue4          True             1             1
Queue5          True             1             1
Queue6          True             1             1
Queue7          True             1             1
Queue8          True             1             1
-------------------------------------------------------------------------------
High Slope
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
QueueId        State      Start-Avg(%)   Max-Avg(%)   Max-Prob(%)
-------------------------------------------------------------------------------
Queue1          Down            70           90            75
Queue2          Down            70           90            75
Queue3          Down            70           90            75
Queue4          Down            70           90            75
Queue5          Down            70           90            75
Queue6          Down            70           90            75
Queue7          Down            70           90            75
Queue8          Down            70           90            75
-------------------------------------------------------------------------------
Low Slope
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
QueueId        State      Start-Avg(%)   Max-Avg(%)   Max-Prob(%)
-------------------------------------------------------------------------------
Queue1          Down            50           75            75
Queue2          Down            50           75            75
Queue3          Down            50           75            75
Queue4          Down            50           75            75
Queue5          Down            50           75            75
Queue6          Down            50           75            75
Queue7          Down            50           75            75
Queue8          Down            50           75            75
-------------------------------------------------------------------------------
Burst Sizes and Time Average Factor
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
QueueId         CBS            MBS       Time Average Factor        Queue-Mgmt
-------------------------------------------------------------------------------
Queue1          def              def              7           default
Queue2          def              def              7           default
Queue3          def              def              7           default
Queue4          def              def              7           default
Queue5          def              def              7           default
Queue6          def              def              7           default
Queue7          def              def              7           default
Queue8          def              def              7           default
-------------------------------------------------------------------------------
Aggregate Policer (Not Available)
-------------------------------------------------------------------------------
rate               : n/a                      burst            : n/a
-------------------------------------------------------------------------------
Ingress QoS Classifier Usage
-------------------------------------------------------------------------------
Classifiers Allocated: 4                    Meters Allocated   : 2
Classifiers Used     : 1                    Meters Used        : 1
-------------------------------------------------------------------------------
Sap Statistics
-------------------------------------------------------------------------------
                      Packets                Octets
Ingress Stats:        5496351                8244526500
Egress Stats:         0                      0
```

```
-------------------------------------------------------------------------------
Sap per Meter stats
-------------------------------------------------------------------------------
                        Packets                 Octets
Ingress Meter 1 (Unicast)
For. InProf           : 3                       4500
For. OutProf          : 5506597                 8259894000
-------------------------------------------------------------------------------
Sap per Queue stats
-------------------------------------------------------------------------------
                        Packets                 Octets
Egress Queue 1 (be)
Fwd Stats             :  56935                  86541200
Drop InProf           :  0                      0
Drop OutProf          :  0                      0

Egress Queue 2 (l2)
Fwd Stats             :  0                      0
Drop InProf           :  0                      0
Drop OutProf          :  0                      0

Egress Queue 3 (af)
Fwd Stats             :  0                      0
Drop InProf           :  0                      0
Drop OutProf          :  0                      0

Egress Queue 4 (l1)
Fwd Stats             :  0                      0
Drop InProf           :  0                      0
Drop OutProf          :  0                      0

Egress Queue 5 (h2)
Fwd Stats             :  0                      0
Drop InProf           :  0                      0
Drop OutProf          :  0                      0

Egress Queue 6 (ef)
Fwd Stats             :  0                      0
Drop InProf           :  0                      0
Drop OutProf          :  0                      0

Egress Queue 7 (h1)
Fwd Stats             :  0                      0
Drop InProf           :  0                      0
Drop OutProf          :  0                      0

Egress Queue 8 (nc)
Fwd Stats             :  0                      0
Drop InProf           :  0                      0
Drop OutProf          :  0                      0

-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
Service Endpoints
-------------------------------------------------------------------------------
Endpoint name               : x
Description                 : (Not Specified)
Revert time                 : 0
Act Hold Delay              : 0
Ignore Standby Signaling    : false
Suppress Standby Signaling  : true
Block On Mesh Fail          : false
Tx Active                   : 1/1/3:64
Tx Active Up Time           : 0d 01:31:46
```

```
Revert Time Count Down       : N/A
Tx Active Change Count       : 0
Last Tx Active Change        : 05/19/2000 12:13:40
-------------------------------------------------------------------------------
Members
-------------------------------------------------------------------------------
SAP      : 1/1/3:64                                  Oper Status: Up
===============================================================================
Endpoint name                : y
Description                  : (Not Specified)
Revert time                  : 0
Act Hold Delay               : 0
Ignore Standby Signaling     : false
Suppress Standby Signaling   : true
Block On Mesh Fail           : false
Tx Active                    : 12:64
Tx Active Up Time            : 0d 00:00:27
Revert Time Count Down       : N/A
Tx Active Change Count       : 105
Last Tx Active Change        : 05/20/2000 12:32:15
-------------------------------------------------------------------------------
Members
-------------------------------------------------------------------------------
Spoke-sdp: 12:64 Prec:4                          Oper Status: Up
Spoke-sdp: 24:64 Prec:4                          Oper Status: Up
===============================================================================
===============================================================================
*A:DUT-B_sasx>show>service#
```

Sample output (split horizon group)

```
*A:SASX>show>service# id 1 all

===============================================================================
Service Detailed Information
===============================================================================
Service Id        : 1                   Vpn Id            : 0
Service Type      : VPLS
Description       : (Not Specified)
Customer Id       : 1
Last Status Change: 07/22/2011 13:24:25
Last Mgmt Change  : 07/21/2011 09:04:33
Admin State       : Up                  Oper State        : Up
MTU               : 1514                Def. Mesh VC Id   : 1
MTU Check         : Enabled
SAP Count         : 2                   SDP Bind Count    : 0
Snd Flush on Fail : Disabled            Host Conn Verify  : Disabled

-------------------------------------------------------------------------------
Split Horizon Group specifics
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
Split Horizon Group : access
-------------------------------------------------------------------------------
Description       : (Not Specified)
Instance Id       : 1                   Last Change       : 07/21/2011 09:03:50

-------------------------------------------------------------------------------
Service Destination Points(SDPs)
-------------------------------------------------------------------------------
No Matching Entries
-------------------------------------------------------------------------------
Service Access Points
```

```
-------------------------------------------------------------------------------

-------------------------------------------------------------------------------
SAP 1/1/1:10
-------------------------------------------------------------------------------
Service Id         : 1
SAP                : 1/1/1:10                Encap             : q-tag
Description        : (Not Specified)
Admin State        : Up                      Oper State        : Up
Flags              : None
Last Status Change : 07/21/2011 08:47:19
Last Mgmt Change   : 07/22/2011 13:24:25
Dot1Q Ethertype    : 0x8100                  QinQ Ethertype    : 0x8100
Split Horizon Group: (Not Specified)

Max Nbr of MAC Addr: No Limit                Total MAC Addr    : 0
Learned MAC Addr   : 0                       Static MAC Addr   : 0
Admin MTU          : 1518                    Oper MTU          : 1518
Ingr IP Fltr-Id    : n/a                     Egr IP Fltr-Id    : n/a
Ingr Mac Fltr-Id   : n/a                     Egr Mac Fltr-Id   : n/a
Ingr IPv6 Fltr-Id  : n/a                     Egr IPv6 Fltr-Id  : n/a
tod-suite          : None
Egr Agg Rate Limit : max
Mac Learning       : Enabled                 Discard Unkwn Srce: Disabled
Mac Aging          : Enabled                 Mac Pinning       : Disabled
BPDU Translation   : Disabled
L2PT Termination   : Disabled

Acct. Pol          : None                    Collect Stats     : Disabled
-------------------------------------------------------------------------------
Stp Service Access Point specifics
-------------------------------------------------------------------------------
Stp Admin State    : Up                      Stp Oper State    : Down
Core Connectivity  : Down
Port Role          : N/A                     Port State        : Forwarding
Port Number        : 2048                    Port Priority     : 128
Port Path Cost     : 10                      Auto Edge         : Enabled
Admin Edge         : Disabled                Oper Edge         : N/A
Link Type          : Pt-pt                   BPDU Encap        : Dot1d
Root Guard         : Disabled                Active Protocol   : N/A
Last BPDU from     : N/A
CIST Desig Bridge  : N/A                     Designated Port   : N/A

Forward transitions: 0                       Bad BPDUs rcvd    : 0
Cfg BPDUs rcvd     : 0                       Cfg BPDUs tx      : 0
TCN BPDUs rcvd     : 0                       TCN BPDUs tx      : 0
TC bit BPDUs rcvd  : 0                       TC bit BPDUs tx   : 0
RST BPDUs rcvd     : 0                       RST BPDUs tx      : 0
MST BPDUs rcvd     : 0                       MST BPDUs tx      : 0
-------------------------------------------------------------------------------
ARP host
-------------------------------------------------------------------------------
Admin State        : outOfService
Host Limit         : 1                       Min Auth Interval : 15 minutes

-------------------------------------------------------------------------------
QOS
-------------------------------------------------------------------------------
Ingress qos-policy : 1                       Egress qos-policy : 1
-------------------------------------------------------------------------------
Sap Egress Policy (1)
-------------------------------------------------------------------------------
Scope              : Template
Remark             : False                   Remark Pol Id     : 2
```

```
Accounting         : frame-based
Description    : Default SAP egress QoS policy.
-------------------------------------------------------------------------------
Queue Rates and Rules
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
QueueId        CIR          CIR Adpt Rule        PIR          PIR Adpt Rule
-------------------------------------------------------------------------------
Queue1          0              closest            max            closest
Queue2          0              closest            max            closest
Queue3          0              closest            max            closest
Queue4          0              closest            max            closest
Queue5          0              closest            max            closest
Queue6          0              closest            max            closest
Queue7          0              closest            max            closest
Queue8          0              closest            max            closest
-------------------------------------------------------------------------------
Parent Details
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
QueueId          Port       CIR Level      PIR Weight
-------------------------------------------------------------------------------
Queue1          True             1             1
Queue2          True             1             1
Queue3          True             1             1
Queue4          True             1             1
Queue5          True             1             1
Queue6          True             1             1
Queue7          True             1             1
Queue8          True             1             1
-------------------------------------------------------------------------------
High Slope
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
QueueId        State      Start-Avg(%)   Max-Avg(%)   Max-Prob(%)
-------------------------------------------------------------------------------
Queue1          Down            70           90            75
Queue2          Down            70           90            75
Queue3          Down            70           90            75
Queue4          Down            70           90            75
Queue5          Down            70           90            75
Queue6          Down            70           90            75
Queue7          Down            70           90            75
Queue8          Down            70           90            75
-------------------------------------------------------------------------------
Low Slope
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
QueueId        State      Start-Avg(%)   Max-Avg(%)   Max-Prob(%)
-------------------------------------------------------------------------------
Queue1          Down            50           75            75
Queue2          Down            50           75            75
Queue3          Down            50           75            75
Queue4          Down            50           75            75
Queue5          Down            50           75            75
Queue6          Down            50           75            75
Queue7          Down            50           75            75
Queue8          Down            50           75            75
-------------------------------------------------------------------------------
Burst Sizes and Time Average Factor
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
QueueId         CBS            MBS       Time Average Factor        Queue-Mgmt
-------------------------------------------------------------------------------
```

```
Queue1          def               def               7           default
Queue2          def               def               7           default
Queue3          def               def               7           default
Queue4          def               def               7           default
Queue5          def               def               7           default
Queue6          def               def               7           default
Queue7          def               def               7           default
Queue8          def               def               7           default
-------------------------------------------------------------------------------
Aggregate Policer (Available)
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
rate               : n/a                      burst             : n/a
-------------------------------------------------------------------------------
Ingress QoS Classifier Usage
-------------------------------------------------------------------------------
Classifiers Allocated: 4                    Meters Allocated   : 2
Classifiers Used     : 2                    Meters Used        : 2
-------------------------------------------------------------------------------
Sap Statistics
-------------------------------------------------------------------------------
                        Packets                 Octets
Ingress Stats:          0                       0
Egress Stats:           0                       0
Ingress Drop Stats:     0                       0

Extra-Tag Drop Stats:   n/a                     n/a
-------------------------------------------------------------------------------
Sap per Meter stats
-------------------------------------------------------------------------------
                        Packets                 Octets

Ingress Meter 1 (Unicast)
For. InProf           : 0                       0
For. OutProf          : 0                       0

Ingress Meter 11 (Multipoint)
For. InProf           : 0                       0
For. OutProf          : 0                       0
-------------------------------------------------------------------------------
Sap per Queue stats
-------------------------------------------------------------------------------
                        Packets                 Octets

Egress Queue 1 (be)
Fwd Stats             :  333437964              501490697856
Drop InProf           :  0                      0
Drop OutProf          :  329635022              495771073088

Egress Queue 2 (l2)
Fwd Stats             :  0                      0
Drop InProf           :  0                      0
Drop OutProf          :  0                      0

Egress Queue 3 (af)
Fwd Stats             :  0                      0
Drop InProf           :  0                      0
Drop OutProf          :  0                      0

Egress Queue 4 (l1)
Fwd Stats             :  0                      0
Drop InProf           :  0                      0
Drop OutProf          :  0                      0
```

```
Egress Queue 5 (h2)
Fwd Stats            :  0                      0
Drop InProf          :  0                      0
Drop OutProf         :  0                      0

Egress Queue 6 (ef)
Fwd Stats            :  0                      0
Drop InProf          :  0                      0
Drop OutProf         :  0                      0

Egress Queue 7 (h1)
Fwd Stats            :  0                      0
Drop InProf          :  0                      0
Drop OutProf         :  0                      0

Egress Queue 8 (nc)
Fwd Stats            :  0                      0
Drop InProf          :  0                      0
Drop OutProf         :  0                      0

-------------------------------------------------------------------------------
SAP 1/1/25:10
-------------------------------------------------------------------------------
Service Id         : 1
SAP                : 1/1/25:10               Encap             : q-tag
Description        : (Not Specified)
Admin State        : Up                      Oper State        : Up
Flags              : None
Last Status Change : 07/21/2011 08:47:19
Last Mgmt Change   : 07/22/2011 13:24:29
Dot1Q Ethertype    : 0x8100                  QinQ Ethertype    : 0x8100
Split Horizon Group: (Not Specified)

Max Nbr of MAC Addr: No Limit                Total MAC Addr    : 0
Learned MAC Addr   : 0                       Static MAC Addr   : 0
Admin MTU          : 1518                    Oper MTU          : 1518
Ingr IP Fltr-Id    : n/a                     Egr IP Fltr-Id    : n/a
Ingr Mac Fltr-Id   : n/a                     Egr Mac Fltr-Id   : n/a
Ingr IPv6 Fltr-Id  : n/a                     Egr IPv6 Fltr-Id  : n/a
tod-suite          : None
Egr Agg Rate Limit : max
Mac Learning       : Enabled                 Discard Unkwn Srce: Disabled
Mac Aging          : Enabled                 Mac Pinning       : Disabled
BPDU Translation   : Disabled
L2PT Termination   : Disabled

Acct. Pol          : None                    Collect Stats     : Disabled



-------------------------------------------------------------------------------
Stp Service Access Point specifics
-------------------------------------------------------------------------------
Stp Admin State    : Up                      Stp Oper State    : Down
Core Connectivity  : Down
Port Role          : N/A                     Port State        : Forwarding
Port Number        : 2049                    Port Priority     : 128
Port Path Cost     : 10                      Auto Edge         : Enabled
Admin Edge         : Disabled                Oper Edge         : N/A
Link Type          : Pt-pt                   BPDU Encap        : Dot1d
Root Guard         : Disabled                Active Protocol   : N/A
Last BPDU from     : N/A
CIST Desig Bridge  : N/A                     Designated Port   : N/A
```

```
Forward transitions: 0                        Bad BPDUs rcvd    : 0
Cfg BPDUs rcvd     : 0                        Cfg BPDUs tx      : 0
TCN BPDUs rcvd     : 0                        TCN BPDUs tx      : 0
TC bit BPDUs rcvd  : 0                        TC bit BPDUs tx   : 0
RST BPDUs rcvd     : 0                        RST BPDUs tx      : 0
MST BPDUs rcvd     : 0                        MST BPDUs tx      : 0
-------------------------------------------------------------------------------
ARP host
-------------------------------------------------------------------------------
Admin State        : outOfService
Host Limit         : 1                        Min Auth Interval : 15 minutes

-------------------------------------------------------------------------------
QOS
-------------------------------------------------------------------------------
Ingress qos-policy : 1                        Egress qos-policy : 1
-------------------------------------------------------------------------------
Sap Egress Policy (1)
-------------------------------------------------------------------------------
Scope              : Template
Remark             : False                    Remark Pol Id     : 2
Accounting         : frame-based
Description    : Default SAP egress QoS policy.
-------------------------------------------------------------------------------
Queue Rates and Rules
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
QueueId        CIR          CIR Adpt Rule        PIR          PIR Adpt Rule
-------------------------------------------------------------------------------
Queue1          0             closest            max            closest
Queue2          0             closest            max            closest
Queue3          0             closest            max            closest
Queue4          0             closest            max            closest
Queue5          0             closest            max            closest
Queue6          0             closest            max            closest
Queue7          0             closest            max            closest
Queue8          0             closest            max            closest
-------------------------------------------------------------------------------
Parent Details
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
QueueId          Port       CIR Level      PIR Weight
-------------------------------------------------------------------------------
Queue1          True            1             1
Queue2          True            1             1
Queue3          True            1             1
Queue4          True            1             1
Queue5          True            1             1
Queue6          True            1             1
Queue7          True            1             1
Queue8          True            1             1
-------------------------------------------------------------------------------
High Slope
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
QueueId        State      Start-Avg(%)   Max-Avg(%)   Max-Prob(%)
-------------------------------------------------------------------------------
Queue1          Down           70           90           75
Queue2          Down           70           90           75
Queue3          Down           70           90           75
Queue4          Down           70           90           75
Queue5          Down           70           90           75
Queue6          Down           70           90           75
Queue7          Down           70           90           75
```

```
Queue8          Down            70           90           75
-------------------------------------------------------------------------------
Low Slope
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
QueueId        State      Start-Avg(%)   Max-Avg(%)   Max-Prob(%)
-------------------------------------------------------------------------------
Queue1          Down            50           75           75
Queue2          Down            50           75           75
Queue3          Down            50           75           75
Queue4          Down            50           75           75
Queue5          Down            50           75           75
Queue6          Down            50           75           75
Queue7          Down            50           75           75
Queue8          Down            50           75           75
-------------------------------------------------------------------------------
Burst Sizes and Time Average Factor
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
QueueId         CBS            MBS       Time Average Factor        Queue-Mgmt
-------------------------------------------------------------------------------
Queue1          def              def              7           default
Queue2          def              def              7           default
Queue3          def              def              7           default
Queue4          def              def              7           default
Queue5          def              def              7           default
Queue6          def              def              7           default
Queue7          def              def              7           default
Queue8          def              def              7           default
-------------------------------------------------------------------------------
Aggregate Policer (Available)
-------------------------------------------------------------------------------
rate               : n/a                      burst             : n/a
-------------------------------------------------------------------------------
Ingress QoS Classifier Usage
-------------------------------------------------------------------------------
Classifiers Allocated: 4                    Meters Allocated   : 2
Classifiers Used     : 2                    Meters Used        : 2
-------------------------------------------------------------------------------
Sap Statistics
-------------------------------------------------------------------------------
                        Packets                 Octets
Ingress Stats:          662979085               997120543840
Egress Stats:           0                       0
Ingress Drop Stats:     0                       0

Extra-Tag Drop Stats:   n/a                     n/a
-------------------------------------------------------------------------------
Sap per Meter stats
-------------------------------------------------------------------------------
                        Packets                 Octets

Ingress Meter 1 (Unicast)
For. InProf           : 0                       0
For. OutProf          : 0                       0

Ingress Meter 11 (Multipoint)
For. InProf           : 3                       4512
For. OutProf          : 662979118               997120593472
-------------------------------------------------------------------------------
Sap per Queue stats
-------------------------------------------------------------------------------
                        Packets                 Octets
```

```
Egress Queue 1 (be)
Fwd Stats            :  663030839               997198381856
Drop InProf          :  0                       0
Drop OutProf         :  0                       0

Egress Queue 2 (l2)
Fwd Stats            :  0                       0
Drop InProf          :  0                       0
Drop OutProf         :  0                       0

Egress Queue 3 (af)
Fwd Stats            :  0                       0
Drop InProf          :  0                       0
Drop OutProf         :  0                       0

Egress Queue 4 (l1)
Fwd Stats            :  0                       0
Drop InProf          :  0                       0
Drop OutProf         :  0                       0

Egress Queue 5 (h2)
Fwd Stats            :  0                       0
Drop InProf          :  0                       0
Drop OutProf         :  0                       0

Egress Queue 6 (ef)
Fwd Stats            :  0                       0
Drop InProf          :  0                       0
Drop OutProf         :  0                       0

Egress Queue 7 (h1)
Fwd Stats            :  0                       0
Drop InProf          :  0                       0
Drop OutProf         :  0                       0

Egress Queue 8 (nc)
Fwd Stats            :  0                       0
Drop InProf          :  0                       0
Drop OutProf         :  0                       0

-------------------------------------------------------------------------------
VPLS Spanning Tree Information
-------------------------------------------------------------------------------
VPLS oper state    : Up                      Core Connectivity : Down
Stp Admin State    : Down                    Stp Oper State    : Down
Mode               : Rstp                    Vcp Active Prot.  : N/A

Bridge Id          : 80:00.7c:20:64:ad:09:87  Bridge Instance Id: 0
Bridge Priority    : 32768                   Tx Hold Count     : 6
Topology Change    : Inactive                Bridge Hello Time : 2
Last Top. Change   : 0d 00:00:00             Bridge Max Age    : 20
Top. Change Count  : 0                       Bridge Fwd Delay  : 15

Root Bridge        : N/A
Primary Bridge     : N/A

Root Path Cost     : 0                       Root Forward Delay: 0
Rcvd Hello Time    : 0                       Root Max Age      : 0
Root Priority      : 0                       Root Port         : N/A

-------------------------------------------------------------------------------
Forwarding Database specifics
-------------------------------------------------------------------------------
Service Id        : 1                  Mac Move          : Disabled
```

```
Mac Move Rate     : 2                   Mac Move Timeout  : 10
Mac Move Retries  : 3
Table Size        : 250                 Total Count       : 0
Learned Count     : 0                   Static Count      : 0
OAM-learned Count : 0                   DHCP-learned Count: 0
Remote Age        : 900                 Local Age         : 300
High Watermark    : 95%                 Low Watermark     : 90%
Mac Learning      : Enabled             Discard Unknown   : Disabled
Mac Aging         : Enabled             Relearn Only      : False

-------------------------------------------------------------------------------
===============================================================================
IGMP Snooping Base info for service 1
===============================================================================
Admin State : Up
Querier     : No querier found
-------------------------------------------------------------------------------
Sap/Sdp                     Oper  MRtr Send  Max  MVR       Num
Id                          State Port Qries Grps From-VPLS Grps
-------------------------------------------------------------------------------
sap:1/1/1:1                 Up    No   No    None Local     13
sap:1/1/10:1                Up    No   No    None Local     0
===============================================================================
===============================================================================
```

Sample output (meter-override)

```
A:7210SAS>show>service# id 1101 sap 1/2/1:1 detail
Ingress Meter Override
-------------------------------------------------------------------------------

Meter Id           : 1
Admin PIR          : 12000                   Admin CIR         : 10000
Oper PIR           : 12000                   Oper CIR          : 10000
PIR Rule           : closest*                CIR Rule          : closest*
MBS                : 20 KBytes CBS : 15 Kbytes
Mode               : Trtcm2*

* means the value is inherited
-------------------------------------------------------------------------------
A:7210SAS>show>service#
```

Sample output (entropy/hash-label)

```
*A:7210SAS>config>service# /show service id 1 all

===============================================================================
Service Detailed Information
===============================================================================
Service Id        : 1                   Vpn Id            : 0
Service Type      : VPLS
Name              : (Not Specified)
Description       : (Not Specified)
Customer Id       : 1
Last Status Change: 01/07/2000 21:19:14
Last Mgmt Change  : 01/07/2000 21:15:25
Admin State       : Up                  Oper State        : Up
MTU               : 1514                Def. Mesh VC Id   : 1
MTU Check         : Enabled
SAP Count         : 0                   SDP Bind Count    : 1
Snd Flush on Fail : Disabled            Host Conn Verify  : Disabled
SAP Type:         : Any
Propagate MacFlush: Disabled            Per Svc Hashing   : Disabled
```

```
Allow IP Intf Bind: Disabled

-------------------------------------------------------------------------------
Split Horizon Group specifics
-------------------------------------------------------------------------------

-------------------------------------------------------------------------------
ETH-CFM service specifics
-------------------------------------------------------------------------------
Tunnel Faults     : ignore              V-Mep Extensions  : Enabled


-------------------------------------------------------------------------------
Service Destination Points(SDPs)
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
 Sdp Id 1:1  -(2.2.2.2)
-------------------------------------------------------------------------------
Description     : (Not Specified)
SDP Id             : 1:1                      Type              : Spoke
Spoke Descr     : (Not Specified)
Split Horiz Grp    : (Not Specified)
VC Type            : Ether                    VC Tag            : n/a
Admin Path MTU     : 0                        Oper Path MTU     : 9190
Far End            : 2.2.2.2                  Delivery          : MPLS
Tunnel Far End     : 2.2.2.2                  LSP Types         : LDP
Hash Label         : Enabled                  Hash Lbl Sig Cap  : Disabled
Oper Hash Label    : Enabled

Admin State        : Up                       Oper State        : Up
Acct. Pol          : None                     Collect Stats     : Disabled
Ingress Label      : 131069                   Egress Label      : 131069
Ingr Mac Fltr-Id   : n/a                      Egr Mac Fltr-Id   : n/a
Ingr IP Fltr-Id    : n/a                      Egr IP Fltr-Id    : n/a
Ingr IPv6 Fltr-Id  : n/a                      Egr IPv6 Fltr-Id  : n/a
Admin ControlWord  : Not Preferred            Oper ControlWord  : False
Last Status Change : 01/07/2000 21:19:14      Signaling         : TLDP
Last Mgmt Change   : 01/07/2000 21:15:25      Force Vlan-Vc     : Disabled
Endpoint           : N/A                      Precedence        : 4
PW Status Sig      : Enabled
Class Fwding State : Down
Flags              : None
Local Pw Bits      : None
Peer Pw Bits       : None
Peer Fault Ip      : None

Application Profile: None
Transit Policy     : None
Max Nbr of MAC Addr: No Limit                 Total MAC Addr    : 0
Learned MAC Addr   : 0                        Static MAC Addr   : 0

MAC Learning       : Enabled                  Discard Unkwn Srce: Disabled
MAC Aging          : Enabled
BPDU Translation   : Disabled
L2PT Termination   : Disabled
MAC Pinning        : Disabled
Ignore Standby Sig : False                    Block On Mesh Fail: False
Oper Group         : (none)                   Monitor Oper Grp  : (none)
Rest Prot Src Mac  : Disabled
Auto Learn Mac Prot: Disabled                 RestProtSrcMacAct : Disable

Ingress Qos Policy : (none)                   Egress Qos Policy : (none)
Ingress FP QGrp    : (none)                   Egress Port QGrp  : (none)
Ing FP QGrp Inst   : (none)                   Egr Port QGrp Inst: (none)
```

```
KeepAlive Information :
Admin State        : Disabled                Oper State        : Disabled
Hello Time         : 10                      Hello Msg Len     : 0
Max Drop Count     : 3                       Hold Down Time    : 10

Statistics            :
I. Fwd. Pkts.      : 0                       I. Fwd. Octs.     : 0
E. Fwd. Pkts.      : 0                       E. Fwd. Octets    : 0
Extra-Tag-Drop-Pkts: n/a                     Extra-Tag-Drop-Oc*: n/a

-------------------------------------------------------------------------------
Control Channel Status
-------------------------------------------------------------------------------
PW Status          : disabled                Refresh Timer     : <none>
Peer Status Expire : false
Request Timer      : <none>
Acknowledgement    : false

-------------------------------------------------------------------------------
ETH-CFM SDP-Bind specifics
-------------------------------------------------------------------------------
V-MEP Filtering    : Disabled

-------------------------------------------------------------------------------
LDP Information :
-------------------------------------------------------------------------------
LDP LSP Id         : 65537

-------------------------------------------------------------------------------
RSVP/Static LSPs
-------------------------------------------------------------------------------
Associated LSP List :
No LSPs Associated


-------------------------------------------------------------------------------
Stp Service Destination Point specifics
-------------------------------------------------------------------------------
Stp Admin State    : Up                      Stp Oper State    : Down
Core Connectivity  : Down
Port Role          : N/A                     Port State        : Forwarding
Port Number        : 0                       Port Priority     : 128
Port Path Cost     : 10                      Auto Edge         : Enabled
Admin Edge         : Disabled                Oper Edge         : N/A
Link Type          : Pt-pt                   BPDU Encap        : Dot1d
Root Guard         : Disabled                Active Protocol   : N/A
Last BPDU from     : N/A
Designated Bridge  : N/A                     Designated Port Id: 0

Fwd Transitions    : 0                       Bad BPDUs rcvd    : 0
Cfg BPDUs rcvd     : 0                       Cfg BPDUs tx      : 0
TCN BPDUs rcvd     : 0                       TCN BPDUs tx      : 0
TC bit BPDUs rcvd  : 0                       TC bit BPDUs tx   : 0
RST BPDUs rcvd     : 0                       RST BPDUs tx      : 0
-------------------------------------------------------------------------------
Number of SDPs : 1
-------------------------------------------------------------------------------
* indicates that the corresponding row element may have been truncated.
-------------------------------------------------------------------------------
Service Access Points
-------------------------------------------------------------------------------
No Sap Associations
```

```
-------------------------------------------------------------------------------
VPLS Spanning Tree Information
-------------------------------------------------------------------------------
VPLS oper state    : Up                      Core Connectivity : Down
Stp Admin State    : Down                    Stp Oper State    : Down
Mode               : Rstp                    Vcp Active Prot.  : N/A

Bridge Id          : 80:00.c4:08:4a:59:b2:61  Bridge Instance Id: 0
Bridge Priority    : 32768                   Tx Hold Count     : 6
Topology Change    : Inactive                Bridge Hello Time : 2
Last Top. Change   : 0d 00:00:00             Bridge Max Age    : 20
Top. Change Count  : 0                       Bridge Fwd Delay  : 15

Root Bridge        : N/A
Primary Bridge     : N/A

Root Path Cost     : 0                       Root Forward Delay: 0
Rcvd Hello Time    : 0                       Root Max Age      : 0
Root Priority      : 0                       Root Port         : N/A

-------------------------------------------------------------------------------
Forwarding Database specifics
-------------------------------------------------------------------------------
Service Id        : 1                  Mac Move          : Disabled
Mac Move Rate     : 2                  Mac Move Timeout  : 10
Mac Move Retries  : 3
Table Size        : 250                Total Count       : 0
Learned Count     : 0                  Static Count      : 0
OAM-learned Count : 0                  DHCP-learned Count: 0
Remote Age        : 900                Local Age         : 300
High Watermark    : 95%                Low Watermark     : 90%
Mac Learning      : Enabled            Discard Unknown   : Disabled
Mac Aging         : Enabled            Relearn Only      : False

-------------------------------------------------------------------------------
IGMP Snooping Base info
-------------------------------------------------------------------------------
Admin State : Down
Querier     : No querier found
-------------------------------------------------------------------------------
Sap/Sdp                    Oper  MRtr Send  Max  MVR       Num
Id                         State Port Qries Grps From-VPLS Grps
-------------------------------------------------------------------------------
sdp:1:1                    Up    No   No    None N/A       0

-------------------------------------------------------------------------------
Service Endpoints
-------------------------------------------------------------------------------
No Endpoints found.
-------------------------------------------------------------------------------

===============================================================================
VPLS Sites
===============================================================================
Site               Site-Id   Dest               Mesh-SDP  Admin   Oper  Fwdr
```

Table 30: Output fields: service ID All

Label	Description
Service Id	The service identifier.

Label	Description
VPN Id	The number that identifies the VPN.
Service Type	Specifies the type of service.
VLL Type	Specifies the VLL type.
SDP Id	The SDP identifier.
Description	Generic information about the service.
Customer Id	The customer identifier.
Last Mgmt Change	The date and time of the most recent management-initiated change.
Endpoint	Specifies the name of the service endpoint.
Flags	Specifies the conditions that affect the operating status of this SAP. Display output includes: ServiceAdminDown, SapAdminDown, InterfaceAdminDown, PortOperDown, L2OperDown, RelearnLimit Exceeded, RxProtSrcMac, ParentIfAdminDown, TodResource Unavail, TodMssResourceUnavail, SapParamMismatch, Sap IngressNamedPoolMismatch, SapEgressNamedPoolMismatch, NoSapEpipeRingNode.
SAP Count	The number of SAPs specified for this service.
SDP Bind Count	The number of SDPs bound to this service.
Split Horizon Group Specifics	
Split Horizon Group	Name of the split horizon group for this VPLS.
Description	Description of the split horizon group.
Instance ID	Displays the Instance identifier of the split horizon group.
Last Changed	Displays the date and time of most recent change to the split horizon group.
Split Horizon Group	Displays the name of the split horizon group the SAP or spoke-SDP is associated.
Service Destination Points (SDPs)	
SDP Id	The SDP identifier.
Type	Indicates whether this Service SDP binding is a spoke or a mesh.
Admin Path MTU	The configured largest service frame size (in octets) that can be transmitted through this SDP to the far-end router, without requiring the packet to be fragmented.

Label	Description
Oper Path MTU	The actual largest service frame size (in octets) that can be transmitted through this SDP to the far-end router, without requiring the packet to be fragmented.
Delivery	Specifies the type of delivery used by the SDP: MPLS.
Admin State	The administrative state of this SDP.
Oper State	The operational state of this SDP.
Jitter Buffer (packets)	Indicates the jitter buffer length in number of packet buffers.
Playout Threshold (packets)	Indicates the playout buffer packets threshold in number of packet buffers.
Playout Threshold (packets)	Indicates the current packet depth of the jitter buffer.
Peer Pw Bits	Indicates the bits set by the LDP peer when there is a fault on its side of the pseudowire. LAC failures occur on the SAP that has been configured on the pipe service, PSN bits are set by SDP-binding failures on the pipe service. The pwNotForwarding bit is set when none of the preceding failures apply, such as an MTU mismatch failure. This value is only applicable if the peer is using the pseudowire status signaling method to indicate faults. pwNotForwarding — Pseudowire not forwarding lacIngressFault Local — Attachment circuit RX fault lacEgresssFault Local — Attachment circuit TX fault psnIngressFault Local — PSN-facing PW RX fault psnEgressFault Local — PSN-facing PW TX fault pwFwdingStandby — Pseudowire in standby mode
LLF Admin State	Displays the Link Loss Forwarding administrative state.
LLF Oper State	Displays the Link Loss Forwarding operational state.
Standby Signaling Master	Indicates whether the parameter standby signaling master is enabled.
Hash Label	Indicates whether use of PW hash label is enabled.
Oper Hash Label	Indicates whether the MPLS packet originated by the node is using PW Hash label if the value displayed is Enabled. If the value displayed is Disabled, the MPLS packets originated by the node is not using Pseudowire Hash label.
Hash Lbl Sig Cap	Indicates whether PW hash label signaling is enabled.

base

Syntax

base

Context

show>service>id

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays basic information about the service ID, including service type, description, and SAPs.

Output

The following output is an example of basic service information, and Table 31: Output fields: service ID base describes the output fields.

Sample output

```
A:Dut-A# show service id 1101 base
===============================================================================
Service Basic Information
===============================================================================
Service Id        : 1101               Vpn Id            : 1101
Service Type      : Epipe
Description       : Default epipe description for service id 1101
Customer Id       : 1
Last Status Change: 07/07/2009 18:13:43
Last Mgmt Change  : 07/07/2009 14:39:14
Admin State       : Up                 Oper State        : Up
MTU               : 1514
Vc Switching      : False
SAP Count         : 1                  SDP Bind Count    : 1
-------------------------------------------------------------------------------
Service Access & Destination Points
-------------------------------------------------------------------------------
Identifier                             Type         AdmMTU  OprMTU  Adm  Opr
-------------------------------------------------------------------------------
sap:lag-4:1101                         q-tag        9212    9212    Up   Up
sdp:1409:1101 S(10.20.1.4)             n/a          0       9186    Up   Up
===============================================================================
A:Dut-A#
```

Table 31: Output fields: service ID base

Label	Description
Service Id	The service identifier.
Vpn Id	Specifies the VPN ID assigned to the service.

Label	Description
Service Type	The type of service: Epipe, VPLS
Description	Generic information about the service.
Customer Id	The customer identifier.
Last Mgmt Change	The date and time of the most recent management-initiated change to this customer.
Adm	The configured state of the service.
Oper	The operating state of the service.
Mtu	The largest frame size (in octets) that the service can handle.
Def. Mesh VC Id	This object is only valid in services that accept mesh SDP bindings. It is used to validate the VC ID portion of each mesh SDP binding defined in the service.
SAP Count	The number of SAPs defined on the service.
SDP Bind Count	The number of SDPs bound to the service.
Identifier	Specifies the service access (SAP) points.
Type	Specifies the signaling protocol used to obtain the ingress and egress labels used in frames transmitted and received.
AdmMTU	Specifies the configured largest service frame size (in octets) that can be transmitted, without requiring the packet to be fragmented.
PBB Tunnel Point	Specifies the endpoint in the B-VPLS environment where the Epipe terminates.
Admin MTU	Specifies the B-VPLS admin MTU.
Backbone-Flooding	Specifies whether the traffic is flooded in the B-VPLS for the destination instead of unicast. If the backbone destination MAC is in the B-VPLS FDB, it is unicast.
ISID	The 24-bit field carrying the service instance identifier associated with the frame. It is used at the destination PE as a demultiplexor field.

endpoint

Syntax

endpoint [*endpoint-name*]

Context

show>service>id

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays service endpoint information.

Parameters

endpoint-name

Specifies the name of an existing endpoint for the service.

Output

The following output is an example of endpoint information, and Table 32: Output fields: service ID endpoint describes the output fields.

Sample output

```
*A:Dut-A>show>service>id# endpoint

===============================================================================
Service 1501 endpoints
===============================================================================
Endpoint name               : coreSide
Description                 : (Not Specified)
Revert time                 : 0
Act Hold Delay              : 0
Standby Signaling Master    : true
Tx Active                   : 1413:1501
Tx Active Up Time           : 0d 03:46:25
Revert Time Count Down      : N/A
Tx Active Change Count      : 2
Last Tx Active Change       : 02/21/2011 13:07:12
-------------------------------------------------------------------------------
Members
-------------------------------------------------------------------------------
Spoke-sdp: 1413:1501 Prec:1                       Oper Status: Up
Spoke-sdp: 1613:1501 Prec:2                       Oper Status: Up
===============================================================================
Endpoint name               : accessSide
Description                 : (Not Specified)
Revert time                 : 0
Act Hold Delay              : 0
Standby Signaling Master    : false
Tx Active                   : lag-3:1501.1501
Tx Active Up Time           : 0d 03:46:52
Revert Time Count Down      : N/A
Tx Active Change Count      : 1
Last Tx Active Change       : 02/21/2011 13:06:45
-------------------------------------------------------------------------------
Members
-------------------------------------------------------------------------------
SAP      : lag-3:1501.1501                        Oper Status: Up
===============================================================================
===============================================================================
```

Table 32: Output fields: service ID endpoint

Label	Description
Service endpoints	
Endpoint name	Identifies the endpoint.
Revert time	Displays the revert time setting for the active spoke SDP.
Act Hold Delay	Not applicable.
Ignore Standby Signaling	Indicates whether standby signaling is ignored. True — standby signaling is ignored False — standby signaling is not ignored
Suppress Standby Signaling	Indicates whether standby signaling is suppressed. True — standby signaling is suppressed False — standby signaling is not suppressed
Tx Active	Identifies the actively transmitting spoke SDP.
Tx Active Up Time	Indicates the length of time that the active spoke SDP has been up.
Revert Time Count Down	Not applicable.
Tx Active Change Count	Indicates the number of times that there has been a change of active spoke SDPs.
Last Tx Active Change	Indicates the date and time when a different spoke SDP became the actively transmitting spoke SDP.

labels

Syntax

labels

Context

show>service>id

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays the labels being used by the service.

Output

The following output is an example of service label information, and Table 33: Output fields: service ID labels describes the output fields.

Sample output

```
*A:ALA-12# show service id 1 labels
===============================================================================
Martini Service Labels
===============================================================================
Svc Id     Sdp Id             Type I.Lbl        E.Lbl
-------------------------------------------------------------------------------
1          10:1               Mesh 0            0
1          20:1               Mesh 0            0
1          30:1               Mesh 0            0
1          40:1               Mesh 130081       131061
1          60:1               Mesh 131019       131016
1          100:1              Mesh 0            0
-------------------------------------------------------------------------------
Number of Bound SDPs : 6
-------------------------------------------------------------------------------
*A:ALA-12#
```

Table 33: Output fields: service ID labels

Label	Description
Svc Id	The service identifier.
Sdp Id	The SDP identifier.
Type	Indicates whether the SDP is a spoke or a mesh.
I. Lbl	The VC label used by the far-end device to send packets to this device in this service by the SDP.
E. Lbl	The VC label used by this device to send packets to the far-end device in this service by the SDP.

sap

Syntax

sap *sap-id* [**detail**]

Context

show>service>id

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays information for the SAPs associated with the service. If no optional parameters are specified, a summary of all associated SAPs is displayed.

Parameters

sap-id

Specifies the ID that displays SAPs for the service in the form *slot*/*mda*/*port*[**.***channel*]. See Common CLI command descriptions for command syntax.

interface *interface-name*

Displays information for the specified IP interface.

ip-address *ip-address*

Displays information associated with the specified IP address.

detail

Displays more information for the SAP.

Output

The following outputs are examples of SAP information, and Table 34: Output fields: service ID SAP describes the output fields.

- Sample output, Table 34: Output fields: service ID SAP
- Sample output for 7210 SAS-R6 and 7210 SAS-R12

Sample output

```
*A:DUT-B_sasx>show>service# id 257 sap 1/1/3:64 detail

===============================================================================
Service Access Points(SAP)
===============================================================================
Service Id         : 257
SAP                : 1/1/3:64                Encap             : q-tag
Description        : (Not Specified)
Admin State        : Up                      Oper State        : Up
Flags              : None
Last Status Change : 05/19/2000 12:13:40
Last Mgmt Change   : 05/20/2000 11:00:53
Loopback Mode      : Internal                No-svc-port used : 1/1/13
Loopback Src Addr  : 00:00:00:22:22:22
Loopback Dst Addr  : 00:00:00:11:11:11
Dot1Q Ethertype    : 0x8100                  QinQ Ethertype    : 0x8100

Admin MTU          : 1518                    Oper MTU          : 1518
Ingr IP Fltr-Id    : n/a                     Egr IP Fltr-Id    : n/a
Ingr Mac Fltr-Id   : n/a                     Egr Mac Fltr-Id   : n/a
tod-suite          : None
Endpoint           : x

Acct. Pol          : None                    Collect Stats     : Disabled
Ignore Oper Down : Disabled

-------------------------------------------------------------------------------
QOS
-------------------------------------------------------------------------------
Ingress qos-policy : 1                       Egress qos-policy : 1
```

```
-------------------------------------------------------------------------------
Sap Egress Policy (1)
-------------------------------------------------------------------------------
Scope              : Template
Remark             : False                    Remark Pol Id     : 2
Accounting         : frame-based
Description    : Default SAP egress QoS policy.
-------------------------------------------------------------------------------
Queue Rates and Rules
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
QueueId        CIR          CIR Adpt Rule        PIR          PIR Adpt Rule
-------------------------------------------------------------------------------
Queue1          0              closest            max            closest
Queue2          0              closest            max            closest
Queue3          0              closest            max            closest
Queue4          0              closest            max            closest
Queue5          0              closest            max            closest
Queue6          0              closest            max            closest
Queue7          0              closest            max            closest
Queue8          0              closest            max            closest
-------------------------------------------------------------------------------
Parent Details
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
QueueId          Port       CIR Level      PIR Weight
-------------------------------------------------------------------------------
Queue1          True             1             1
Queue2          True             1             1
Queue3          True             1             1
Queue4          True             1             1
Queue5          True             1             1
Queue6          True             1             1
Queue7          True             1             1
Queue8          True             1             1
-------------------------------------------------------------------------------
High Slope
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
QueueId        State      Start-Avg(%)   Max-Avg(%)   Max-Prob(%)
-------------------------------------------------------------------------------
Queue1          Down            70           90            75
Queue2          Down            70           90            75
Queue3          Down            70           90            75
Queue4          Down            70           90            75
Queue5          Down            70           90            75
Queue6          Down            70           90            75
Queue7          Down            70           90            75
Queue8          Down            70           90            75
-------------------------------------------------------------------------------
Low Slope
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
QueueId        State      Start-Avg(%)   Max-Avg(%)   Max-Prob(%)
-------------------------------------------------------------------------------
Queue1          Down            50           75            75
Queue2          Down            50           75            75
Queue3          Down            50           75            75
Queue4          Down            50           75            75
Queue5          Down            50           75            75
Queue6          Down            50           75            75
Queue7          Down            50           75            75
Queue8          Down            50           75            75
-------------------------------------------------------------------------------
```

```
Burst Sizes and Time Average Factor
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
QueueId         CBS            MBS       Time Average Factor        Queue-Mgmt
-------------------------------------------------------------------------------
Queue1          def              def              7           default
Queue2          def              def              7           default
Queue3          def              def              7           default
Queue4          def              def              7           default
Queue5          def              def              7           default
Queue6          def              def              7           default
Queue7          def              def              7           default
Queue8          def              def              7           default
-------------------------------------------------------------------------------
Aggregate Policer (Not Available)
-------------------------------------------------------------------------------
rate               : n/a                      burst            : n/a
-------------------------------------------------------------------------------
Ingress QoS Classifier Usage
-------------------------------------------------------------------------------
Classifiers Allocated: 4                    Meters Allocated   : 2
Classifiers Used     : 1                    Meters Used        : 1
-------------------------------------------------------------------------------
Sap Statistics
-------------------------------------------------------------------------------
                      Packets                Octets
Ingress Stats:        5726350                8589525000
Egress Stats:         0                      0
-------------------------------------------------------------------------------
Sap per Meter stats
-------------------------------------------------------------------------------
                      Packets                Octets

Ingress Meter 1 (Unicast)
For. InProf          : 3                     4500
For. OutProf         : 5733754               8600631000
-------------------------------------------------------------------------------
Sap per Queue stats
-------------------------------------------------------------------------------
                      Packets                Octets

Egress Queue 1 (be)
Fwd Stats            :  56935                86541200
Drop InProf          :  0                    0
Drop OutProf         :  0                    0

Egress Queue 2 (l2)
Fwd Stats            :  0                    0
Drop InProf          :  0                    0
Drop OutProf         :  0                    0

Egress Queue 3 (af)
Fwd Stats            :  0                    0
Drop InProf          :  0                    0
Drop OutProf         :  0                    0

Egress Queue 4 (l1)
Fwd Stats            :  0                    0
Drop InProf          :  0                    0
Drop OutProf         :  0                    0

Egress Queue 5 (h2)
Fwd Stats            :  0                    0
Drop InProf          :  0                    0
```

```
Drop OutProf         :  0                       0

Egress Queue 6 (ef)
Fwd Stats            :  0                       0
Drop InProf          :  0                       0
Drop OutProf         :  0                       0

Egress Queue 7 (h1)
Fwd Stats            :  0                       0
Drop InProf          :  0                       0
Drop OutProf         :  0                       0

Egress Queue 8 (nc)
Fwd Stats            :  0                       0
Drop InProf          :  0                       0
Drop OutProf         :  0                       0
===============================================================================
```

Sample output for 7210 SAS-R6 and 7210 SAS-R12

```
*A:Dut-A# show service id 10 sap 5/1/1:800 detail
===============================================================================
Service Access Points(SAP)
===============================================================================
Service Id         : 10
SAP                : 5/1/1:800               Encap             : q-tag
Description        : (Not Specified)
Admin State        : Up                      Oper State        : Down
Flags              : PortOperDown
Last Status Change : 11/07/2017 04:48:25
Last Mgmt Change   : 11/07/2017 05:02:47
Dot1Q Ethertype    : 0x8100                  QinQ Ethertype    : 0x8100
Split Horizon Group: (Not Specified)
Admin MTU          : 1518                    Oper MTU          : 1518
Ingr IP Fltr-Id    : n/a                     Egr IP Fltr-Id    : n/a
Ingr Mac Fltr-Id   : n/a                     Egr Mac Fltr-Id   : n/a
Ingr IPv6 Fltr-Id  : n/a                     Egr IPv6 Fltr-Id  : n/a
BGP IPv4 FlowSpec  : Disabled
BGP IPv6 FlowSpec  : Disabled
tod-suite          : None
Egr Agg Rate CIR   : 0                       Egr Agg Rate PIR  : max
                                             Limit Unused BW   : Disabled
Acct. Pol          : None                    Collect Stats     : Disabled
Anti Spoofing      : None                    Dynamic Hosts     : Enabled
Oper Group         : (none)                  Monitor Oper Grp  : (none)
Host Lockout Plcy  : n/a
Lag Link Map Prof  : (none)
-------------------------------------------------------------------------------
QOS
-------------------------------------------------------------------------------
Ingress qos-policy : 17                      Egress qos-policy : 1
Table-based        : enabled
-------------------------------------------------------------------------------
Aggregate Policer
-------------------------------------------------------------------------------
Rate               : n/a                     Burst             : n/a
-------------------------------------------------------------------------------
Egress Aggregate Meter
-------------------------------------------------------------------------------
Rate               : n/a                     Burst             : n/a
-------------------------------------------------------------------------------
Ingress QoS Classifier Usage
```

```
-------------------------------------------------------------------------------
Classifiers Allocated: 60                   Meters Allocated   : 30
Classifiers Used     : 9                    Meters Used        : 8
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
Sap Statistics
-------------------------------------------------------------------------------
                        Packets                Octets
Ingress Stats:          0                      0
Egress Stats:           0                      0
Ingress Drop Stats:     0                      0

Extra-Tag Drop Stats:   n/a                    n/a
-------------------------------------------------------------------------------
Sap per Meter stats (in/out counter mode)
-------------------------------------------------------------------------------
                        Packets                Octets
Ingress Meter 1
For. InProf           : 0                      0
For. OutProf          : 0                      0

Ingress Meter 2
For. InProf           : 0                      0
For. OutProf          : 0                      0

Ingress Meter 3
For. InProf           : 0                      0
For. OutProf          : 0                      0

Ingress Meter 4
For. InProf           : 0                      0
For. OutProf          : 0                      0

Ingress Meter 5
For. InProf           : 0                      0
For. OutProf          : 0                      0

Ingress Meter 6
For. InProf           : 0                      0
For. OutProf          : 0                      0

Ingress Meter 7
For. InProf           : 0                      0
For. OutProf          : 0                      0

Ingress Meter 8
For. InProf           : 0                      0
For. OutProf          : 0                      0
===============================================================================
```

Table 34: Output fields: service ID SAP

Label	Description
Service Id	The service identifier.
SAP	The SAP and qtag.
Encap	The encapsulation type of the SAP.
Ethertype	Specifies an Ethernet type II Ethertype value.

Label	Description
Admin State	The administrative state of the SAP.
Oper State	The operating state of the SAP.
Flags	Specifies the conditions that affect the operating status of this SAP. Display output includes: ServiceAdminDown, SapAdminDown, InterfaceAdminDown, PortOperDown, PortMTUTooSmall, L2OperDown, SapEgressQoSMismatch,RelearnLimitExceeded, RxProtSrcMac, ParentIfAdminDown, TodResourceUnavail, Tod MssResourceUnavail, SapParamMismatch, ServiceMTUToo Small, SapIngressNamedPoolMismatch, SapEgressNamedPool Mismatch, NoSapEpipeRingNode.
Last Status Change	The time of the most recent operating status change to this SAP.
Last Mgmt Change	The time of the most recent management-initiated change to this SAP.
Admin MTU	The configured largest service frame size (in octets) that can be transmitted through to the far-end router, without requiring the packet to be fragmented.
Oper MTU	The actual largest service frame size (in octets) that can be transmitted through to the far-end router, without requiring the packet to be fragmented.
Ingress qos-policy	The ingress QoS policy ID assigned to the SAP.
Egress qos-policy	The egress QoS policy ID assigned to the SAP.
Ingress Filter-Id	The ingress filter policy ID assigned to the SAP.
Egress Filter-Id	The egress filter policy ID assigned to the SAP.
Acct. Pol	The accounting policy ID assigned to the SAP.
Collect Stats	Specifies whether collect stats is enabled.
Ignore Oper Down	Displays whether the user has enabled or disabled the **ignore-oper-down** parameter.
LLF Admin State	Displays the Link Loss Forwarding administrative state.
LLF Oper State	Displays the Link Loss Forwarding operational state.
Loopback Mode	Displays the Ethernet port loop back mode.
Loopback Src Addr	Displays the configured loopback source address.
Loopback Dst Addr	Displays the configured loopback destination address.

Label	Description
No-svc-port used	Displays the port ID of the port on which no service is configured. This port is used for the port loopback with MAC swap functionality.
Loopback Mode	Displays the Ethernet port loopback mode.
Loopback Src Addr	Displays the configured loopback source address.
Loopback Dst Addr	Displays the configured loopback destination address.
No-svc-port used	Displays the port ID of the port on which no service is configured. This port is used for the port loop back with MAC swap functionality.
Table-based	Indicates the use of table-based resource classification: Enabled (table-based) or Disabled (CAM-based).

sdp

Syntax

sdp [*sdp-id* | **far-end** *ip-addr*] [**detail**]

Context

show>service>id

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays information for the SDPs associated with the service.

If no optional parameters are specified, a summary of all associated SDPs is displayed.

Parameters

sdp-id

Displays information only for the specified SDP ID.

Default All SDPs.

Values 1 to 17407

far-end *ip-addr*

Displays only SDPs matching the specified far-end IP address.

Default SDPs with any far-end IP address.

detail

Displays detailed SDP information.

Output

Table 35: Output fields: service ID SDP describes the show service ID SDP output fields.

Sample output

Table 35: Output fields: service ID SDP

Label	Description
Sdp Id	The SDP identifier.
Type	Indicates whether the SDP is a spoke or a mesh.
Split Horizon Group	Name of the split horizon group that the SDP belongs to.
VC Type	The VC type, ether, vlan, or vpls.
VC Tag	The explicit dot1q value used when encapsulating to the SDP far end.
I. Lbl	The VC label used by the far-end device to send packets to this device in this service by the SDP.
Admin Path MTU	The operating path MTU of the SDP is equal to the admin path MTU (when one is set) or the dynamically computed tunnel MTU, when no admin path MTU is set (the default case).
Oper Path MTU	The actual largest service frame size (in octets) that can be transmitted through this SDP to the far-end router, without requiring the packet to be fragmented.
Far End	Specifies the IP address of the remote end of the MPLS tunnel defined by this SDP.
Delivery	Specifies the type of delivery used by the SDP: MPLS.
Admin State	The administrative state of this SDP.
Oper State	The current state of this SDP.
Ingress Label	The label used by the far-end device to send packets to this device in this service by this SDP.
Egress Label	The label used by this device to send packets to the far-end device in this service by the SDP.
Last Changed	The date and time of the most recent change to the SDP.
Signaling	Specifies the signaling protocol used to obtain the ingress and egress labels used in frames transmitted and received on this SDP.

Label	Description
Admin State	The administrative state of the keepalive process.
Oper State	The operational state of the keepalive process.
Hello Time	Transmission frequency of the SDP echo request messages.
Max Drop Count	Specifies the maximum number of consecutive SDP echo request messages that can be unacknowledged before the keepalive protocol reports a fault.
Hello Msg Len	The length of the SDP echo request messages transmitted on this SDP.
Hold Down Time	Specifies the amount of time to wait before the keepalive operating status is eligible to enter the alive state.
I. Fwd. Pkts.	Specifies the number of forwarded ingress packets.
I. Dro. Pkts	Specifies the number of dropped ingress packets.
E. Fwd. Pkts.	Specifies the number of forwarded egress packets.
Associated LSP List	When the SDP type is MPLS, a list of LSPs used to reach the far-end router displays. All the LSPs in the list must terminate at the IP address specified in the Far End field.

split-horizon-group

Syntax

split-horizon-group [*group-name*]

Context

show>service>id

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays service split horizon groups.

Output

The following output is an example of split horizon group information, and Table 36: Output fields: split horizon group describes the output fields.

Sample output

```
*A:7210-SAS>show>service# id 1 split-horizon-group
```

```
===============================================================================
Service: Split Horizon Group
===============================================================================
Name                            Description
-------------------------------------------------------------------------------
    access
-------------------------------------------------------------------------------
R = Residential Split Horizon Group
A = Auto Created Split Horizon Group
No. of Split Horizon Groups: 1
===============================================================================
*A:7210-SAS>show>service# id 1 split-horizon-group access

===============================================================================
Service: Split Horizon Group
===============================================================================
Name                            Description
-------------------------------------------------------------------------------
    access
-------------------------------------------------------------------------------
Associations
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
R = Residential Split Horizon Group
SAPs Associated : 0               SDPs Associated : 0
*A:7210-SAS>show>service#
```

Table 36: Output fields: split horizon group

Label	Description
Name	The name of the split horizon group. When preceded by "R", the group is a residential split horizon group.
Description	A description of the split horizon group as configured by the user.
Associations	A list of SAPs and SDPs associated with the split horizon group.

stp

Syntax

stp [**detail**]

Context

show>service>id

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays information for the spanning tree protocol instance for the service.

Parameters

detail

Displays more information.

Output

The following output is an example of STP information, and Table 37: Output fields: show service ID STP describes the output fields.

Sample output

```
A:Dut-A>show>service>id# stp
===============================================================================
Stp info, Service 305
===============================================================================
Bridge Id          : 00:0d.00:20:ab:cd:00:01  Top. Change Count : 5
Root Bridge        : This Bridge              Stp Oper State    : Up
Primary Bridge     : N/A                      Topology Change   : Inactive
Mode               : Rstp                     Last Top. Change  : 0d 08:35:16
Vcp Active Prot.   : N/A
Root Port          : N/A                      External RPC      : 0
===============================================================================
Stp port info
===============================================================================
Sap/Sdp Id         Oper-     Port-      Port-       Port-  Oper-  Link-  Active
                   State     Role       State       Num    Edge   Type   Prot.
-------------------------------------------------------------------------------
1/1/16:305         Up        Designated Forward     2048   False  Pt-pt  Rstp
lag-4:305          Up        Designated Forward     2000   False  Pt-pt  Rstp
1217:305           Up        N/A        Forward     2049   N/A    Pt-pt  N/A
1317:305           Up        N/A        Forward     2050   N/A    Pt-pt  N/A
1417:305           Up        N/A        Forward     2051   N/A    Pt-pt  N/A
1617:305           Pruned    N/A        Discard     2052   N/A    Pt-pt  N/A
===============================================================================
A:Dut-A>show>service>id#


A:Dut-A>show>service>id# stp detail
===============================================================================
Spanning Tree Information
===============================================================================
VPLS Spanning Tree Information
-------------------------------------------------------------------------------
VPLS oper state    : Up                       Core Connectivity : Down
Stp Admin State    : Up                       Stp Oper State    : Up
Mode               : Rstp                     Vcp Active Prot.  : N/A

Bridge Id          : 00:0d.00:20:ab:cd:00:01  Bridge Instance Id: 13
Bridge Priority    : 0                        Tx Hold Count     : 6
Topology Change    : Inactive                 Bridge Hello Time : 2
Last Top. Change   : 0d 08:35:29              Bridge Max Age    : 20
Top. Change Count  : 5                        Bridge Fwd Delay  : 15
MST region revision: 0                        Bridge max hops   : 20
MST region name    :

Root Bridge        : This Bridge
Primary Bridge     : N/A

Root Path Cost     : 0                        Root Forward Delay: 15
Rcvd Hello Time    : 2                        Root Max Age      : 20
Root Priority      : 13                       Root Port         : N/A
-------------------------------------------------------------------------------
```

```
Spanning Tree Sap/Spoke SDP Specifics
-------------------------------------------------------------------------------
SAP Identifier     : 1/1/16:305               Stp Admin State   : Up
Port Role          : Designated               Port State        : Forwarding
Port Number        : 2048                     Port Priority     : 128
Port Path Cost     : 10                       Auto Edge         : Enabled
Admin Edge         : Disabled                 Oper Edge         : False
Link Type          : Pt-pt                    BPDU Encap        : PVST
Root Guard         : Disabled                 Active Protocol   : Rstp
Last BPDU from     : 80:04.00:0a:1b:2c:3d:4e
CIST Desig Bridge  : This Bridge              Designated Port   : 34816
Forward transitions: 5                        Bad BPDUs rcvd    : 0
Cfg BPDUs rcvd     : 0                        Cfg BPDUs tx      : 0
TCN BPDUs rcvd     : 0                        TCN BPDUs tx      : 0
RST BPDUs rcvd     : 29                       RST BPDUs tx      : 23488
MST BPDUs rcvd     : 0                        MST BPDUs tx      : 0

SAP Identifier     : lag-4:305                Stp Admin State   : Up
Port Role          : Designated               Port State        : Forwarding
Port Number        : 2000                     Port Priority     : 128
Port Path Cost     : 10                       Auto Edge         : Enabled
Admin Edge         : Disabled                 Oper Edge         : False
Link Type          : Pt-pt                    BPDU Encap        : Dot1d
Root Guard         : Disabled                 Active Protocol   : Rstp
Last BPDU from     : 80:04.00:0a:1b:2c:3d:4e
CIST Desig Bridge  : This Bridge              Designated Port   : 34768
Forward transitions: 4                        Bad BPDUs rcvd    : 0
Cfg BPDUs rcvd     : 0                        Cfg BPDUs tx      : 0
TCN BPDUs rcvd     : 0                        TCN BPDUs tx      : 0
RST BPDUs rcvd     : 23                       RST BPDUs tx      : 23454
MST BPDUs rcvd     : 0                        MST BPDUs tx      : 0

SDP Identifier     : 1217:305                 Stp Admin State   : Down
Port Role          : N/A                      Port State        : Forwarding
Port Number        : 2049                     Port Priority     : 128
Port Path Cost     : 10                       Auto Edge         : Enabled
Admin Edge         : Disabled                 Oper Edge         : N/A
Link Type          : Pt-pt                    BPDU Encap        : Dot1d
Root Guard         : Disabled                 Active Protocol   : N/A
Last BPDU from     : N/A
Designated Bridge  : N/A                      Designated Port Id: 0
Fwd Transitions    : 0                        Bad BPDUs rcvd    : 0
Cfg BPDUs rcvd     : 0                        Cfg BPDUs tx      : 0
TCN BPDUs rcvd     : 0                        TCN BPDUs tx      : 0
RST BPDUs rcvd     : 0                        RST BPDUs tx      : 0

SDP Identifier     : 1317:305                 Stp Admin State   : Down
Port Role          : N/A                      Port State        : Forwarding
Port Number        : 2050                     Port Priority     : 128
Port Path Cost     : 10                       Auto Edge         : Enabled
Admin Edge         : Disabled                 Oper Edge         : N/A
Link Type          : Pt-pt                    BPDU Encap        : Dot1d
Root Guard         : Disabled                 Active Protocol   : N/A
Last BPDU from     : N/A
Designated Bridge  : N/A                      Designated Port Id: 0
Fwd Transitions    : 0                        Bad BPDUs rcvd    : 0
Cfg BPDUs rcvd     : 0                        Cfg BPDUs tx      : 0
TCN BPDUs rcvd     : 0                        TCN BPDUs tx      : 0
RST BPDUs rcvd     : 0                        RST BPDUs tx      : 0

SDP Identifier     : 1417:305                 Stp Admin State   : Down
Port Role          : N/A                      Port State        : Forwarding
Port Number        : 2051                     Port Priority     : 128
Port Path Cost     : 10                       Auto Edge         : Enabled
```

```
Admin Edge         : Disabled                 Oper Edge         : N/A
Link Type          : Pt-pt                    BPDU Encap        : Dot1d
Root Guard         : Disabled                 Active Protocol   : N/A
Last BPDU from     : N/A
Designated Bridge  : N/A                      Designated Port Id: 0
Fwd Transitions    : 1                        Bad BPDUs rcvd    : 0
Cfg BPDUs rcvd     : 0                        Cfg BPDUs tx      : 0
TCN BPDUs rcvd     : 0                        TCN BPDUs tx      : 0
RST BPDUs rcvd     : 0                        RST BPDUs tx      : 0

SDP Identifier     : 1617:305                 Stp Admin State   : Down
Port Role          : N/A                      Port State        : Discarding
Port Number        : 2052                     Port Priority     : 128
Port Path Cost     : 10                       Auto Edge         : Enabled
Admin Edge         : Disabled                 Oper Edge         : N/A
Link Type          : Pt-pt                    BPDU Encap        : Dot1d
Root Guard         : Disabled                 Active Protocol   : N/A
Last BPDU from     : N/A
Designated Bridge  : N/A                      Designated Port Id: 0
Fwd Transitions    : 0                        Bad BPDUs rcvd    : 0
Cfg BPDUs rcvd     : 0                        Cfg BPDUs tx      : 0
TCN BPDUs rcvd     : 0                        TCN BPDUs tx      : 0
RST BPDUs rcvd     : 0                        RST BPDUs tx      : 0
===============================================================================
A:Dut-A>show>service>id#

*7210-SAS>show>service>id# stp detail

===============================================================================
Spanning Tree Information
===============================================================================

-------------------------------------------------------------------------------
VPLS Spanning Tree Information
-------------------------------------------------------------------------------
VPLS oper state    : Up                       Core Connectivity : Down
Stp Admin State    : Up                       Stp Oper State    : Up
Mode               : Mstp                     Vcp Active Prot.  : N/A

Bridge Id          : 80:00.00:25:ba:04:66:a0  Bridge Instance Id: 0
Bridge Priority    : 32768                    Tx Hold Count     : 6
Topology Change    : Inactive                 Bridge Hello Time : 2
Last Top. Change   : 0d 02:54:16              Bridge Max Age    : 20
Top. Change Count  : 27                       Bridge Fwd Delay  : 15

Root Bridge        : 40:00.7c:20:64:ac:ff:63
Primary Bridge     : N/A

Root Path Cost     : 10                       Root Forward Delay: 15
Rcvd Hello Time    : 2                        Root Max Age      : 20
Root Priority      : 16384                    Root Port         : 2048

MSTP info for CIST :
Regional Root      : 80:00.7c:20:64:ad:04:5f  Root Port         : 2048
Internal RPC       : 10                       Remaining Hopcount: 19
MSTP info for MSTI 1 :
Regional Root      : This Bridge              Root Port         : N/A
Internal RPC       : 0                        Remaining Hopcount: 20
MSTP info for MSTI 2 :
Regional Root      : 00:02.7c:20:64:ad:04:5f  Root Port         : 2048
Internal RPC       : 10                       Remaining Hopcount: 19


-------------------------------------------------------------------------------
```

```
Spanning Tree Sap Specifics
-------------------------------------------------------------------------------
SAP Identifier     : 1/1/7:0                 Stp Admin State   : Up
Port Role          : Root                    Port State        : Forwarding
Port Number        : 2048                    Port Priority     : 128
Port Path Cost     : 10                      Auto Edge         : Enabled
Admin Edge         : Disabled                Oper Edge         : False
Link Type          : Pt-pt                   BPDU Encap        : Dot1d
Root Guard         : Disabled                Active Protocol   : Mstp
Last BPDU from     : 80:00.7c:20:64:ad:04:5f  Inside Mst Region : True
CIST Desig Bridge  : 80:00.7c:20:64:ad:04:5f  Designated Port   : 34816
MSTI 1 Port Prio   : 128                     Port Path Cost    : 10
MSTI 1 Desig Brid  : This Bridge             Designated Port   : 34816
MSTI 2 Port Prio   : 128                     Port Path Cost    : 10
MSTI 2 Desig Brid  : 00:02.7c:20:64:ad:04:5f  Designated Port   : 34816
Forward transitions: 17                      Bad BPDUs rcvd    : 0
Cfg BPDUs rcvd     : 0                       Cfg BPDUs tx      : 0
TCN BPDUs rcvd     : 0                       TCN BPDUs tx      : 0
RST BPDUs rcvd     : 0                       RST BPDUs tx      : 0
MST BPDUs rcvd     : 7310                    MST BPDUs tx      : 7277

SAP Identifier     : 1/1/8:0                 Stp Admin State   : Up
Port Role          : Alternate               Port State        : Discarding
Port Number        : 2049                    Port Priority     : 128
Port Path Cost     : 10                      Auto Edge         : Enabled
Admin Edge         : Disabled                Oper Edge         : False
Link Type          : Pt-pt                   BPDU Encap        : Dot1d
Root Guard         : Disabled                Active Protocol   : Mstp
Last BPDU from     : 80:00.7c:20:64:ad:04:5f  Inside Mst Region : True
CIST Desig Bridge  : 80:00.7c:20:64:ad:04:5f  Designated Port   : 34817
MSTI 1 Port Prio   : 128                     Port Path Cost    : 10
MSTI 1 Desig Brid  : This Bridge             Designated Port   : 34817
MSTI 2 Port Prio   : 128                     Port Path Cost    : 10
MSTI 2 Desig Brid  : 00:02.7c:20:64:ad:04:5f  Designated Port   : 34817
Forward transitions: 14                      Bad BPDUs rcvd    : 0
Cfg BPDUs rcvd     : 0                       Cfg BPDUs tx      : 0
TCN BPDUs rcvd     : 0                       TCN BPDUs tx      : 0
RST BPDUs rcvd     : 0                       RST BPDUs tx      : 0
MST BPDUs rcvd     : 7326                    MST BPDUs tx      : 7307

SAP Identifier     : 1/1/9:0                 Stp Admin State   : Up
Port Role          : Designated              Port State        : Forwarding
Port Number        : 2050                    Port Priority     : 128
Port Path Cost     : 10                      Auto Edge         : Enabled
Admin Edge         : Disabled                Oper Edge         : True
Link Type          : Pt-pt                   BPDU Encap        : Dot1d
Root Guard         : Disabled                Active Protocol   : Mstp
Last BPDU from     : N/A                     Inside Mst Region : True
CIST Desig Bridge  : This Bridge             Designated Port   : 34818
MSTI 1 Port Prio   : 128                     Port Path Cost    : 10
MSTI 1 Desig Brid  : This Bridge             Designated Port   : 34818
MSTI 2 Port Prio   : 128                     Port Path Cost    : 10
MSTI 2 Desig Brid  : This Bridge             Designated Port   : 34818
Forward transitions: 2                       Bad BPDUs rcvd    : 0
Cfg BPDUs rcvd     : 0                       Cfg BPDUs tx      : 0
TCN BPDUs rcvd     : 0                       TCN BPDUs tx      : 0
RST BPDUs rcvd     : 0                       RST BPDUs tx      : 0
MST BPDUs rcvd     : 0                       MST BPDUs tx      : 7415

SAP Identifier     : 1/1/25:0                Stp Admin State   : Up
Port Role          : Alternate               Port State        : Discarding
Port Number        : 2051                    Port Priority     : 128
Port Path Cost     : 10                      Auto Edge         : Enabled
Admin Edge         : Disabled                Oper Edge         : False
```

```
Link Type          : Pt-pt                    BPDU Encap        : Dot1d
Root Guard         : Disabled                 Active Protocol   : Mstp
Last BPDU from     : 80:00.7c:20:64:ad:04:5f  Inside Mst Region : True
CIST Desig Bridge  : 80:00.7c:20:64:ad:04:5f  Designated Port   : 34820
MSTI 1 Port Prio   : 128                      Port Path Cost    : 10
MSTI 1 Desig Brid  : This Bridge              Designated Port   : 34819
MSTI 2 Port Prio   : 128                      Port Path Cost    : 10
MSTI 2 Desig Brid  : 00:02.7c:20:64:ad:04:5f  Designated Port   : 34820
Forward transitions: 10                       Bad BPDUs rcvd    : 0
Cfg BPDUs rcvd     : 0                        Cfg BPDUs tx      : 0
TCN BPDUs rcvd     : 0                        TCN BPDUs tx      : 0
RST BPDUs rcvd     : 0                        RST BPDUs tx      : 0
MST BPDUs rcvd     : 7329                     MST BPDUs tx      : 7303

SAP Identifier     : lag-1:0                  Stp Admin State   : Up
Port Role          : Alternate                Port State        : Discarding
Port Number        : 2052                     Port Priority     : 128
Port Path Cost     : 10                       Auto Edge         : Enabled
Admin Edge         : Disabled                 Oper Edge         : False
Link Type          : Pt-pt                    BPDU Encap        : Dot1d
Root Guard         : Disabled                 Active Protocol   : Mstp
Last BPDU from     : 80:00.7c:20:64:ad:04:5f  Inside Mst Region : True
CIST Desig Bridge  : 80:00.7c:20:64:ad:04:5f  Designated Port   : 34822
MSTI 1 Port Prio   : 128                      Port Path Cost    : 10
MSTI 1 Desig Brid  : This Bridge              Designated Port   : 34820
MSTI 2 Port Prio   : 128                      Port Path Cost    : 10
MSTI 2 Desig Brid  : 00:02.7c:20:64:ad:04:5f  Designated Port   : 34822
Forward transitions: 11                       Bad BPDUs rcvd    : 0
Cfg BPDUs rcvd     : 0                        Cfg BPDUs tx      : 0
TCN BPDUs rcvd     : 0                        TCN BPDUs tx      : 0
RST BPDUs rcvd     : 0                        RST BPDUs tx      : 0
MST BPDUs rcvd     : 7322                     MST BPDUs tx      : 7299

===============================================================================
```

Table 37: Output fields: show service ID STP

Label	Description
RSTP Admin State	Indicates the administrative state of the Rapid Spanning Tree Protocol instance associated with this service.
Core Connectivity	Indicates the connectivity status to the core.
RSTP Oper State	Indicates the operational state of the Rapid Spanning Tree Protocol instance associated with this service. This field is applicable only when STP is enabled on the router.
Bridge-id	Specifies the MAC address used to identify this bridge in the network.
Hold Time	Specifies the interval length during which no more than two Configuration BPDUs shall be transmitted by this bridge.
Bridge fwd delay	Specifies how fast a bridge changes its state when moving toward the forwarding state.
Bridge Hello time	Specifies the amount of time between the transmission of Configuration BPDUs.

Label	Description
Bridge max age	Specifies the maximum age of Spanning Tree Protocol information learned from the network on any port before it is discarded. This is the actual value that this bridge is currently using.
Bridge priority	Defines the priority of the Spanning Tree Protocol instance associated with this service.
Topology change	Specifies whether a topology change is currently in progress.
Last Top. change	Specifies the time (in hundredths of a second) after the last time a topology change was detected by the Spanning Tree Protocol instance associated with this service.
Top. change count	Specifies the total number of topology changes detected by the Spanning Tree Protocol instance associated with this service after the management entity was last reset or initialized.
Root bridge-id	Specifies the bridge identifier of the root of the spanning tree as determined by the Spanning Tree Protocol instance associated with this service. This value is used as the Root Identifier parameter in all Configuration BPDUs originated by this node.
Root path cost	Specifies the cost of the path to the root bridge as seen from this bridge.
Root forward delay	Specifies how fast the root changes its state when moving toward the forwarding state.
hello time	Specifies the amount of time between the transmission of configuration BPDUs.
Root max age	Specifies the maximum age of Spanning Tree Protocol information learned from the network on any port before it is discarded.
Root priority	This object specifies the priority of the bridge that is currently selected as root-bridge for the network.
Root port	Specifies the port number of the port which provides the lowest cost path from this bridge to the root bridge.
SAP Identifier	The ID of the access port where this SAP is defined.
RSTP State	The operational state of RSTP.
STP Port State	Specifies the port identifier of the port on the designated bridge for this port's segment.
BPDU encap	Specifies the type of encapsulation used on BPDUs sent out and received on this SAP.

Label	Description
Port Number	Specifies the value of the port number field which is contained in the least significant 12 bits of the 16-bit port ID associated with this SAP.
Priority	Specifies the value of the port priority field which is contained in the most significant 4 bits of the 16-bit port ID associated with this SAP.
Cost	Specifies the contribution of this port to the path cost of paths toward the spanning tree root which include this port.
Fast Start	Specifies whether Fast Start is enabled on this SAP.
Designated Port	Specifies the port identifier of the port on the designated bridge for this port's segment.
Designated Bridge	Specifies the bridge identifier of the bridge that this port considers to be the designated bridge for this port's segment.

3.10.2.4 Clear commands

id

Syntax

id *service-id*

Context

clear>service

clear>service>statistics

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command clears commands for a specific service.

Parameters

service-id

Specifies the ID that uniquely identifies a service.

Values *service-id*: 1 to 214748364

svc-name: A string up to 64 characters.

spoke-sdp

Syntax

spoke-sdp *sdp-id*:*vc-id* **ingress-vc-label**

Context

clear>service>id

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command clears and resets the spoke-SDP bindings for the service.

Parameters

sdp-id

Specifies the spoke-SDP ID to be reset.

Values 1 to 17407

vc-id

Specifies the virtual circuit ID on the SDP ID to be reset.

Values 1 to 4294967295

ingress-vc-label

Keyword that specifies to clear the ingress VC label.

sap

Syntax

sap *sap-id* {**all** | **counters** | **stp**}

Context

clear>service>statistics

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command clears SAP statistics for a SAP.

Parameters

sap-id

Specifies the physical port identifier portion of the SAP definition. See Common CLI command descriptions for command syntax.

all

Clears all SAP queue statistics and STP statistics.

counters

Clears all queue statistics associated with the SAP.

stp

Clears all STP statistics associated with the SAP.

l2pt

Clears all L2PT statistics associated with the SDP.

sdp

Syntax

sdp *sdp-id* **keep-alive**

Context

clear>service>statistics

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command clears keepalive statistics associated with the SDP ID.

Parameters

sdp-id

Specifies the SDP ID for which to clear keepalive statistics.

Values 1 to 17407

counters

Syntax

counters

Context

clear>service>statistics>id

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command clears all traffic queue counters associated with the service ID.

spoke-sdp

Syntax

spoke-sdp *sdp-id*[**:***vc-id*] {**all** | **counters** | **stp**}

Context

clear>service>statistics>id

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command clears statistics for the spoke-SDP bound to the service.

Parameters

sdp-id

Specifies the spoke-SDP ID for which to clear statistics.

Values 1 to 17407

vc-id

Specifies the virtual circuit ID on the SDP ID to be reset.

Values 1 to 4294967295

all

Clears all queue statistics and STP statistics associated with the SDP.

counters

Clears all queue statistics associated with the SDP.

stp

Clears all STP statistics associated with the SDP.

stp

Syntax

stp

Context
clear>service>statistics>id

Platforms
Supported on all 7210 SAS platforms as described in this document

Description
This command clears all spanning tree statistics for the service ID.

statistics

Syntax
statistics

Context
clear>service

Platforms
Supported on all 7210 SAS platforms as described in this document

Description
Commands in this context clear statistics for a specific service entity.

3.10.2.5 Debug commands

id

Syntax
id *service-id*

Context
debug>service

Platforms
Supported on all 7210 SAS platforms as described in this document

Description
This command debugs commands for a specific service.

Parameters

service-id

Specifies the ID that uniquely identifies a service.

sap

Syntax

[**no**] **sap** *sap-id*

Context

debug>service>id

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables debugging for a particular SAP.

Parameters

sap-id

Specifies the SAP ID.

event-type

Syntax

[**no**] **event-type** {**arp** | **config-change** | **oper-status-change**}

Context

debug>service>id

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables a particular debugging event type.

The **no** form of this command disables the event type debugging.

Parameters

arp

Displays ARP events.

config-change

Debugs configuration change events.

svc-oper-status-change

Debugs service operational status changes.

Output

The following output is an example of event type debugging information.

Sample output

```
A:bksim180# debug service id 1000 sap 1/7/1 event-type arp
DEBUG OUTPUT show on CLI is as follows:
3 2008/11/17 18:13:24.35 UTC MINOR: DEBUG #2001 Base Service 1000 SAP 1/7/1
"Service 1000 SAP 1/7/1:
RX: ARP_REQUEST (0x0001)
hwType     : 0x0001
prType     : 0x0800
hwLength   : 0x06
prLength   : 0x04
srcMac     : 8c:c7:01:07:00:03
destMac    : 00:00:00:00:00:00
srcIp      : 239.1.1.2
destIp     : 239.1.1.1
"

4 2008/11/17 18:13:24.35 UTC MINOR: DEBUG #2001 Base Service 1000 SAP 1/7/1
"Service 1000 SAP 1/7/1:
TX: ARP_RESPONSE (0x0002)
hwType     : 0x0001
prType     : 0x0800
hwLength   : 0x06
prLength   : 0x04
srcMac     : 00:03:0a:0a:0a:0a
destMac    : 8c:c7:01:07:00:03
srcIp      : 239.1.1.1
destIp     : 239.1.1.2
"
```

sdp

Syntax

[**no**] **sdp** *sdp-id:vc-id*

Context

debug>service>id

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables debugging for a particular SDP.

Parameters

sdp-id

Specifies the SDP ID.

4 Ethernet Virtual Private Networks

This chapter provides information about Ethernet Virtual Private Networks (EVPN) for 7210 SAS-R6 and 7210 SAS-R12.

4.1 EVPN applications

EVPN, as described in RFC 7432, *BGP MPLS-Based Ethernet VPN,* is an IETF technology that uses a new BGP address family and allows Virtual Private LAN Services (VPLS) to operate in a similar manner to IP-VPNs, in which the MAC addresses and information to set up flooding trees are distributed by BGP.

EVPN is designed to fill the gaps of traditional L2VPN technologies, such as VPLS. The main objective of EVPN is to build E-LAN services similar to IP-VPNs defined in RFC 4364, while supporting MAC learning in the control plane (distributed using multi-protocol BGP (MP-BGP)), efficient multi-destination traffic delivery, and single-active/all-active multi-homing.

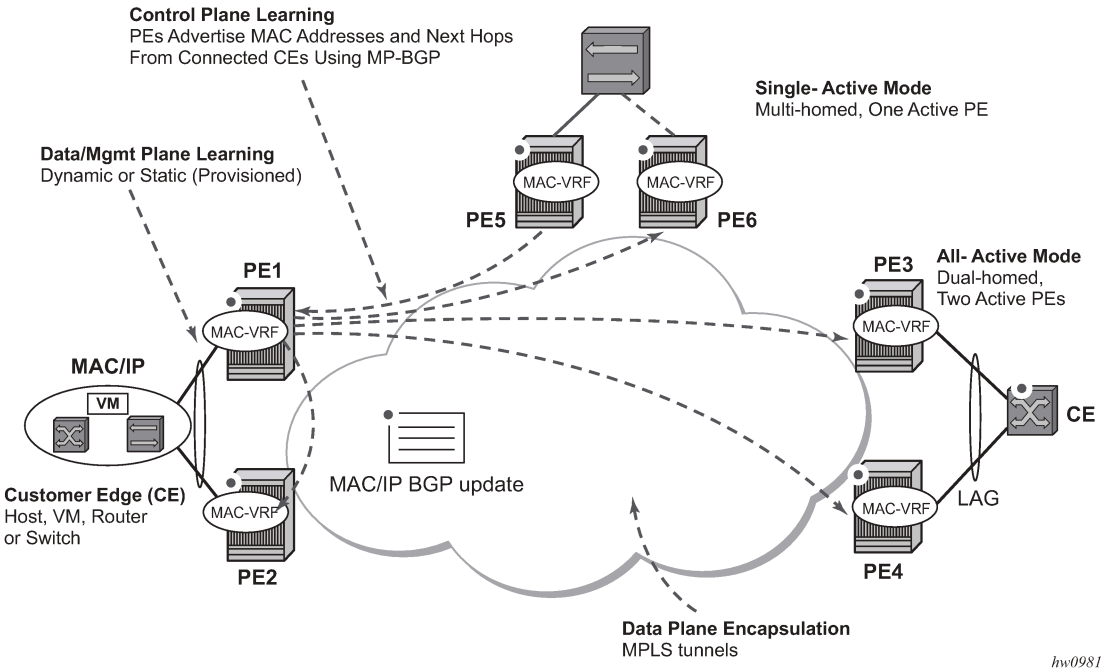
EVPN can be used as the control plane for different data plane encapsulations. The Nokia implementation supports EVPN for MPLS tunnels (EVPN-MPLS), where PEs are connected by any type of MPLS tunnel. EVPN-MPLS is generally used as an evolution for VPLS services. The EVPN-MPLS functionality is standardized in RFC 7432.

4.1.1 EVPN for MPLS tunnels in E-LAN services

The following figure shows the use of EVPN for MPLS tunnels on the 7210 SAS. In this example, EVPN is used as the control plane for E-LAN services.

Note:
The following figure shows generic EVPN capabilities. It does not imply support on all 7210 SAS platforms referenced in this guide. For more information about the supported EVPN capabilities for the platforms referenced in this guide, see the following sections in this chapter.

Figure 34: EVPN for MPLS in VPLS services



Service providers that offer E-LAN services request EVPN for its multi-homing capabilities and to leverage the optimization EVPN provides.

EVPN supports single-active multi-homing (per-service load-balancing multi-homing). Although VPLS already supports single-active multi-homing, EVPN single-active multi-homing is seen as the superior technology because of its mass-withdrawal capabilities to speed up convergence in scaled environments.

EVPN technology provides significant benefits, including:

- IP-VPN-like operation and control for E-LAN services
- reduction and (in some cases) suppression of the broadcast, unknown unicast, and multicast (BUM) traffic in the network
- simple provisioning and management
- new set of tools to control the distribution of MAC addresses and ARP entries in the network
- potential to use single unified control-plane for both L2 VPN services and L3 VPN services
- superior multi-homing capabilities

The SR OS EVPN-MPLS implementation is compliant with RFC 7432.

4.2 EVPN for MPLS tunnels

This section provides information about EVPN for MPLS tunnels (EVPN-MPLS).

4.2.1 BGP-EVPN control plane for MPLS tunnels

The following table lists the supported EVPN routes and their usage in the 7210 SAS EVPN-MPLS.

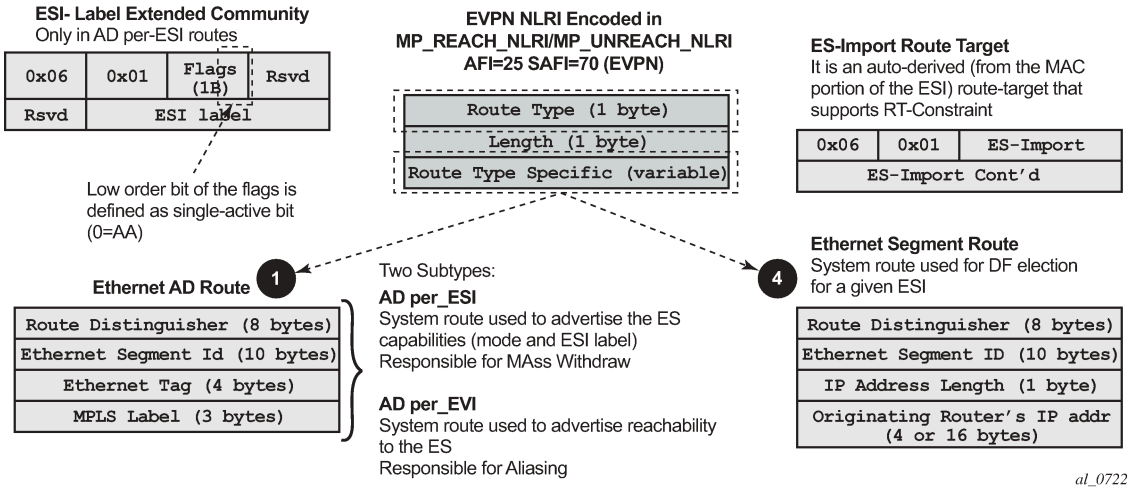
Table 38: EVPN routes and usage

EVPN route	Usage	EVPN-MPLS 7210 SAS support
Type 1 - Ethernet auto-discovery route (A-D)	Mass-withdraw, ESI labels, aliasing	Yes[13]
Type 2 - MAC/IP advertisement route	MAC/IP advertisement, IP advertisement for ARP resolution	Yes
Type 3 - Inclusive multicast Ethernet Tag route	Flooding tree setup (BUM flooding)	Yes
Type 4 - Ethernet segment (ES) route	ES discovery and DF election	Yes

RFC 7432 describes the BGP-EVPN control plane for MPLS tunnels. If EVPN multi-homing is not required, two route types are needed to set up a basic EVPN Instance (EVI): MAC/IP Advertisement and the Inclusive Multicast Ethernet Tag routes. If multi-homing is required, the ES and the Auto-Discovery routes are also needed.

When EVPN multi-homing is enabled in the system, two additional routes are required. The following figure shows the fields in routes type 1 and 4 and their associated extended communities.

Figure 35: EVPN routes type 1 and 4



13 ESI labels and aliasing are not supported on 7210 SAS platforms.

4.2.1.1 EVPN route type 3 — inclusive multicast Ethernet tag route

The 7210 SAS router generates this route type for setting up the flooding tree (BUM flooding) for a specified VPLS service. The received inclusive multicast routes add entries to the VPLS flood list. When BGP-EVPN MPLS is enabled, the standard supports ingress replication, p2mp mLDP, and composite tunnels as tunnel types in route type 3. On the 7210 SAS, only ingress replication is supported.

4.2.1.2 EVPN route type 2 — MAC/IP advertisement route

The 7210 SAS router generates this route type for advertising MAC addresses (and IP addresses if proxy-ARP/proxy-ND is enabled). The router generates MAC advertisement routes for the following entities:

- learned MACs on SAPs, if the **mac-advertisement** command is enabled
- conditional static MACs, if the **mac-advertisement** command is enabled
- learned MACs on spoke-SDPs, if the **mac-advertisement** command is enabled

Note:

- The **unknown-mac-route** command is not supported for EVPN-MPLS services.
- Proxy-ARP and proxy-ND commands are not supported for IP/MAC associations learned over spoke-SDP.

The route type 2 generated by a router uses the following fields and values:

- **route distinguisher**

  This is taken from the route distinguisher (RD) of the VPLS service within the BGP context. The RD can be configured or derived from the **bgp-evpn evi** value.

- **ethernet segment identifier (ESI)**

  This is zero (0) for MACs learned from single-homed CEs and different from zero for MACs learned from multi-homed CEs.

- **ethernet tag ID**

  This is zero (0).

- **MAC address length**

  This is always 48.

- **MAC address**

  This is learned or statically configured.

- **IP address and IP address length**
  - This is the IP address associated with the MAC being advertised with a length of 32 (or 128 for IPv6).
  - In general, any MAC route without IP has IPL (IP length) = 0 and the IP is omitted.
  - When received, any IPL value not equal to zero, 32, or 128 discards the route.

- **MPLS label 1**

This carries the MPLS label allocated by the system to the VPLS service. The label value is encoded in the high-order 20 bits of the field and is the same label used in type 3 routes for the same service, unless **bgp-evpn mpls ingress-replication-bum-label** is configured in the service.

- **MPLS label 2**

  This is 0.

- **MAC mobility extended community**

  This is used for signaling the sequence number in case of MAC moves and the "sticky" bit in case of advertising conditional static MACs. If a MAC route is received with a MAC mobility of *ext-community*, the sequence number and the "sticky" bit are considered for the route selection.

4.2.1.3 EVPN route type 1 — Ethernet Auto-Discovery route

The 7210 SAS router generates this route type to advertise for multi-homing functions. The system can generate two types of Ethernet Auto-Discovery (AD) routes:

- Ethernet AD route per-ESI
- Ethernet AD route per-EVI

The Ethernet AD per-ESI route uses the following fields and values:

- **route distinguisher**

  This is taken from the service-level RD.

- **ethernet segment identifier (ESI)**

  This contains a 10-byte identifier as configured in the system for a specified **ethernet-segment**.

- **ethernet tag ID**

  This value, MAX-ET (0xFFFFFFFF), is reserved and used only for AD routes per ESI.

- **MPLS label**

  This is zero (0).

- **ESI label extended community**

  This includes the single-active bit (0 for all-active and 1 for single-active) and ESI label for all-active multi-homing split-horizon. The 7210 SAS always sets the single-active bit to "1", as long as single-active is supported. In addition, 7210 SAS does not allocate and send the ESI label for single-active multi-homing.

- **route-target extended community**

  This is taken from the service level route target (RT).

The system can send only a separate Ethernet AD per-ESI route per service.

The Ethernet AD per-EVI route uses the following fields and values:

- **route distinguisher**

  This is taken from the service level RD.

- **ethernet segment identifier (ESI)**

  This contains a 10-byte identifier, as configured in the system for a specified **ethernet-segment**.

- **ethernet tag ID**

This is zero (0).

- **MPLS label**

  This encodes the unicast label allocated for the service (high-order 20 bits).

- **route-target extended community**

  This is taken from the service level RT.

Note: The AD per-EVI route is not sent with the ESI label Extended Community.

4.2.1.4 EVPN route type 4 — ES route

The 7210 SAS router generates this route type for multi-homing ES discovery and DF (Designated Forwarder) election, as follows:

- **Route Distinguisher**

  This is taken from the system level RD.

- **Ethernet Segment Identifier (ESI)**

  This contains a 10-byte identifier, as configured in the system for a specified **ethernet-segment**.

- **ES-import route-target community**

  This value is automatically derived from the MAC address portion of the ESI.

  This extended community is treated as an RT and is supported by RT-constraint (route-target BGP family).

4.2.1.5 BGP tunnel encapsulation extended community

The following routes are sent with the RFC 5512 BGP Encapsulation Extended Community:

- MAC/IP
- Inclusive Multicast Ethernet Tag
- AD per-EVI routes

ES routes and AD per-ESI routes are not sent with this extended community.

The router processes MPLS encapsulation: 10, the BGP tunnel encapsulation tunnel value registered by IANA for RFC 5512. Any other tunnel value makes the route "treat-as-withdraw".

If the encapsulation value is MPLS, the BGP validates the high-order 20 bits of the label field, ignoring the low-order 4 bits.

If the encapsulation extended community (as defined in RFC 5512) is not present in a received route, BGP treats the route as an MPLS. On the 7210 SAS, only MPLS encapsulation is supported.

4.2.2 EVPN for MPLS tunnels in VPLS services

EVPN can be used in MPLS networks where provider edge (PE) routers are interconnected through any type of MPLS tunnel, including RSVP-TE, LDP, BGP, Segment Routing IS-IS, or Segment Routing OSPF.

As with VPRN services, the tunnel selection for a VPLS service (with BGP-EVPN MPLS enabled) is based on the **auto-bind-tunnel** command.

The EVPN-MPLS VPLS service uses a regular VPLS service where EVPN-MPLS "bindings" can coexist with SAPs. The following example shows configuration output for a VPLS service with EVPN-MPLS.

Example: VPLS service with EVPN-MPLS configuration output

```
*A:PE-1>config>service>vpls# info
----------------------------------------------
description "evpn-mpls-service"
bgp

bgp-evpn
         evi 10
         mpls
                 auto-bind-tunnel resolution any
                 no shutdown

sap 1/1/1:1 create
exit
----------------------------------------------
```

First configure a **bgp-evpn** context as **mpls**. In addition, the minimum set of commands that must be configured to set up the EVPN-MPLS instance are the **evi** and the **auto-bind-tunnel resolution** commands.

Note:
Ensure that the EVI and the system IP are configured before executing the **configure>service>vpls>bgp-evpn>mpls>no shutdown** command.

The **evi** value, which is the EVPN instance (EVI) identifier, is unique in the system. It is used by the service-carving algorithm for multi-homing (if configured) and for auto-deriving RT and RDs in EVPN-MPLS services.

If the **evi** value is not specified, the value is zero and no RD or RTs are auto-derived from it. If it is specified, and no other RD or RT are configured in the service, the following applies:

- the RD is derived from: *system_ip*:**evi**
- the RT is derived from: *autonomous-system*:**evi**

Note:
When vsi-import and vsi-export polices are configured, the RT must be configured in the policies, and those values take precedence over the auto-derived RTs. The operational RT for a service is displayed by the **show service id** *svc-id* **bgp** command output. Nokia recommends that the user should not configure a VPLS ID using the **bgp-ad>vpls-id** command in the service.

When the **evi** command is configured, a **config>service>vpls>bgp** node (even empty) is required to output correct information using the **show service id 1 bgp** and **show service system bgp-route-distinguisher** commands.

The configuration of an EVI is enforced for EVPN services with SAPs in an Ethernet segment. See EVPN multi-homing in VPLS services for more information about ESs.

The following options are specific to EVPN-MPLS and are configured in the **config>service>vpls>bgp-evpn>mpls** context:

- **control-word**

Enable or disable the **control-word** command to guarantee interoperability to other vendors. In accordance with RFC 7432, this command is required to avoid frame disordering.

- **auto-bind-tunnel**

  This command is used to select the type of MPLS transport tunnel used for a specific instance. The command is used in the same way as in VPRN services. See auto-bind-tunnel for more information.

  For BGP-EVPN MPLS, **bgp** must be explicitly added to the **resolution-filter** in EVPN (BGP is implicit in VPRNs).

- **force-vlan-vc-forwarding**

  This command allows the system to preserve the VLAN ID and pBits of the service-delimiting qtag in a new tag added in the customer frame before sending the frame to the EVPN core.

  Note:
  Nokia recommends that the user should not configure the **force-vlan-vc-forwarding** command on the 7210 SAS-R6 and 7210 SAS-R12. Instead, Nokia recommends using the **no force-vlan-vc-forwarding** configuration, which is the default setting.

- **split-horizon-group**

  This command associates a user-created split-horizon group to all the EVPN-MPLS destinations. See EVPN and VPLS integration for more information.

- **ingress-replication-bum-label**

  When this command is enabled, it allows the PE to advertise a label for BUM traffic (inclusive multicast routes) that is different from the label advertised for unicast traffic (with the MAC/IP routes). This is useful to avoid potential transient packet duplication in all-active multi-homing.

  Note:
  On the 7210 SAS, because all-active multi-homing is not supported by default, the **ingress-replication-bum-label** command is disabled. The user has the option to enable this command.

In addition to the preceding options, the following **bgp-evpn** commands are also available for EVPN-MPLS services:

- **[no] mac-advertisement**
- **mac-duplication** and settings

When EVPN-MPLS is established among some PEs in the network, EVPN unicast and multicast "bindings" to the remote EVPN destinations are created on each PE. A specified ingress PE creates the following:

- a unicast EVPN-MPLS destination binding to a remote egress PE, as soon as a MAC/IP route is received from that egress PE
- a multicast EVPN-MPLS destination binding to a remote egress PE, only if the egress PE advertises an inclusive multicast Ethernet tag route with a BUM label (only possible if the egress PE is configured with **ingress-replication-bum-label**)

These bindings, as well as the MACs learned on them, can be checked using the **show** commands in the following output example, where the remote PE(192.0.2.69) is configured with **no ingress-replication-bum-label** and PE(192.0.2.70) is configured with **ingress-replication-bum-label**. As a result, the device has a single EVPN-MPLS destination binding to PE(192.0.2.69) and two bindings (unicast and multicast) to PE(192.0.2.70). The following example shows configuration output.

Example: EVPN-MPLS configuration output

```
*A:Dut# show service id 1 evpn-mpls

===============================================================================
BGP EVPN-MPLS Dest
===============================================================================
TEP Address     Egr Label     Num. MACs   Mcast           Last Change
                 Transport
-------------------------------------------------------------------------------
192.0.2.69      262118        1           Yes             06/11/2015 19:59:03
                ldp
192.0.2.70      262139        0           Yes             06/11/2015 19:59:03
                ldp
192.0.2.70      262140        1           No              06/11/2015 19:59:03
                ldp
192.0.2.72      262140        0           Yes             06/11/2015 19:59:03
                ldp
192.0.2.72      262141        1           No              06/11/2015 19:59:03
                ldp
192.0.2.73      262139        0           Yes             06/11/2015 19:59:03
                ldp
192.0.2.254     262142        0           Yes             06/11/2015 19:59:03
                bgp
-------------------------------------------------------------------------------
Number of entries : 7
-------------------------------------------------------------------------------
===============================================================================

*A:Dut# show service id 1 fdb detail

===============================================================================
Forwarding Database, Service 1
===============================================================================
ServId    MAC               Source-Identifier        Type     Last Change
                                                     Age
-------------------------------------------------------------------------------
1         00:ca:fe:ca:fe:69 eMpls:                   EvpnS    06/11/15 21:53:48
                            192.0.2.69:262118
1         00:ca:fe:ca:fe:70 eMpls:                   EvpnS    06/11/15 19:59:57
                            192.0.2.70:262140
1         00:ca:fe:ca:fe:72 eMpls:                   EvpnS    06/11/15 19:59:57
                            192.0.2.72:262141
-------------------------------------------------------------------------------
No. of MAC Entries: 3
-------------------------------------------------------------------------------
Legend:  L=Learned O=Oam P=Protected-MAC C=Conditional S=Static
===============================================================================
```

4.2.2.1 EVPN and VPLS integration

In accordance with *draft-ietf-bess-evpn-vpls-seamless-integ*, the 7210 SAS EVPN implementation supports the integration of EVPN-MPLS and VPLS to the same network within the same service. Because EVPN is not deployed in greenfield deployments, this feature is useful for facilitating the integration between both technologies and for migrating VPLS services to EVPN-MPLS.

The following behavior enables the integration of EVPN and SDP-bindings in the same VPLS network:

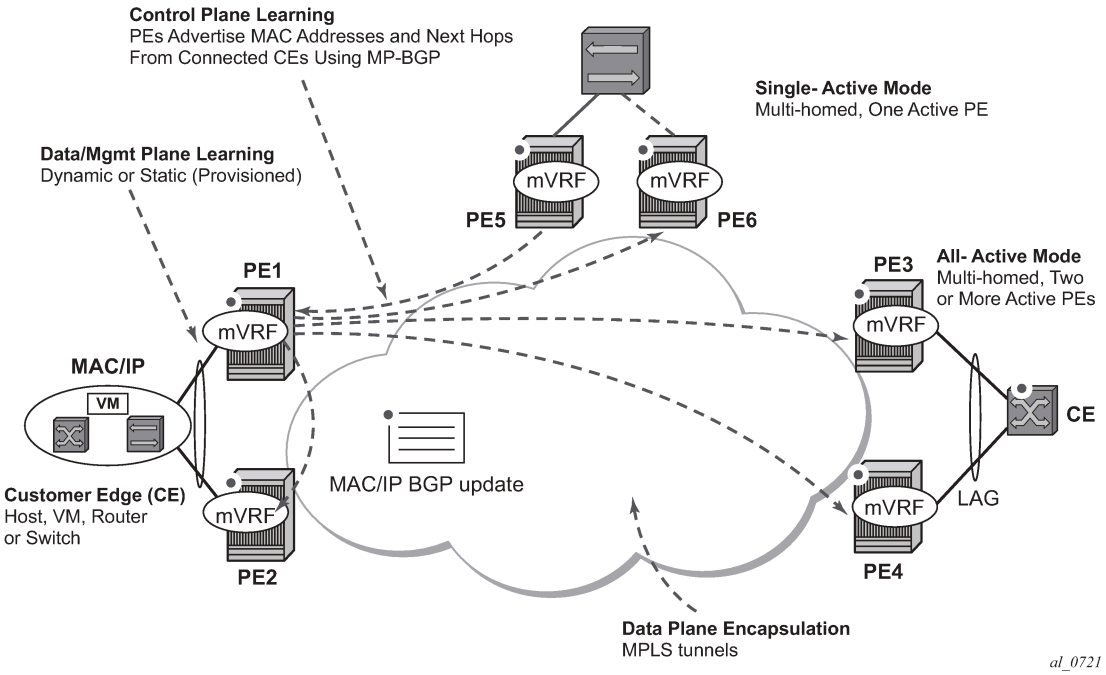
- Systems with EVPN endpoints and SDP-bindings to the same far-end bring down the SDP-bindings.

  - The router allows the establishment of an EVPN endpoint and an SDP-binding to the same far-end, but the SDP-binding is kept operationally down. Only the EVPN endpoint is operationally up. This applies to spoke-SDPs (manual).
  - If an EVPN endpoint to a specified far-end exists and a spoke-SDP establishment is attempted, the spoke-SDP is set up but is kept down with an operational flag, indicating that there is an EVPN route to the same far-end.
  - If an spoke-SDP exists and a valid or used EVPN route arrives, the EVPN endpoint is set up and the spoke-SDP is brought down with an operational flag indicating that there is an EVPN route to the same far-end.
  - In the case of an SDP-binding and EVPN endpoint to different far-end IPs on the same remote PE, both links are up. This may occur if the SDP-binding is terminated in an IPv4 address that is different from the system address where the EVPN endpoint is terminated.

- Users can add spoke-SDPs and all the EVPN-MPLS endpoints in the same split-horizon group (SHG).
  - The following CLI command is added under the **bgp-evpn>mpls** context so that the EVPN-MPLS endpoints can be added to a split-horizon group: **bgp-evpn mpls [no] split-horizon-group** *group-name*.
  - The **bgp-evpn mpls split-horizon-group** command must reference a user-configured split-horizon group. User-configured split-horizon groups can be configured within the service context. The same *group-name* can be associated with SAPs, spoke-SDPs, pw-template-bindings, and EVPN-MPLS endpoints.
  - If the **bgp-evpn mpls split-horizon-group** command is not used, the default split-horizon group (that contains all the EVPN endpoints) is still used but cannot be referred to using SAPs/spoke-SDPs.
  - The 7210 SAS-R6 and 7210 SAS-R12 equipped with an IMM-c card do not support a user-configured SHG. To configure the spoke-SDP and EVPN bindings in the same SHG group, the user can reference the default SHG using spoke-SDPs by configuring the **use-evpn-default-shg** option when the spoke-SDP is created. See VPLS services command reference for more information about the **use-evpn-default-shg** option.
- The system disables the advertisement of MACs learned on spoke-SDPs or SAPs that are part of an EVPN split-horizon group.
  - When the SAPs or spoke-SDPs (manual) are configured within the same split-horizon group as the EVPN endpoints, MAC addresses are still learned on them, but they are not advertised in EVPN.
  - The preceding statement is also true if proxy-ARP/proxy-ND is enabled and an IP-to-MAC pair is learned on a SAP that belongs to the EVPN split-horizon group.
  - The SAPs added to an EVPN split-horizon group should not be part of any EVPN multi-homed ES. If that occurs, the PE still advertises the AD per-EVI route for the SAP, attracting EVPN traffic that could not possibly be forwarded to that SAP.

The following figure shows an example of EVPN-VPLS integration.

Figure 36: EVPN-VPLS integration



The following example shows the configuration for PE1, PE5, and PE2 from the EVPN-VPLS integration example in the preceding figure.

Example: EVPN-VPLS integration configuration for PE1, PE5, and PE2

```
*A:PE1>config>service# info
----------------------------------------------
vpls 1 customer 1 create
  split-horizon-group "SHG-1" create
  bgp
    route-target target:65000:1
  bgp-evpn
    evi 1
    mpls
      no shutdown
  spoke-sdp 12:1 create
  exit
  spoke-sdp 13:1 split-horizon-group "SHG-1" create
  exit
  spoke-sdp 14:1 split-horizon-group "SHG-1" create
  exit
  spoke-sdp 15:1 split-horizon-group "SHG-1" create
  exit
  sap 1/1/1:1 create
  exit

*A:PE5>config>service# info
----------------------------------------------
split-horizon-group "SHG-1" create
vpls 1 customer 1 create
  bgp
    route-target target:65000:1
  spoke-sdp 52:1 create
  exit
```

```
  spoke-sdp 51:1 split-horizon-group "SHG-1" create
  exit
  spoke-sdp 53:1 split-horizon-group "SHG-1" create
  exit
  spoke-sdp 54:1 split-horizon-group "SHG-1" create
  exit

*A:PE2>config>service# info
----------------------------------------------
vpls 1 customer 1 create
  end-point CORE create
    no suppress-standby-signaling
  spoke-sdp 21:1 end-point CORE
    precedence primary
  spoke-sdp 25:1 end-point CORE
```

The following applies to the configuration described in the preceding examples:

- PE1, PE3, and PE4 have BGP-EVPN enabled in VPLS-1. PE2 has active/standby spoke SDPs to PE1 and PE5. In this configuration:
  - PE1, PE3, and PE4 have manual spoke SDPs, but they are kept operationally down as long as there are EVPN endpoints active among them.
  - Manual spoke SDPs on PE1, PE3, and PE4 and EVPN endpoints are instantiated within the same SHG, for example, the default SHG.
  - Manual spoke SDPs from PE1 and PE5 to PE2 are not part of the default SHG.
- For spoke SDPs and EVPN in the same SHG, MACs learned locally on a spoke SDP are not advertised in EVPN
- BUM traffic operation on PE1:
  - When CE1 sends BUM traffic, PE1 floods to all the active bindings.
  - When CE2 sends BUM traffic, PE2 sends it to PE1 (active spoke SDP) and PE1 floods to all the bindings and SAPs.
  - When CE5 sends BUM traffic, PE5 floods to the three EVPN PEs. PE1 floods to the active spoke SDP and SAPs, never to the EVPN PEs because they are part of the same SHG.

4.2.2.2 Auto-derived RD in services with multiple BGP families

A single RD is used per service and not per BGP family or protocol. On the 7210 SAS, BGP-AD is not supported with BGP-EVPN.

Note: On the 7210 SAS, to prevent auto-derived RD in services from using BGP-AD information, Nokia recommends that the user should not configure the **bgp-ad>vpls-id** command.

The following rules apply:

- The VPLS RD is selected based on the following precedence:
  - Manual RD always takes precedence when configured.
  - If no manual-rd configuration exists, the RD is derived from the **bgp-evpn>evi**.
  - If no manual-rd or **bgp-evpn>evi** configuration exists, there is no RD and the service fails.
- The selected RD (see the preceding selection criteria) is displayed by the Oper Route Dist field of the **show service id bgp** command.

- The service supports dynamic RD changes; for example, the manual RD can be updated dynamically, even if it is currently in use as the service RD.

  Note: When the RD changes, the active routes for that VPLS are withdrawn and re-advertised with the new RD.

- If one of the mechanisms to derive the RD for a specified service is removed from the configuration, the system selects a new RD based on the preceding rules. For example, if the manual RD is removed form the configuration, the routes are withdrawn, the new RD is selected from the EVI, and the routes re-advertised with the new RD. See Auto-derived RD in services with multiple BGP families for more information about rules governing the RD selection.

  Note: The reconfiguration fails if the new RD already exists in a different VPLS or Epipe service.

4.2.3 EVPN multi-homing in VPLS services

EVPN multi-homing implementation is based on the concept of the Ethernet Segment (ES). An ES is a logical structure that can be defined in one or more PEs and identifies the CE (or access network) multi-homed to the EVPN PEs. An ES is associated with port or LAG objects and shared by all the services defined on those objects. On the 7210 SAS, only the following service objects are allowed to be configured as an ES: port and LAG.

Each ES has a unique Ethernet Segment Identifier (ESI) that is 10 bytes long and is manually configured in the router.

Note: Because the **esi** command is advertised in the control plane to all the PEs in the EVPN network, it is important to ensure that the 10-byte **esi** value is unique throughout the entire network. Single-homed CEs are assumed to be connected to an ES with esi = 0 (single-homed ESs are not explicitly configured).

4.2.4 EVPN all-active multi-homing

Note:
The 7210 SAS supports only single-active multi-homing. All-active multi-homing (with aliasing) is not supported on any 7210 SAS platform described in this document. References to all-active multi-homing (and aliasing) are only included in this section for completeness of feature description and are not intended to imply support on the 7210 SAS. See the 7210 SAS Software Release Notes 25.*x*.R*x*, part number 3HE 21188 000*x* TQZZA, for information about features supported in each load of the Release 25.*x*.R*x* software.

In accordance with RFC 7432, all-active multi-homing is only supported on access LAG SAPs, and it is mandatory to configure the CE with a LAG to avoid duplicated packets to the network. LACP is optional.

When PE3 installs MAC1 in the Forwarding Database (FDB), it associates MAC1 not only with the advertising PE (PE1), but also with all the PEs advertising the same esi (ESI2) for the service. In this example, PE1 and PE2 advertise an AD per-EVI route for ESI2; therefore, PE3 installs the two next-hops associated with MAC1.

To enable aliasing, configure ECMP greater than 1 in the **bgp-evpn>mpls** context.

4.2.4.1 All-active multi-homing procedures

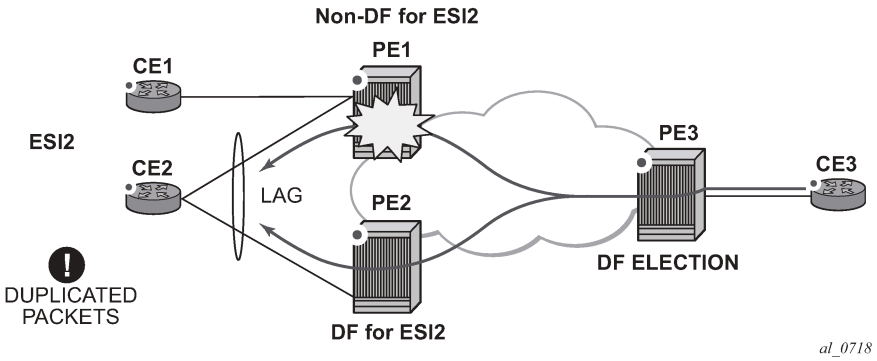
This section describes procedures implemented in SR OS to provide all-active multi-homing for a specified ES.

4.2.4.1.1 Designated Forwarder election

Using Designated Forwarder (DF) election in EVPN all-active multi-homing prevents duplicate packets on the multi-homed CE. The DF election procedure elects one DF PE per ESI per service; the rest of the PEs are non-DF for the ESI and service. Only the DF forwards BUM traffic from the EVPN network toward the ES SAPs (the multi-homed CE). The non-DF PEs do not forward BUM traffic to the local ES SAPs.

The following figure shows the need for DF election in all-active multi-homing.

Figure 37: DF election



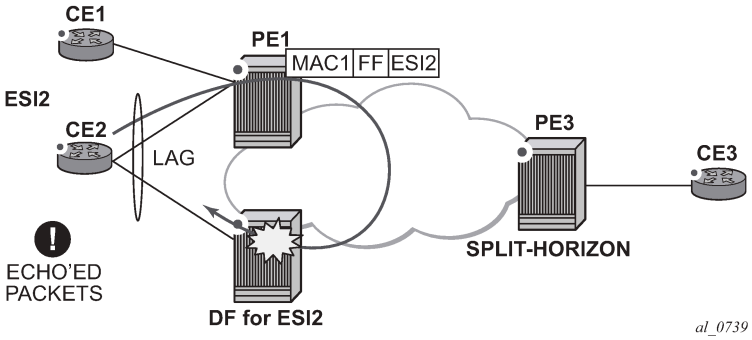
Note: BUM traffic from the CE to the network and known unicast traffic in any direction is allowed on both the DF and non-DF PEs.

4.2.4.1.2 Split-horizon

The EVPN split-horizon procedure ensures that BUM traffic originated by the multi-homed PE and sent from the non-DF to the DF is not replicated back to the CE in the form of echoed packets. To avoid echoed packets, the non-DF (PE1) sends all the BUM packets to the DF (PE2) with an indication of the source ES. That indication is the ESI Label (ESI2 in Figure 38: Split-horizon), previously signaled by PE2 in the AD per-ESI route for the ES. When it receives an EVPN packet (after the EVPN label lookup), PE2 finds the ESI label that identifies its local ES ESI2. The BUM packet is replicated to other local CEs but not to the ESI2 SAP.

The following figure shows the EVPN split-horizon concept for all-active multi-homing.

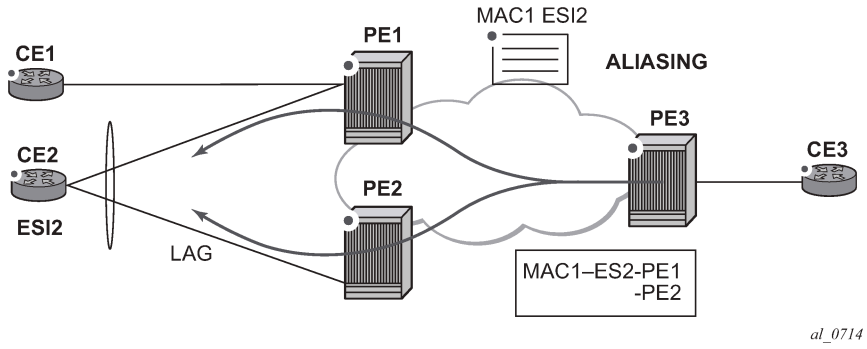
Figure 38: Split-horizon



4.2.4.1.3 Aliasing

The following figure shows the EVPN aliasing procedure for all-active multi-homing. Because CE2 is multi-homed to PE1 and PE2 using an all-active ES, "aliasing" is the procedure by which PE3 can load-balance the known unicast traffic between PE1 and PE2, even if the destination MAC address is only advertised by PE1.

Figure 39: Aliasing



4.2.4.2 All-active multi-homing service model

The following examples show output of the PE1 and PE2 configurations that provides all-active multi-homing to the CE2 shown in Figure 39: Aliasing .

Example: PE1 configuration output

```
*A:PE1>config>lag(1)# info
----------------------------------------------
  mode access
  encap-type dot1q
  port 1/1/2
  lacp active administrative-key 1 system-id 00:00:00:00:00:22
  no shutdown

*A:PE1>config>service>system>bgp-evpn# info
----------------------------------------------
```

```
  route-distinguisher 10.1.1.1:0
  ethernet-segment "ESI2" create
    esi 01:12:12:12:12:12:12:12:12:12
    multi-homing all-active
    service-carving
      mode auto
    lag 1
    no shutdown

*A:PE1>config>redundancy>evpn-multi-homing# info
----------------------------------------------
    boot-timer 120
    es-activation-timer 10

*A:PE1>config>service>vpls# info
----------------------------------------------
  description "evpn-mpls-service with all-active multihoming"
  bgp
  bgp-evpn
    evi 10
    mpls
      no shutdown
      auto-bind-tunnel resolution any
      ingress-replication-bum-label
  sap lag-1:1 create
  exit
```

Example: PE2 configuration output

```
*A:PE1>config>lag(1)# info
----------------------------------------------
  mode access
  encap-type dot1q
  port 1/1/1
  lacp active administrative-key 1 system-id 00:00:00:00:00:22
  no shutdown

*A:PE1>config>service>system>bgp-evpn# info
----------------------------------------------
  route-distinguisher 10.1.1.1:0
  ethernet-segment "ESI12" create
    esi 01:12:12:12:12:12:12:12:12:12
    multi-homing all-active
    service-carving
      mode auto
    lag 1
    no shutdown

*A:PE1>config>redundancy>evpn-multi-homing# info
----------------------------------------------
    boot-timer 120
    es-activation-timer 10

*A:PE1>config>service>vpls# info
----------------------------------------------
  description "evpn-mpls-service with all-active multihoming"
  bgp
    route-distinguisher 65001:60
    route-target target:65000:60
  bgp-evpn
    evi 10
    mpls
      no shutdown
```

```
    auto-bind-tunnel resolution any
sap lag-1:1 create
exit
```

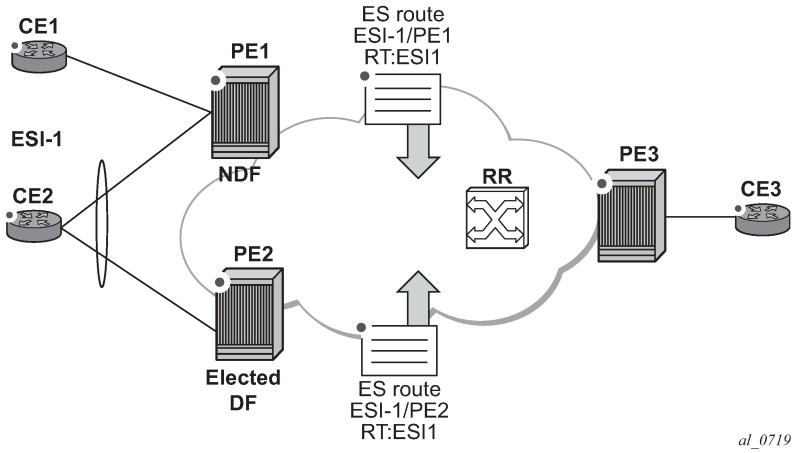
The following considerations apply when the all-active multi-homing procedure is enabled:

- The **ethernet-segment** command must be configured with a name and a 10-byte **esi** using the **config service system bgp-evpn ethernet-segment** *es_name* **create** and **config service system bgp-evpn ethernet-segment esi** *value* commands.
- When configuring the **esi**, the system enforces that the 6 high-order octets after the type are not zero, which ensures that the auto-derived route-target for the ES route is not zero). In addition, the entire ESI value must be unique in the system.
- Only a LAG can be associated with the all-active ES. LAG is used exclusively for EVPN multi-homing. Other LAG ports in the system can continue to be used for MC-LAG and other services.
- When the LAG is configured on PE1 and PE2, the same **admin-key**, **system-priority**, and **system-id** must be configured on both PEs so that CE2 can respond as though it is connected to the same system.
- Only one SAP per service can be part of the same **ethernet-segment**.

4.2.4.3 ES discovery and DF election procedures

The ES discovery and DF election are implemented in three logical steps, as shown in the following figure.

Figure 40: ES discovery and DF election



4.2.4.3.1 Step 1 — ES advertisement and discovery

ES ESI-1 is configured with all the required parameters, as described in All-active multi-homing service model. When **ethernet-segment no shutdown** is executed, PE1 and PE2 advertise an ES route for ESI-1. They both include the route-target auto-derived from the MAC portion of the configured ESI. If the route-target address family is configured in the network, this allows the RR to keep the dissemination of the ES routes under control.

In addition to the ES route, PE1 and PE2 advertise AD per-ESI routes and AD per-EVI routes:

- AD per-ESI routes announces the ES capabilities, including the mode (single-active or all-active) and the ESI label for split horizon.
- AD per-EVI routes are advertised so that PE3 knows what services (EVIs) are associated with the ESI. These routes are used by PE3 for its aliasing and backup procedures.

4.2.4.3.2 Step 2 — DF election

When ES routes exchange between PE1 and PE2 is complete, both run the DF election for all the services in the **ethernet-segment**.

PE1 and PE2 elect a Designated Forwarder (DF) per ESI service. The default DF election mechanism in the SR OS is **service-carving** (as per RFC 7432). The following applies when the mechanism is enabled on a specified PE:

- An ordered list of PE IPs where ESI-1 resides is built. The IPs are derived from the origin IP fields of all the ES routes received for ESI-1, as well as the local system address. The lowest IP is considered ordinal "0" in the list.
- The local IP can only be considered a "candidate" after successful **ethernet-segment no shutdown** for a specified service.

  Note:
  The remote PE IPs must be present in the local PE RTM so that they can participate in the DF election.

- A PE only considers a specified remote IP address as candidate for the DF election algorithm for a specified service if, as well as the ES route, the corresponding AD routes per-ESI and per-EVI for that PE have been received and properly activated.
- All remote PEs that receive the AD per-ES routes (for example, PE3) interpret ESI-1 as all-active if all the PEs send their AD per-ES routes with the single-active bit = 0. Otherwise, if at least one PE sends an AD route per-ESI with the single-active flag set or the local ESI configuration is single-active, the ESI behaves as single-active.
- An **es-activation-timer** can be configured at the **redundancy>bgp-evpn-multi-homing>es-activation-timer** level or at the **service>system>bgp-evpn>eth-seg>es-activation-timer** level. This timer, which is 3 seconds by default, delays the transition from non-DF to DF for a specified service after the DF election has run:
  - This use of the **es-activation-timer** is different from zero and minimizes the risks of loops and packet duplication because of "transient" multiple DFs.
  - The same **es-activation-timer** should be configured in all PEs that are part of the same ESI. It is up to the user to configure either a long timer to minimize the risks of loops/duplication or even **es-activation-timer=0** to speed up the convergence for non-DF to DF transitions. When the user configures a specific value, the value configured at the ES level supersedes the configured global value.
- The DF election is triggered by the following events:
  - The **config service system bgp-evpn eth-seg no shutdown** command triggers the DF election for all the services in the ESI.
  - Reception of a new update or withdrawal of an ES route (containing an ESI configured locally) triggers the DF election for all the services in the ESI.

  - Reception of a new update or withdrawal of an AD per-ES route (containing an ESI configured locally) triggers the DF election for all the services associated with the list of route-targets received along with the route.
  - Reception of a new update of an AD per-ES route with a change in the ESI-label extended community (single-active bit or MPLS label) triggers the DF election for all the services associated with the list of route-targets received along with the route.
  - Reception of a new update or withdrawal of an AD route per-EVI (containing an ESI configured locally) triggers the DF election for that service.
- When the PE boots up, the boot-timer allows the necessary time for the control plane protocols to come up before bringing up the ES and running the DF algorithm. The boot-timer is configured at the system level, using the **config redundancy bgp-evpn-multi-homing boot-timer** command, and should use a value that is long enough to allow the node (with any cards, if available) to boot up and BGP sessions to come up before exchanging ES routes and running the DF election for each EVI/ISID:
  - The system does not advertise ES routes until the boot timer expires. This guarantees that the peer ES PEs do not run the DF election until the PE is ready to become the DF, if it needs to.
  - The **show** command displays the configured boot-timer and the remaining timer, if the system is still in boot-stage.

Example: bgp-evpn-multi-homing show output

```
A:PE1# show redundancy bgp-evpn-multi-homing
===============================================================================
Redundancy BGP EVPN Multi-homing Information
===============================================================================
Boot-Timer              : 10 secs
Boot-Timer Remaining    : 0 secs
ES Activation Timer     : 3 secs
===============================================================================
```

- When **service-carving mode auto** is configured (default mode), the DF election algorithm runs the function [V(evi) mod N(peers) = i(ordinal)] to identify the DF for a specified service and ESI, as follows.

  As shown in Figure 40: ES discovery and DF election, PE1 and PE2 are configured with ESI-1. When V(10) mod N(2) = 0, PE1 is elected DF for VPLS-10 (because its IP address is lower than PE2's and it is the first PE in the candidate list).

  Note: The algorithm uses the configured **evi** in the service and not the *service-id*. The **evi** for a service must match in all PEs that are part of the ESI. This guarantees that the election algorithm is consistent across all PEs of the ESI. The **evi** must be always configured in a service with SAPs that are created in an ES.

- A **service-carving** command is supported to manually configure the EVI identifiers for which the PE is primary: **service-carving mode manual/manual evi** *start-evi* **to** *end-evi*. The following considerations apply:
  - The system is the PE forwarding/multicasting traffic for the **evi** identifiers included in the configuration. The PE is secondary (non-DF) for the non-specified **evi** identifiers.
  - If a range is configured but **service-carving** is not **mode manual**, the range has no effect.
  - Only two PEs are supported when **service-carving mode manual** is configured. If manual mode is configured for a third PE for an ESI, the two non-primary PEs remain non-DF regardless of the primary status.

  - For example, as shown in Figure 40: ES discovery and DF election: if PE1 is configured with **service-carving manual evi** 1 to 100 and PE2 with **service-carving manual evi** 101 to 200, PE1 is the primary PE for service VPLS 10 and PE2 the secondary PE.

- If **service-carving** is disabled, the lowest originator IP wins the election for a specified service and ESI. Use the **config service system bgp-evpn eth-seg service-carving mode off** command to disable service-carving.

Example: Ethernet segment configuration and DF status

The following example shows the **ethernet-segment** configuration and DF status for all EVIs configured in the **ethernet-segment**.

```
*A:Dut-B# /show service system bgp-evpn ethernet-segment name "eslag1" all
===============================================================================
Service Ethernet Segment
===============================================================================
Name                    : eslag1
Admin State             : Enabled            Oper State         : Up
ESI                     : 00:bc:01:00:00:00:00:00:00:01
Multi-homing            : allActive          Oper Multi-homing  : allActive
Lag Id                  : 1
ES Activation Timer     : 3 secs (default)
Exp/Imp Route-Target    : target:bc:01:00:00:00:00
Svc Carving             : auto
ES SHG Label            : 131070
===============================================================================
===============================================================================
EVI Information
===============================================================================
EVI                 SvcId               Actv Timer Rem      DF
-------------------------------------------------------------------------------
1                   1                   0                   no
-------------------------------------------------------------------------------
Number of entries: 1
===============================================================================
-------------------------------------------------------------------------------
DF Candidate list
-------------------------------------------------------------------------------
EVI                                     DF Address
-------------------------------------------------------------------------------
1                                       10.20.1.2
1                                       10.20.1.3
-------------------------------------------------------------------------------
Number of entries: 2
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
```

4.2.4.3.3 Step 3 — DF and non-DF service behavior

Based on the result of the DF election or the manual service-carving, the control plane on the non-DF (PE1) instructs the datapath to remove the LAG SAP (associated with the ESI) from the default flooding list for BM traffic (unknown unicast traffic may still be sent if the EVI label is a unicast label and the source MAC address is not associated with the ESI). On PE1 and PE2, both LAG SAPs learn the same MAC address (coming from the CE).

For example, in the following sample configuration output, 00:ca:ca:ba:ce:03 is learned on both PE1 and PE2 access LAG (on ESI-1). However, PE1 learns the MAC as "Learned" whereas PE2 learns it as "Evpn".

This is because CE2 hashes the traffic for that source MAC to PE1. And PE2 learns the MAC through EVPN but associates the MAC to the ESI SAP, because the MAC belongs to the ESI.

Example: PE1 and PE2 learning 00:ca:ca:ba:ce:03

```
*A:PE1# show service id 1 fdb detail
===============================================================================
Forwarding Database, Service 1
===============================================================================
ServId    MAC               Source-Identifier        Type     Last Change
                                                     Age
-------------------------------------------------------------------------------
1         00:ca:ca:ba:ce:03 sap:lag-1:1              L/0      06/11/15 00:14:47
1         00:ca:fe:ca:fe:70 eMpls:                   EvpnS    06/11/15 00:09:06
                            192.0.2.70:262140
1         00:ca:fe:ca:fe:72 eMpls:                   EvpnS    06/11/15 00:09:39
                            192.0.2.72:262141
-------------------------------------------------------------------------------
No. of MAC Entries: 3
-------------------------------------------------------------------------------
Legend:  L=Learned O=Oam P=Protected-MAC C=Conditional S=Static
===============================================================================

*A:PE2# show service id 1 fdb detail
===============================================================================
Forwarding Database, Service 1
===============================================================================
ServId    MAC               Source-Identifier        Type     Last Change
                                                     Age
-------------------------------------------------------------------------------
1         00:ca:ca:ba:ce:03 sap:lag-1:1              Evpn     06/11/15 00:14:47
1         00:ca:fe:ca:fe:69 eMpls:                   EvpnS    06/11/15 00:09:40
                            192.0.2.69:262141
1         00:ca:fe:ca:fe:70 eMpls:                   EvpnS    06/11/15 00:09:40
                            192.0.2.70:262140
-------------------------------------------------------------------------------
No. of MAC Entries: 3
-------------------------------------------------------------------------------
Legend:  L=Learned O=Oam P=Protected-MAC C=Conditional S=Static
===============================================================================
```

When PE1 (non-DF) and PE2 (DF) exchange BUM packets for **evi** 1, the packets are sent including the ESI label at the bottom of the stack (in both directions). The ESI label advertised by each PE for ESI-1 can be displayed using the following command.

Example: Displaying ESI label advertisement

```
*A:PE1# show service system bgp-evpn ethernet-segment name "ESI-1"
===============================================================================
Service Ethernet Segment
===============================================================================
Name                    : ESI-1
Admin State             : Up                 Oper State         : Up
ESI                     : 01:00:00:00:00:71:00:00:00:01
Multi-homing            : allActive          Oper Multi-homing  : allActive
Lag Id                  : 1
ES Activation Timer     : 0 secs
Exp/Imp Route-Target    : target:00:00:00:00:71:00

Svc Carving             : auto
ES SHG Label            : 262142
===============================================================================
```

```
*A:PE2# show service system bgp-evpn ethernet-segment name "ESI-1"

===============================================================================
Service Ethernet Segment
===============================================================================
Name                    : ESI-1
Admin State             : Up                 Oper State         : Up
ESI                     : 01:00:00:00:00:71:00:00:00:01
Multi-homing            : allActive          Oper Multi-homing  : allActive
Lag Id                  : 1
ES Activation Timer     : 20 secs
Exp/Imp Route-Target    : target:00:00:00:00:71:00

Svc Carving             : auto
ES SHG Label            : 262142
===============================================================================
```

4.2.4.4 Aliasing

As shown in the example in Figure 40: ES discovery and DF election, if the service configuration on PE3 has ECMP > 1, PE3 adds PE1 and PE2 to the list of next-hops for ESI-1. As soon as PE3 receives a MAC for ESI-1, it starts load-balancing between PE1 and PE2 the flows to the remote ESI CE.

Example: Configuration output for the FDB in PE3

The following example shows configuration output for the FDB in PE3.

Note: MAC 00:ca:ca:ba:ce:03 is associated with the **ethernet-segment** eES:01:00:00:00:00:71:00:00:00:01 (esi configured on PE1 and PE2 for ESI-1).

```
*A:PE3# show service id 1 fdb detail
===============================================================================
Forwarding Database, Service 1
===============================================================================
ServId    MAC               Source-Identifier        Type     Last Change
                                                     Age
-------------------------------------------------------------------------------
1         00:ca:ca:ba:ce:03 eES:                     Evpn     06/11/15 00:14:47
                            01:00:00:00:00:71:00:00:00:01
1         00:ca:fe:ca:fe:69 eMpls:                   EvpnS    06/11/15 00:09:18
                            192.0.2.69:262141
1         00:ca:fe:ca:fe:70 eMpls:                   EvpnS    06/11/15 00:09:18
                            192.0.2.70:262140
1         00:ca:fe:ca:fe:72 eMpls:                   EvpnS    06/11/15 00:09:39
                            192.0.2.72:262141
-------------------------------------------------------------------------------
No. of MAC Entries: 4
-------------------------------------------------------------------------------
Legend:  L=Learned O=Oam P=Protected-MAC C=Conditional S=Static
===============================================================================
```

Example: Configuration output for all EVPN-MPLS destination bindings on PE3

The following example shows configuration output for all the EVPN-MPLS destination bindings on PE3, including the ES destination bindings.

Note: The **ethernet-segment** eES:01:00:00:00:00:71:00:00:00:01 is resolved to PE1 and PE2 addresses.

```
*A:Dut-B# /show service id 1 evpn-mpls
===============================================================================
BGP EVPN-MPLS Dest
===============================================================================
TEP Address     Egr Label     Num. MACs   Mcast           Last Change
                 Transport
-------------------------------------------------------------------------------
10.20.1.3       131069        0           Yes             02/02/2014 15:29:40
                rsvp
10.20.1.4       131069        0           Yes             02/02/2014 15:29:33
                rsvp
10.20.1.5       131059        0           Yes             02/02/2014 15:29:42
                rsvp
-------------------------------------------------------------------------------
Number of entries : 3
-------------------------------------------------------------------------------
===============================================================================
===============================================================================
BGP EVPN-MPLS Ethernet Segment Dest
===============================================================================
Eth SegId                       Num. Macs               Last Change
-------------------------------------------------------------------------------
00:de:01:00:00:00:00:00:00:01   1                       02/02/2014 15:47:04
-------------------------------------------------------------------------------
Number of entries: 1
-------------------------------------------------------------------------------
```

Example: PE3 configuration

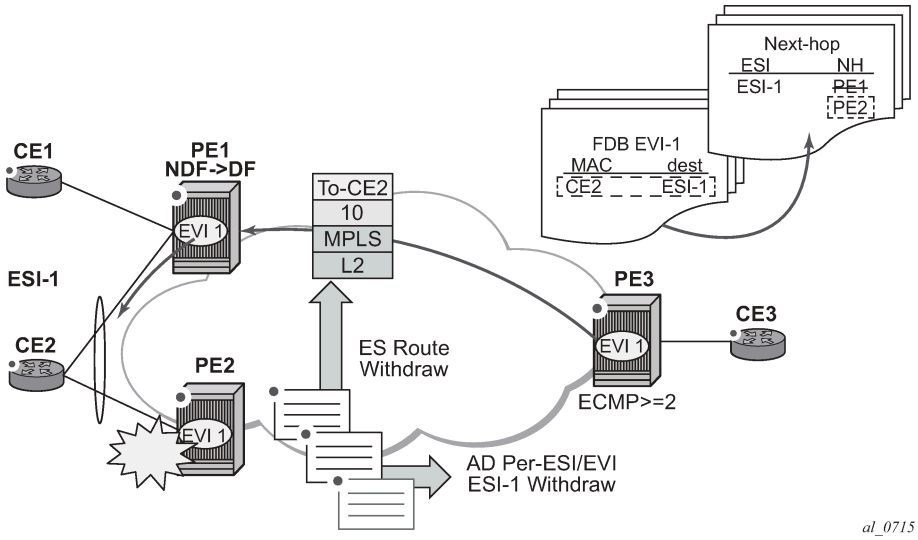
PE3 performs aliasing for all the MACs associated with that ESI. This is possible because PE1 is configured with ECMP parameter >1. The following example shows configuration output.

```
*A:PE3>config>service>vpls# info
----------------------------------------------
            bgp
            exit
            bgp-evpn
                evi 1
                mpls
                    ecmp 4
                    auto-bind-tunnel
                        resolution any
                    exit
                    no shutdown
                exit
            exit
            proxy-arp
                shutdown
            exit
            stp
                shutdown
            exit
            sap 1/1/1:2 create
            exit
            no shutdown
```

4.2.4.5 Network failures and convergence for all-active multi-homing

The following figure shows the behavior on the remote PEs (PE3) when there is an **ethernet-segment** failure.

Figure 41: All-active multi-homing ES failure



The following steps describe the unicast traffic behavior on PE3:

1. PE3 can only forward MAC DA = CE2 to both PE1 and PE2 when the MAC advertisement route from PE1 (or PE2) and the set of Ethernet AD per-ES routes and Ethernet AD per-EVI routes from PE1 and PE2 are active at PE3.
2. In case of a failure between CE2 and PE2, PE2 withdraws its set of Ethernet AD routes and ES route, and PE3 forwards traffic destined for CE2 to PE1 only. PE3 does not need to wait for the withdrawal of the individual MAC.
3. The same handling is used if the failure was at PE1.
4. If after step2, PE2 withdraws its MAC advertisement route, PE3 treats traffic to MAC DA = CE2 as unknown unicast, unless PE1 has previously advertised the MAC.

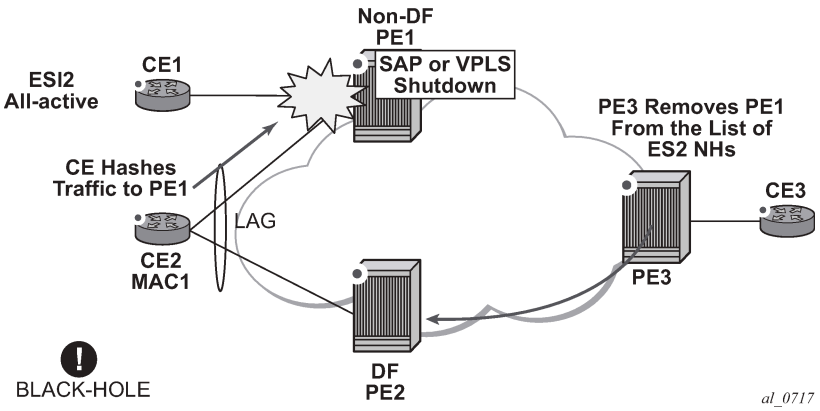
For BUM traffic, the following events trigger a DF election on a PE, and only the DF forwards BUM traffic after the **esi-activation-timer** expires (if there was a transition from non-DF to DF):

- reception of ES route update (local ES **shutdown**/**no shutdown** or remote route)
- new AD-ES route update/withdraw
- new AD-EVI route update/withdraw
- local ES port/SAP/service shutdown
- service carving range change (affecting the EVI)
- multi-homing mode change (single/all active to all/single-active)

4.2.4.6 Logical failures on ESs and black holes

Specific "failure scenarios" in the network can trigger effects. The following figure shows some of these scenarios.

Figure 42: Black hole caused by SAP/SVC shutdown



If an individual VPLS service is **shutdown** in PE1 (the example is also valid for PE2), the corresponding LAG SAP goes operationally down. This event triggers the withdrawal of the AD per-EVI route for that SAP. PE3 removes PE1 from its list of aliased next-hops, and PE2 takes over as DF (if it was not the DF already). However, this does not prevent the network from black-holing the traffic that CE2 "hashes" to the link to PE1. Because traffic sent from CE2 to PE2 or traffic from the rest of the CEs to CE2 is unaffected, the situation is not easily detected on the CE.

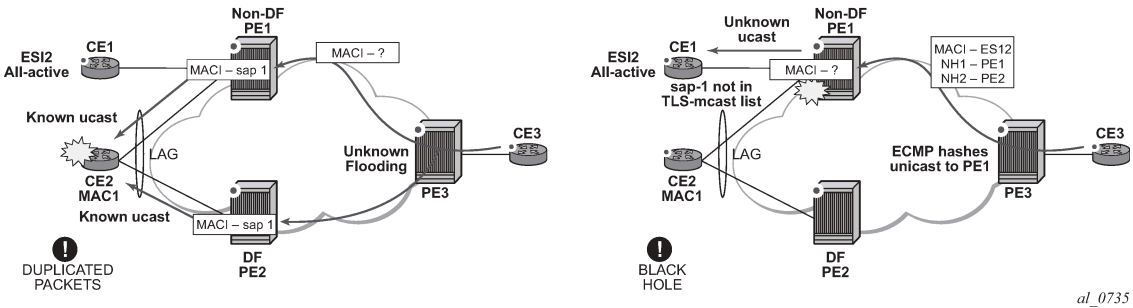
The same result occurs if the ES SAP is administratively **shutdown** instead of the service.

Note:
When the **bgp-evpn mpls shutdown** command is executed, the SAP associated with the ES goes operationally down (**StandbyforMHprotocol**). If no other SAPs or SDP-bindings are configured in the service, the service also goes operationally down. However, if other SAPs or SDP-bindings are present, the service remains operationally up.

4.2.4.7 Transient issues because of MAC route delays

The following figure shows scenarios that may cause potential transient issues in the network.

Figure 43: Transient issues caused by "slow" MAC learning



In the preceding figure, the scenario on the left shows an example of transient packet duplication caused by delay in PE3 to learn MAC1.

In an all-active multi-homing scenario, if a specified MAC address (for example, MAC1), is not yet learned in a remote PE (for example, PE3), but it is known in the two PEs of the ES (for example, PE1 and PE2), the latter PEs may send duplicated packets to the CE.

Configuring **ingress-replication-bum-label** in PE1 and PE2 resolves the issue. PE1 and PE2 know that the received packet is an unknown unicast packet; consequently, the NDF (PE1) does not send the packets to the CE, which prevents transient and duplication.

In Figure 43: Transient issues caused by "slow" MAC learning, the scenario on the right shows an example of transient black hole caused by delay in PE1 to learn MAC1.

In an all-active multi-homing scenario, MAC1 is known in PE3 and aliasing is applied to MAC1. However, MAC1 is not yet known in PE1, which is the NDF for the ES. If PE3 hashing picks up PE1 as the destination of the aliased MAC1, the packets are blackholed. To resolve this issue, unknown unicast traffic that arrives with a unicast label should not be blocked on the NDF. If PE1 and PE2 are configured using **ingress-replication-bum-label**, PE3 sends unknown unicast packets with a BUM label and known unicast with a unicast label. In the latter case, PE1 considers it safe to forward the frame to the CE, even if it is unknown unicast.

Note: This is a transient issue that is resolved as soon as MAC1 is learned in PE1 and the frames are forwarded as known unicast.

4.2.5 EVPN single-active multi-homing

The 7210 SAS SR OS supports only single-active multi-homing on access LAG SAPs and regular SAPs for a specified VPLS service. For LAG SAPs, the CE is configured with a different LAG to each PE in the ES (in contrast to a single LAG in an all-active multi-homing).

The following SR OS procedures support EVPN single-active multi-homing for a specified ES:

- **DF election**

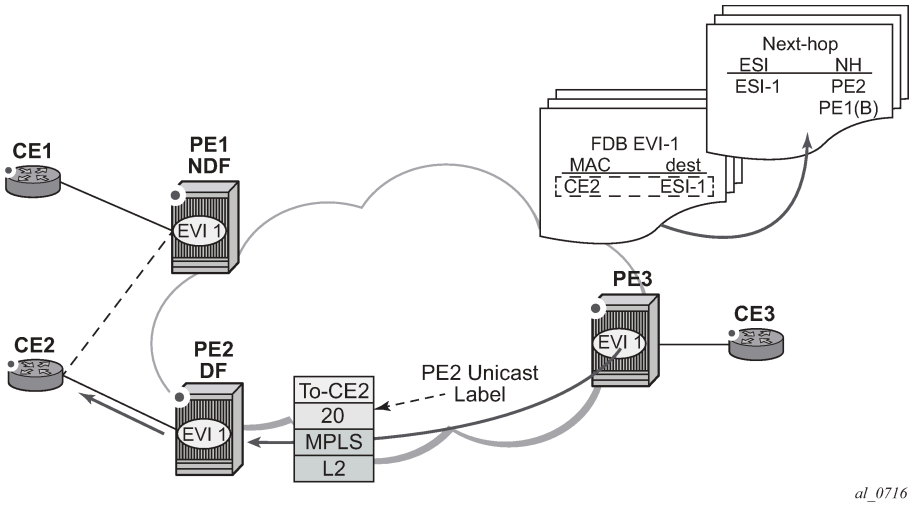
  The DF election in single-active multi-homing determines the forwarding for BUM traffic from the EVPN network to the ES CE. DF election also determines the forwarding of any traffic (unicast or BUM) in any direction (to or from the CE).

- **backup PE**

  In single-active multi-homing, the remote PEs do not perform aliasing to the PEs in the ES. The remote PEs identify the DF based on the MAC routes and send the unicast flows for the ES to the PE in the DF. The remote PEs also program a backup PE as an alternative next-hop for the remote ESI in case of failure. This is in accordance with the Backup PE procedure, defined in RFC 7432.

  The following figure shows an example backup PE for PE3.

Figure 44: Backup PE



4.2.5.1 Single-active multi-homing service model

The following example shows a PE1 configuration that provides single-active multi-homing to CE2, as shown in Figure 44: Backup PE.

Example: PE1 configuration

```
*A:PE1>config>service>system>bgp-evpn# info
----------------------------------------------
  route-distinguisher 10.1.1.1:0
  ethernet-segment "ESI2" create
    esi 01:12:12:12:12:12:12:12:12:12
    multi-homing single-active no-esi-label
    service-carving
      mode auto
    lag 1
    no shutdown

*A:PE1>config>redundancy>evpn-multi-homing# info
----------------------------------------------
    boot-timer 120
    es-activation-timer 10

*A:PE1>config>service>vpls# info
----------------------------------------------
  description "evpn-mpls-service with single-active multihoming"
  bgp
  bgp-evpn
    evi 10
    mpls
      no shutdown
      auto-bind-tunnel resolution any
  lag 1:1 create
  exit
```

The PE2 example configuration for this scenario is as follows.

Example: PE2 configuration

```
*A:PE1>config>service>system>bgp-evpn# info
----------------------------------------------
  route-distinguisher 10.1.1.1:0
  ethernet-segment "ESI2" create
    esi 01:12:12:12:12:12:12:12:12:12
    multi-homing single-active no-esi-label
    service-carving
    lag 2
    no shutdown

*A:PE1>config>redundancy>evpn-multi-homing# info
----------------------------------------------
    boot-timer 120
    es-activation-timer 10

*A:PE1>config>service>vpls# info
----------------------------------------------
  description "evpn-mpls-service with single-active multihoming"
  bgp
  bgp-evpn
    evi 10
    mpls
      no shutdown
      auto-bind-tunnel resolution any
  lag 2:1 create
  exit
```

In single-active multi-homing, the non-DF PEs for a specified ESI block unicast and BUM traffic in both directions (upstream and downstream) on the object associated with the ESI. Otherwise, single-active multi-homing is similar to all-active multi-homing with the following differences:

- The **ethernet-segment** is configured for single-active: **service>system>bgp-evpn>eth-seg>multi-homing single-active**.
- The advertisement of the ESI-label in an AD per-ESI is optional in standards for **single-active** ESs. Use the **service system bgp-evpn eth-seg multi-homing single-active no-esi-label** command to control the ESI label advertisement. By default on the 7210 SAS, the ESI label is not used for single-active ESs, and there is no option available to enable the use of the ESI label.

  Note:
  The 7210 SAS ignores the ESI label received from an EVPN peer, which means that BUM traffic sent by the 7210 SAS to a peer DF node is always sent without the ESI label advertised by the DF.

- For single-active multi-homing, the ES can be associated with a **port** or *lag-id*, as shown in Figure 44: Backup PE, where:
  - **port** is used for single-active SAP redundancy without the need for LAG
  - **lag** is used for single-active LAG redundancy

  Note:
  For a LAG configured with single-active homing, the LAG parameters **key**, *system-id*, and **system-priority** must be different on the PEs that are part of the ES.

- For single-active multi-homing, when the PE is non-DF for the service, the SAPs on the **ethernet-segment** are down and show **StandByForMHProtocol** as the reason.

- From a service perspective, single-active multi-homing can provide redundancy to CEs (MHD, Multi-Homed Devices) with the following setup:
  - **LAG with or without LACP**

    In this case, the multi-homed ports on the CE are part of the different LAGs (a LAG per multi-homed PE is used in the CE).
  - **regular Ethernet 802.1q/ad ports**

    In this case, the multi-homed ports on the CE/network are not part of any LAG.

4.2.5.2 ES and DF election procedures

In all-active multi-homing, the non-DF keeps the SAP up, although it removes it from the default flooding list. In the single-active multi-homing implementation, the non-DF brings the SAP operationally down. For more information, see ES discovery and DF election procedures.

The following **show** command output is an example status of the single-active ESI-7413 in the non-DF.

Example: Single-active ESI-7413 status

```
*A:Dut-B# show service system bgp-evpn ethernet-segment name "eslag1"
===============================================================================
Service Ethernet Segment
===============================================================================
Name                    : eslag1
Admin State             : Enabled            Oper State         : Up
ESI                     : 00:bc:01:00:00:00:00:00:00:01
Multi-homing            : singleActiveNoEsi* Oper Multi-homing  : singleActive*
Lag Id                  : 1
ES Activation Timer     : 3 secs (default)
Exp/Imp Route-Target    : target:bc:01:00:00:00:00
Svc Carving             : auto
ES SHG Label            : N/A
===============================================================================
* indicates that the corresponding row element may have been truncated.
===============================================================================
*A:Dut-D# /show service system bgp-evpn ethernet-segment name "eslag1" evi 1
===============================================================================
EVI DF and Candidate List
===============================================================================
EVI           SvcId         Actv Timer Rem      DF  DF Last Change
-------------------------------------------------------------------------------
1             1             0                   no  03/13/2000 11:43:16
===============================================================================
===============================================================================
DF Candidates                           Time Added
-------------------------------------------------------------------------------
10.20.1.4                               03/13/2000 12:00:30
10.20.1.5                               03/13/2000 11:43:16
-------------------------------------------------------------------------------
Number of entries: 2
===============================================================================
*A:Dut-D#
```

4.2.5.3 Backup PE function

In the example in Figure 44: Backup PE, the remote PE3 imports AD routes per ESI where the single-active flag is set. PE3 interprets the **ethernet-segment** as single-active if at least one PE sends an AD route per-ESI with the single-active flag set. MACs for a specified service and ESI are learned from a single PE, that is, the DF for that <ESI, EVI>.

The remote PE installs a single EVPN-MPLS destination (TEP, label) for a received MAC address and a backup next-hop to the PE for which the AD routes per-ESI and per-EVI are received. For example, in the following **show** command sample output, 00:ca:ca:ba:ca:06 is associated with the remote **ethernet-segment** eES 01:74:13:00:74:13:00:00:74:13. This ES is resolved to PE(192.0.2.73), which is the DF on the ES.

Example: Remote Ethernet segment association

```
*A:PE3# show service id 1 fdb detail
===============================================================================
Forwarding Database, Service 1
===============================================================================
ServId    MAC               Source-Identifier        Type     Last Change
                                                     Age
-------------------------------------------------------------------------------
1         00:ca:ca:ba:ca:02 sap:1/1/1:2              L/0      06/12/15 00:33:39
1         00:ca:ca:ba:ca:06 eES:                     Evpn     06/12/15 00:33:39
                            01:74:13:00:74:13:00:00:74:13
1         00:ca:fe:ca:fe:69 eMpls:                   EvpnS    06/11/15 21:53:47
                            192.0.2.69:262118
1         00:ca:fe:ca:fe:70 eMpls:                   EvpnS    06/11/15 19:59:57
                            192.0.2.70:262140
1         00:ca:fe:ca:fe:72 eMpls:                   EvpnS    06/11/15 19:59:57
                            192.0.2.72:262141
-------------------------------------------------------------------------------
No. of MAC Entries: 5
-------------------------------------------------------------------------------
Legend:  L=Learned O=Oam P=Protected-MAC C=Conditional S=Static
===============================================================================
*A:Dut-D# /show service id 1 evpn-mpls
===============================================================================
BGP EVPN-MPLS Dest
===============================================================================
TEP Address     Egr Label     Num. MACs   Mcast           Last Change
                 Transport
-------------------------------------------------------------------------------
10.20.1.2       131061        0           Yes             03/13/2000 11:26:29
                rsvp
10.20.1.2       131062        1           No              03/13/2000 12:10:04
                rsvp
10.20.1.5       131061        0           Yes             03/13/2000 11:18:23
                rsvp
-------------------------------------------------------------------------------
Number of entries : 3
-------------------------------------------------------------------------------
===============================================================================
===============================================================================
BGP EVPN-MPLS Ethernet Segment Dest
===============================================================================
Eth SegId                       Num. Macs               Last Change
-------------------------------------------------------------------------------
00:de:01:00:00:00:00:00:00:01   453                     03/13/2000 12:10:14
-------------------------------------------------------------------------------
Number of entries: 1
```

```
-------------------------------------------------------------------------------
===============================================================================
*A:Dut-D# /show service id 1 evpn-mpls esi 00:de:01:00:00:00:00:00:00:01
===============================================================================
BGP EVPN-MPLS Ethernet Segment Dest
===============================================================================
Eth SegId                       Num. Macs               Last Change
-------------------------------------------------------------------------------
00:de:01:00:00:00:00:00:00:01   453                     03/13/2000 12:10:14
===============================================================================
===============================================================================
BGP EVPN-MPLS Dest TEP Info
===============================================================================
TEP Address             Egr Label               Last Change
                        Transport
-------------------------------------------------------------------------------
```

If PE3 sees only two single-active PEs in the same ESI, the second PE is the backup PE. Upon receiving an AD per-ES/per-EVI route withdrawal for the ESI from the primary PE, PE3 starts sending the unicast traffic to the backup PE immediately.

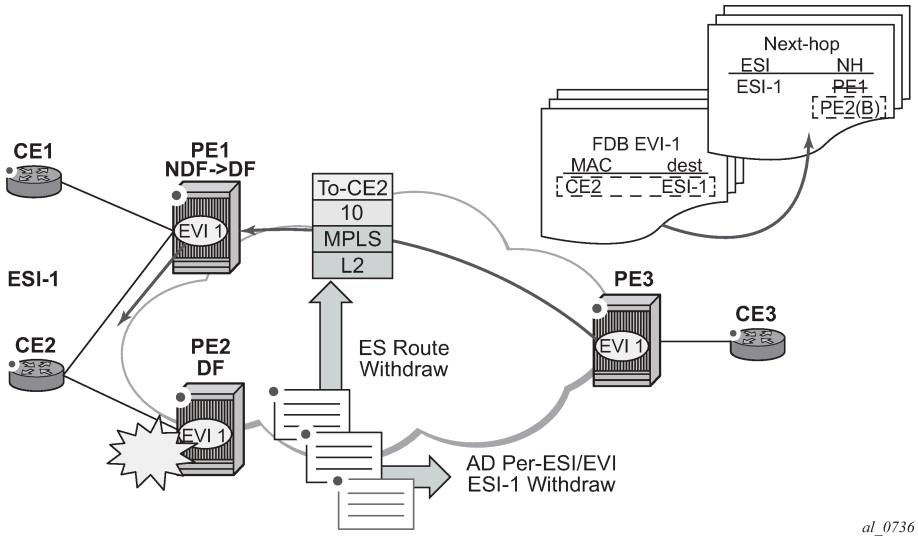
If PE3 receives AD routes for the same ESI and EVI from more than two PEs, the PE does not install any backup route in the datapath. Upon receiving an AD per-ES/per-EVI route withdrawal for the ESI, it flushes the MACs associated with the ESI.

Note: On the 7210 SAS, an ES can be multi-homed to up to two PEs.

4.2.5.4 Network failures and convergence for single-active multi-homing

The following figure shows an example of remote PE (PE3) behavior when there is an **ethernet-segment** failure.

Figure 45: Single-active multi-homing ES failure



The following steps list the behavior of the remote PE3 for unicast traffic:

1. PE3 forwards MAC DA = CE2 to PE2 when the MAC advertisement route came from PE2 and the set of Ethernet AD per-ES routes and Ethernet AD per-EVI routes from PE1 and PE2 are active at PE3.
2. If there is a failure between CE2 and PE2, PE2 withdraws its set of Ethernet AD and ES routes. PE3 does not need to wait for the withdrawal of the individual MAC, and immediately forwards the traffic destined for CE2 to PE1 (the backup PE) only.
3. After the (2) PE2 withdraws its MAC advertisement route, PE3 treats traffic to MAC DA = CE2 as unknown unicast, unless the MAC has been previously advertised by PE1.

A DF election on PE1 is also triggered. A DF election is triggered by the same events as all-active multi-homing. In this case, the DF forwards traffic to CE2 when the **esi-activation-timer** expires; the timer is triggered when a transition from non-DF to DF occurs.

4.3 General EVPN topics

This section provides information about general topics related to EVPN.

Note: Hash labels (that is, the Flow Aware Transport label (RFC 6391)) are not supported with 7210 SAS EVPN VPLS services.

4.3.1 ARP and ND snooping and proxy support

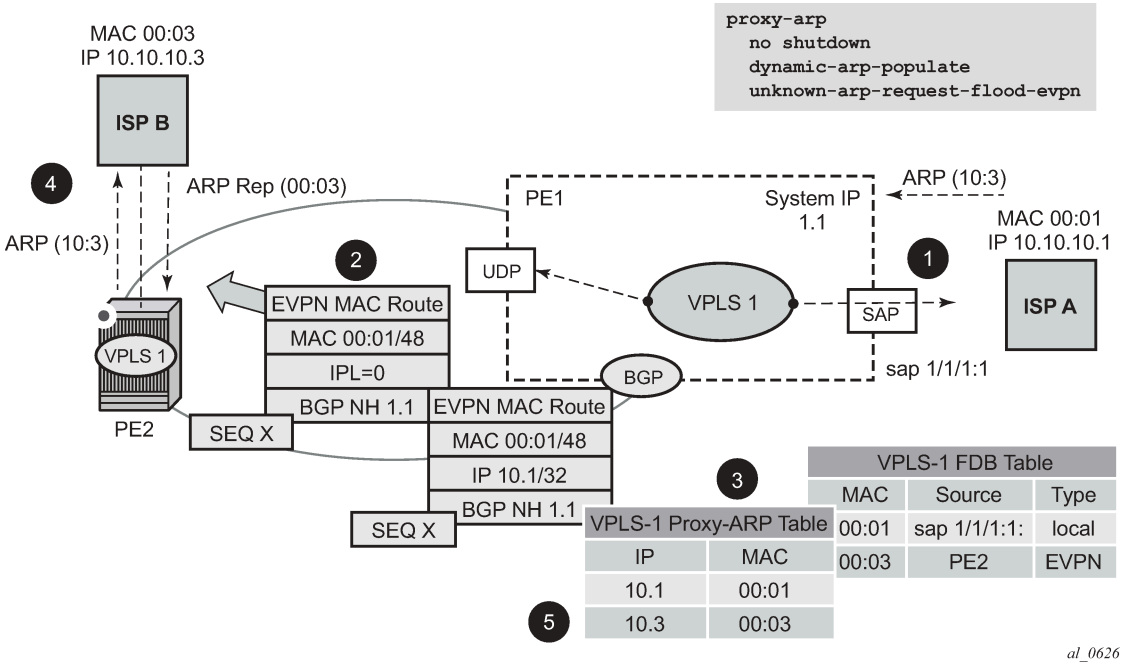
VPLS services support proxy-Address Resolution Protocol (proxy-ARP) and proxy-Neighbor Discovery (proxy-ND) functions cannot be enabled or disabled per service. When enabled, the **config>service>system>evpn-proxy-arp-nd** command populates the corresponding proxy-ARP or proxy-ND table with IP-to-MAC entries learned from the following sources:

- EVPN-received IP-to-MAC entries
- user-configured static IP-to-MAC entries
- snooped dynamic IP-to-MAC entries (learned from ARP, GARP, or NA messages received on local SAPs; snooped dynamic IP-to-MAC entries on spoke-SDP bindings are not supported)

In addition, any ingress ARP or ND frame on a SAP are intercepted and processed. The system answers ARP requests and Neighbor Solicitation messages if the requested IP address is present in the proxy table.

The following figure shows an example proxy-ARP usage in an EVPN network. Proxy-ND functions in a similar way. The MAC address notation in the diagram is shortened for readability.

Figure 46: Proxy-ARP example usage in an EVPN network



In the preceding figure, PE1 is configured as follows:

Example: PE1 configuration

```
*A:Dut-B>config>service>system# info
----------------------------------------------
 evpn-proxy-arp-nd
----------------------------------------------
*A:Dut-B>config>service>vpls# info
----------------------------------------------
           description "Vpls 1 "
           service-mtu 1400
           split-horizon-group "vpls1" create
               description "Default description for SHG vpls1"
           exit
           bgp
               route-distinguisher auto-rd
               route-target export target:100:1 import target:100:1
               pw-template-binding 100
               exit
           exit
           bgp-evpn
               evi 1
               mpls
                   split-horizon-group "vpls1"
                   ingress-replication-bum-label
                   auto-bind-tunnel
                       resolution-filter
                           ldp
                       exit
                       resolution filter
                   exit
                   no shutdown
               exit
```

```
            exit
            stp
                shutdown
            exit
            sap lag-1:1 create
                description "Default sap description for service id 1"
                no shutdown
            exit
            proxy-arp
                age-time 600
                send-refresh 200
                dup-detect window 3 num-moves 3 hold-down max anti-spoof-
mac 00:aa:aa:aa:aa:aa
                dynamic-arp-populate
                no shutdown
            exit
            no shutdown
----------------------------------------------
*A:Dut-B>config>service>vpls#
```

Figure 46: Proxy-ARP example usage in an EVPN network shows the following steps, assuming proxy-ARP is **no shutdown** on PE1 and PE2, and the tables are empty:

1. ISP-A sends ARP-request for 10.10.10.3.
2. PE1 learns the MAC 00:01 in the FDB as usual and advertises it in EVPN without any IP. Optionally if the MAC is configured as a Cstatic MAC, it is advertised as a protected MAC to other PEs with the sticky bit set.
3. The ARP-request is sent to the CPM, where it is handled as follows.
   - An ARP entry (IP 10.1'MAC 00:01) is populated into the proxy-ARP table.
   - EVPN advertises MAC 00:01 and IP 10.1 in EVPN with the same SEQ number and protected bit as the previous route-type 2 for MAC 00:01.
   - A GARP is also issued to other SAPs/SDP-bindings (assuming they are not in the same split-horizon group as the source). If the **garp-flood-evpn** command is enabled, the GARP message is also sent to the EVPN network.
   - The original ARP-request can still be flooded to the EVPN or not based on the **unknown-arp-request-flood-evpn** command.
4. Assuming PE1 was configured with **unknown-arp-request-flood-evpn**, the ARP-request is flooded to PE2 and delivered to ISP-B. ISP-B replies with its MAC in the ARP-reply. The ARP-reply is finally delivered to ISP-A.
5. PE2 learns MAC 00:01 in the FDB and the entry 10.1'00:01 in the proxy-ARP table, based on the EVPN advertisements.
6. When ISP-B replies with its MAC in the ARP-reply, the MAC is handled as follows:
   - MAC 00:03 is learned in FDB at PE2 and advertised in EVPN.
   - MAC 00:03 and IP 10.3 are learned in the proxy-ARP table and advertised in EVPN with the same SEQ number as the previous MAC route.
   - ARP-reply is unicasted to MAC 00:01.
7. EVPN advertisements are used to populate PE1's FDB (MAC 00:03) and proxy-ARP (IP 10.3 to MAC 00:03) tables as mentioned in5.

From this point onward, the PEs reply to any ARP-request for 00:01 or 00:03 without the need for flooding the message in the EVPN network. By replying to known ARP-requests and Neighbor Solicitations, the PEs help to significantly reduce the flooding in the network.

Use the following commands to customize proxy-ARP/proxy-ND behavior:

- **dynamic-arp-populate** and **dynamic-nd-populate**

  These commands enable the addition of dynamic entries to the proxy-ARP or proxy-ND table (disabled by default). When executed, the system populates proxy-ARP/proxy-ND entries from snooped GARP/ARP/NA messages on SAPs/SDP-bindings, in addition to the entries coming from EVPN (if EVPN is enabled). These entries are shown as dynamic.

- **static** *ipv4-address mac-address*, **static** *ipv4-address mac-address*, and static *ipv6-address mac-address* {**host** | **router**}

  These commands configure static entries to be added to the table.

  Note:
  A static IP-to-MAC entry requires the addition of the MAC address to the FDB as either learned or CStatic (conditional static mac) to become active (*Status active*).

- **age-time** *seconds*

  This command specifies the aging timer per proxy-ARP/proxy-ND entry. When the aging expires, the entry is flushed. The age is reset when a new ARP/GARP/NA for the same IP-to-MAC is received.

- **send-refresh** *seconds*

  If this command is enabled, the system sends ARP-request or Neighbor Solicitation (NS) messages at the configured time, which enables the owner of the IP to reply and, therefore, refresh its IP-to-MAC (proxy-ARP entry) and MAC (FDB entry).

- **table-size** *seconds*

  This command enables the user to limit the number of entries learned on a specified service. By default, the table-size limit is 250.

  Flooding unknown ARP-requests, NS messages, or unsolicited GARPs and NA messages in an EVPN network can be configured using the following commands:

  – **proxy-arp [no] unknown-arp-request-flood-evpn**
  – **proxy-arp [no] garp-flood-evpn**
  – **proxy-nd [no] unknown-ns-flood-evpn**
  – **proxy-nd [no] host-unsolicited-na-flood-evpn**
  – **proxy-nd [no] router-unsolicited-na-flood-evpn**

- **dup-detect** [**anti-spoof-mac** *mac-address*] **window** *minutes* **num-moves** *count* **hold-down** *minutes* | *max*

  This command enables a mechanism that detects duplicate IPs and ARP/ND spoofing attacks. The following is a summary of the **dup-detect** command mechanism:

  – Attempts (relevant to dynamic and EVPN entry types) to add the same IP (different MAC) are monitored for **window** *minutes* value and when the *count* value is reached within the configured **window**, the proxy-ARP/proxy-ND entry for the IP is suspected and marked as duplicate. An alarm is also triggered.

- The condition is cleared when **hold-down** time expires (*max* does not expire) or a **clear** command is issued.
- If the **anti-spoof-mac** command is configured, the proxy-ARP or proxy-ND offending entry's MAC is replaced by the configured *mac-address* and advertised in an unsolicited GARP/NA for local SAP or SDP-bindings and in EVPN to remote PEs.
- This mechanism assumes that the same **anti-spoof-mac** is configured in all PEs for the service, and that traffic with destination **anti-spoof-mac** received on SAPs/SDP-bindings is dropped. An ingress MAC filter must be configured to drop traffic to the **anti-spoof-mac**.

The following table shows the combinations that produce a **Status = Active** proxy-ARP entry in the table. The system only replies to proxy-ARP requests for active entries. Any other combination result in a **Status = inActv** entry. If the service is not active, the proxy-ARP entries are not active, regardless of the FDB entries

Note:
A static entry is active in the FDB even when the service is down.

Table 39: Proxy-ARP entry combinations

Proxy-ARP entry type	FDB entry type (for the same MAC)
Dynamic	learned
Static	CStatic
EVPN	EVPN, EVPNS with matching ESI
Duplicate	—

When proxy-ARP or proxy-ND is enabled on services with multi-homed ESs, a proxy-ARP entry type "EVPN" may be associated with a "learned" FDB entry because the CE can send traffic for the same MAC to all the multi-homed PEs in the ES. In such cases, the entry is inactive, in accordance with the preceding table.

4.3.1.1 Proxy-ARP/ND periodic refresh, unsolicited refresh, and confirm-messages

When proxy-ARP or proxy-ND is enabled, the system starts populating the proxy table and responding to ARP-requests or NS messages. To keep the active IP-to-MAC entries alive and ensure that all the host/routers in the service update their ARP/ND caches, the system may generate the following three types of ARP/ND messages for a specified IP-to-MAC entry:

- **periodic refresh messages (ARP-requests or NS for a specified IP)**

  These messages are activated by the **send-refresh** command and their objective is to keep the existing FDB and proxy-ARP/ND entries alive to minimize EVPN withdrawals and re-advertisements.
- **unsolicited refresh messages (unsolicited GARP or NA messages)**

  These messages are sent by the system when a new entry is learned or updated. Their objective is to update the attached host/router caches.
- **confirm messages (unicast ARP-requests or unicast NS messages)**

These messages are sent by the system when a new MAC is learned for an existing IP. The objective of the confirm messages is to verify that a specified IP has moved to a different part of the network and is associated with the new MAC. If the IP has not moved, it forces the owners of the duplicate IP to reply and triggers **dup-detect**.

4.3.1.2 Proxy-ND and the Router flag in Neighbor Advertisement messages

RFC 4861 describes the use of the (R) or "Router" flag in NA messages as follows:

- a node capable of routing IPv6 packets must reply to NS messages with NA messages where the R flag is set (R=1)
- hosts must reply with NA messages where R=0

The use of the R flag in NA messages impacts how the hosts select their default gateways when sending packets "off-link". Therefore, it is important that the proxy-ND function on the 7210 SAS meet one of the following criteria:

1. provide the appropriate R flag information in proxy-ND NA replies.
2. flood the received NA messages if it cannot provide the appropriate R flag when replying

Because of the use of the R flag, the procedure for learning proxy-ND entries and replying to NS messages differs from the procedures for proxy-ARP in IPv4: the router or host flag is added to each entry, and that determines the flag to use when responding to a NS.

4.3.1.3 Procedure to add the R flag to a specified entry

The procedure to add the R flag to a specified entry is as follows:

- Dynamic entries are learned based on received NA messages. The R flag is also learned and added to the proxy-ND entry so that the appropriate R flag is used in response to NS requests for a specified IP.
- Static entries are configured as host or router as per the [**no**] **static** *ip-address ieee-address* {**host** | **router**} command.
- EVPN entries are learned from BGP and the **evpn-nd-advertise** {**host** | **router**} the R flag added to them.
- In addition, the **evpn-nd-advertise** {**host** | **router**} command indicates what static and dynamic IP-to-MAC entries the system advertises in EVPN. If **evpn-nd-advertise router** is configured, the system should flood the received unsolicited NA messages for hosts. This is controlled by the [**no**] **host-unsolicited-na-flood-evpn** command. The opposite is also recommended, so that the **evpn-nd-advertise host** is configured using the **router-unsolicited-na-flood-evpn** command.

4.3.1.4 Configuration guidelines for proxy-ARP and proxy-ND

On the 7210 SAS, users can enable or disable proxy-ARP and proxy-ND commands for all EVPN services configured on the node; however, the option to enable or disable proxy-ARP or proxy-ND per service is not available.

Use the following syntax to enable or disable proxy-ARP or proxy-ND capability per node.

```
configure>service>system>[no]evpn-proxy-arp-nd
```

If the per-node **evpn-proxy-arp-nd** command is disabled, it is not possible to enable the **proxy-arp** or **proxy-nd** command per service, and **proxy-arp** or **proxy-nd** is disabled for all EVPN services on the node.

When the **evpn-proxy-arp-nd** command is enabled, the user must run the following sequence of commands to disable the per-node **proxy-arp** and **proxy-nd** commands, if required:

1. Run the **config>service>system>no evpn-proxy-arp-nd** command.
2. Run the **config>service>vpls>no proxy-arp** command.
3. Run the **config>service>vpls>no proxy-nd** command.

The following example shows the command usage to enable **proxy-arp** and **proxy-nd** for all services, with all parameters set to default values:

Example: Enabling proxy-arp and proxy-nd for all services

```
------------------------------------------------------------------------------
configure
  service
    system
       evpn-proxy-arp-nd
    exit
  exit

  service
    vpls 100
       proxy-arp
          no age-time
          dup-detect window 3 num-moves 5 hold-down 9
          no dynamic-arp-populate
          ...  (so on for other parameters supported under proxy-arp)
          no shutdowm
                exit

       proxy-nd
          no age-time
          dup-detect window 3 num-moves 5 hold-down 9
          no dynamic-nd-populate
          ...  (so on for other parameters supported under proxy-nd)
          no shutdowm
                exit
         exit
  exit
------------------------------------------------------------------------------
```

When the user runs the **config>service>system>evpn-proxy-arp-nd** command, the software automatically runs a **no shutdown** command for **proxy-arp** and **proxy-nd** for all services. Similarly, when the user runs the **config>service>system>no evpn-proxy-arp-nd** command, the software automatically runs a **shutdown** command for **proxy-arp** and **proxy-nd** for all services.

When the **evpn-proxy-arp-nd** command is enabled, the **proxy-arp** or **proxy-nd** command is enabled for all services and cannot be disabled for individual services. Configuring service-specific **proxy-arp** or **proxy-nd** command parameters is supported only when the **evpn-proxy-arp-nd** command is enabled.

4.3.1.4.1 Proxy-ARP and proxy-ND support for spoke-SDP bindings

The 7210 SAS does not support proxy-ARP and proxy-ND on spoke-SDP bindings. ARP or ND packets received on spoke-SDP bindings are not identified or sent to the CPU for further processing.

When using spoke-SDP bindings on the 7210 SAS, Nokia recommends that users disable proxy-ARP and proxy-ND functionality on all PEs belonging to the EVPN service, or enable the forwarding of ARP or ND packets over EVPN bindings on all PEs that belong to the EVPN service, so that ARP or ND packets are flooded throughout the EVPN instance.

4.3.2 BGP-EVPN MAC mobility

EVPN defines a mechanism to allow the smooth mobility of MAC addresses from one CE/NVE to another. The 7210 SAS supports this procedure and the MAC mobility extended community in MAC advertisement routes:

- The router honors and generates the Sequence (SEQ) number in the MAC mobility extended community for MAC moves.
- When a MAC is EVPN-learned and it is attempted to be learned locally, a BGP update is sent with SEQ number changed to "previous SEQ"+1 (exception: **mac-duplication detect** *num-moves* value is reached).
- A SEQ number = zero or no MAC mobility *ext-community* are interpreted as sequence zero.
- In case of mobility, the following MAC selection procedure is followed:
  - If a PE has two or more active remote EVPN routes for the same MAC, the highest SEQ number is selected. The tie-breaker is the lowest IP (BGP NH IP).
  - If a PE has two or more active EVPN routes and it is the originator of one of them, the highest SEQ number is selected. The tie-breaker is the lowest IP (BGP NH IP of the remote route is compared to the local system address).

Note: When EVPN multi-homing is used in EVPN-MPLS, the ESI is compared to determine whether a MAC received from two different PEs should be processed within the context of MAC mobility or multi-homing. Two MAC routes that are associated with the same remote or local ESI but different PEs are considered reachable through all those PEs. Mobility procedures are not triggered if the MAC route still belongs to the same ESI.

4.3.3 BGP-EVPN MAC duplication

EVPN defines a mechanism to protect the EVPN service from control plane churn as a result of loops or accidental duplicated MAC addresses. The 7210 SAS supports an enhanced version of this procedure, which is described in this section.

In a scenario where two or more hosts are misconfigured using the same (duplicate) MAC address, the duplicate MAC address is learned by the PEs in the VPLS. As a result, the traffic originating from the hosts triggers continuous MAC moves among the PEs attached to the hosts. It is important to recognize such situations and avoid incrementing the sequence number (in the MAC Mobility attribute) to infinity.

To remedy accidentally duplicated MAC addresses, a router that detects a MAC mobility event through local learning starts a **window** *in-minutes* timer (the default value is 3). If the configured **num-moves** *num* value is detected before the timer expires (the default value is 5), the router concludes that a duplicate MAC situation has occurred and sends a trap message to alert the operator. Use the **show service id** *svc-id* **bgp-evpn** command to display the MAC addresses. The following is a sample configuration output.

Example: BGP-EVPN MAC duplication configuration

```
10 2014/01/14 01:00:22.91 UTC MINOR: SVCMGR #2331 Base
```

```
"VPLS Service 1 has MAC(s) detected as duplicates by EVPN mac-
duplication detection."
# show service id 1 bgp-evpn
===============================================================================
BGP EVPN Table
===============================================================================
MAC Advertisement  : Enabled           Unknown MAC Route  : Disabled
MPLS Admin Status : Enabled           Creation Origin    : manual
MAC Dup Detn Moves : 5                 MAC Dup Detn Window: 3
MAC Dup Detn Retry : 9                 Number of Dup MACs : 1
-------------------------------------------------------------------------------
Detected Duplicate MAC Addresses            Time Detected
-------------------------------------------------------------------------------
00:00:00:00:00:12                           01/14/2014 01:00:23
-------------------------------------------------------------------------------
===============================================================================
```

After a duplicate MAC address is detected, the router stops sending and processing BGP MAC advertisement routes for that MAC address until one of the following occurs:

1. The MAC is flushed because of a local event (SAP or SDP-binding associated with the MAC fails) or the reception of a remote update with better SEQ number (because of a MAC flush at the remote router).
2. The **retry** *in-minutes* timer expires, which flushes the MAC and restarts the process.

Note: The other routers in the VPLS instance forward the traffic for the duplicate MAC address to the router advertising the best route for the MAC.

The values of **num-moves** and **window** can be configured for different environments. In scenarios where BGP rapid-update EVPN is configured, the operator should configure a shorter window timer than scenarios where BGP updates are sent per the configured **min-route-advertisement** interval, which is the default.

The preceding MAC duplication parameters can be configured per VPLS service under the **bgp-evpn mac-duplication** context. The following is a sample configuration output.

Example: MAC duplication parameter configuration

```
A:Dut-B>config>service>vpls>bgp-evpn# info
----------------------------------------------
                evi 1
                mac-duplication
                    detect num-moves 5 window 2
                    retry 10
                exit
                mpls
                    split-horizon-group "vpls1"
                    ingress-replication-bum-label
                    auto-bind-tunnel
                        resolution-filter
                            ldp
                        exit
                        resolution filter
                    exit
                    no shutdown
                exit
----------------------------------------------
```

4.3.4 Conditional static MAC and protection

In RFC 7432, the MAC Mobility Extended Community section defines the use of the sticky bit to signal static MAC addresses. These addresses must be protected to prevent attempts to dynamically learn them in a different place in the EVPN-MPLS VPLS service.

Note: On the 7210 SAS, the conditional static MACs are not protected using MAC-protect functionality. A Cstatic MAC is advertised to other PEs with the sticky bit set so that it is prevented from being learned dynamically at a different place in the EVPN-MPLS VPLS service. MAC frames whose source MAC address matches the statically configured MAC address are forwarded based on destination MAC address lookup and are not dropped.

In the 7210 SAS, any conditional static MAC address that is defined in an EVPN-MPLS VPLS service is advertised by BGP-EVPN as a static address (that is, with the sticky bit set). The following example shows configuration output of a conditional static MAC.

Example: Conditional static MAC configuration

```
*A:Dut-B>config>service>vpls# info
----------------------------------------------
            description "evpn mpls service "
…….
            sap lag-1:1 create
                description "Default sap description for service id 1"
                no shutdown
            exit
            static-mac
                mac 00:ca:ca:ca:ca:00 create sap lag-1:1 monitor fwd-status
            exit
```

```
A:Dut-C# show router bgp routes evpn mac hunt mac-address 00:ca:ca:ca:ca:00
……..
===============================================================================
BGP EVPN MAC Routes
===============================================================================
-------------------------------------------------------------------------------
RIB In Entries
-------------------------------------------------------------------------------
Network        : n/a
Nexthop        : 10.20.1.2
From           : 10.20.1.2
Res. Nexthop   : 10.10.3.2
Local Pref.    : 100                    Interface Name : ip-10.10.3.3
Aggregator AS  : None                   Aggregator     : None
Atomic Aggr.   : Not Atomic             MED            : 0
AIGP Metric    : None                   IGP Cost       : 400
Connector      : None
Community      : target:100:1 bgp-tunnel-encap:MPLS
                 mac-mobility:Seq:0/Static
Cluster        : No Cluster Members
Originator Id  : None                   Peer Router Id : 10.20.1.2
Flags          : Used  Valid  Best  IGP
Route Source   : Internal
AS-Path        : No As-Path
EVPN type      : MAC
ESI            : 00:bc:01:00:00:00:00:00:00:01
Tag            : 0
IP Address     : n/a
```

```
Route Dist.    : 2.2.2.2:1
Mac Address    : 00:ca:ca:ca:ca:00
MPLS Label1    : LABEL 131056          MPLS Label2    : n/a
Route Tag      : 0
Neighbor-AS    : n/a
Orig Validation: N/A
Add Paths Send : Default
Last Modified  : 00h02m02s

-------------------------------------------------------------------------------
RIB Out Entries
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
Routes : 1
===============================================================================
```

4.3.5 BGP and EVPN route selection for EVPN routes

When two or more EVPN routes are received at a PE, BGP route selection typically takes place when the route key or the routes are equal. When the route key is different, but the PE has to make a selection (for example, the same MAC is advertised in two routes with different RDs), BGP hands over the routes to EVPN and the EVPN application performs the selection.

EVPN and BGP selection criteria are as follows:

- **EVPN route selection for MAC routes**

  When two or more routes with the same *mac-length*/*mac* but different route key are received, BGP transfers the routes to EVPN. EVPN selects the route based on the following tie-breaking order:

  1. conditional static MACs (local protected MACs)
  2. EVPN static MACs (remote protected MACs)
  3. data plane learned MACs (regular learning on SAPs/SDP-bindings)
  4. EVPN MACs with higher SEQ number
  5. lowest IP (next-hop IP of the EVPN NLRI)
  6. lowest Ethernet tag (that is zero for MPLS)
  7. lowest RD

- **BGP route selection for MAC routes with the same route-key**

  The priority order is as follows:

  1. EVPN static MACs (remote protected MACs)
  2. EVPN MACs with higher sequence number
  3. regular BGP selection (local-pref, aigp metric, shortest as-path, …, lowest IP)

- **BGP route selection for the rest of the EVPN routes follows regular BGP selection**

Note:
If BGP runs through the selection criteria and a specified and valid EVPN route is not selected in favor of another EVPN route, the non-selected route is displayed by the **show router bgp routes evpn** *evpn-type* **detail** command with a tie-breaker reason.

4.3.6 EVPN interaction with other features

This section describes the interaction of EVPN with other features.

4.3.6.1 EVPN-MPLS with existing VPLS features

When enabling existing VPLS features in an EVPN-MPLS-enabled service, the following considerations apply:

- EVPN-MPLS is only supported in regular VPLS. Other VPLS types, such as M-VPLS, are not supported with EVPN-MPLS.
- In general, no router-generated control packets are sent to the EVPN destination bindings, except for proxy-ARP/proxy-ND confirm messages for EVPN-MPLS.
- For xSTP and M-VPLS services, the following applies:
  - xSTP can be configured in BGP-EVPN services. BPDUs are not sent over the EVPN bindings.
  - BGP-EVPN is blocked in M-VPLS services; however, a different M-VPLS service can manage a SAP or spoke-SDP in a BGP-EVPN-enabled service.
- For BGP-EVPN-enabled VPLS services, **mac-move** can be used in SAPs/SDP-bindings; however, MACs learned through BGP-EVPN are not considered.

  Note:
  MAC duplication provides protection against MAC moves between EVPN and SAPs/SDP-bindings.

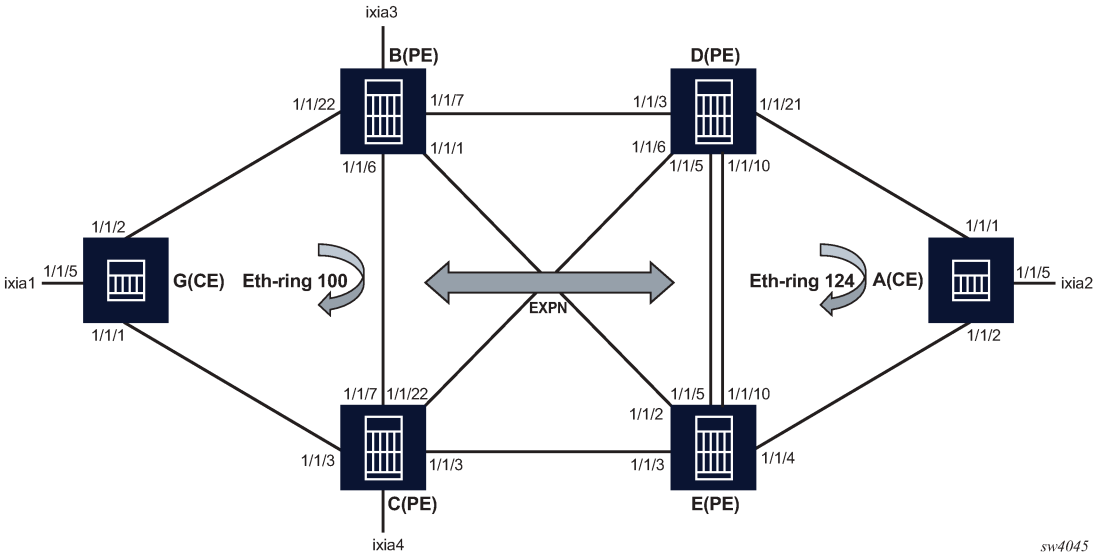
- The **disable-learning** command and other FDB-related tools only work for data-plane-learned MAC addresses.
- MAC OAM tools (**mac-ping**, **mac-trace**, **mac-populate**, **mac-purge**, and **cpe-ping**) are not supported for BGP-EVPN services.
- SAPs that belong to a specified ES but are configured on non-BGP-EVPN-MPLS-enabled VPLS or Epipe services are kept down using the **StandByForMHProtocol** flag.
- CPE ping is not supported on EVPN services.
- Other features not supported in conjunction with BGP-EVPN are:
  - endpoints and attributes
  - BPDU translation
  - L2PT termination
  - MAC-pinning
  - IGMP snooping in VPLS services when BGP-EVPN MPLS is enabled (in the service)
  - DHCP snooping
  - ETH-CFM (MEPs, vMEPs, MIPs)
  - **allow-ip-int-bind** (R-VPLS)

4.3.6.2 EVPN with G.8032 in an access ring

It is possible to use the G.8032 operation in an access ring with EVPN. The only supported configuration is a G.8032 sub-ring with a non-virtual link and without MAC flush propagation from the EVPN network to the G.8032 sub-ring. This section provides a sample configuration and guidelines about the configuration.

The following figure shows the network topology of an access ring with EVPN. It shows a G.8032 sub-ring formed by nodes G, B, C on the left side of the figure and nodes A, D, E on the right side of the figure, connected to the EVPN network formed by nodes B, C, D, E.

Figure 47: Network topology of an access ring



Nodes B, C, D, E connect to both the EVPN network using network ports and to the G.8032 ring using access ports. For example, on node B, network ports 1/1/7, 1/1/1, and 1/1/6 connect PE-B to remote EVPN nodes D, E, C, respectively. Additionally, on node B, access port 1/1/22 is part of the G.8032 access ring that connects PE-B to the G.8032 ring formed with access CE node G.

EVPN bindings are protected by using fast reroute (FRR) paths; however, in the event a failure occurs in the EVPN network, MAC flush is not propagated from the EVPN network to the G.8032 ring.

G.8032 data SAPs and control SAPs on the EVPN PE nodes (B, C, D, E) can be configured only on non-ES ports. Non-ES LAGs cannot be used with G.8032 on 7210 SAS.

Example: Access CE node A configuration

The following example shows a configuration of the access CE node, node A in Figure 47: Network topology of an access ring, which is part of the G.8032 access ring.

```
#--------------------------------------------------
echo "System Configuration"
#--------------------------------------------------
    system
        name "Dut-A"
#--------------------------------------------------
echo "Ethernet Rings Configuration"
#--------------------------------------------------
    eth-ring 124
```

```
    exit
    eth-ring 124
        description "Ethernet Ring 124"
        guard-time 20
        revert-time 60
        rpl-node owner
        path a 1/1/1 raps-tag 124
            description "Ethernet Ring : 124 Path : pathA"
            rpl-end
            eth-cfm
                mep 6 domain 1 association 1241
                    ccm-enable
                    control-mep
                    control-sap-tag 724
                    no shutdown
                exit
            exit
            no shutdown
        exit
        path b 1/1/2 raps-tag 124
            description "Ethernet Ring : 124 Path : pathB"
            eth-cfm
                mep 7 domain 1 association 1242
                    ccm-enable
                    control-mep
                    control-sap-tag 724
                    no shutdown
                exit
            exit
            no shutdown
        exit
        no shutdown
    exit
#--------------------------------------------------
------snipped------------
#--------------------------------------------------
echo "Service Configuration"
#--------------------------------------------------
    service
        customer 1 create
            description "Default customer"
        exit
        vpls 1 customer 1 svc-sap-type any create
            description "Default tls description for service id 1"
            disable-learning

            stp
                shutdown
            exit
            sap 1/1/5:1 create
                description "Default sap description for service id 1"
                egress
                exit
            exit
            sap 1/1/1:1 eth-ring 124 create
                stp
                    shutdown
                exit
                egress
                exit
            exit
            sap 1/1/2:1 eth-ring 124 create
                stp
                    shutdown
```

```
                exit
                egress
                exit
            exit
            no shutdown
        exit
        vpls 124 customer 1 vpn 124 svc-sap-type any create
            description "Default tls description for service id 124"
            stp
                shutdown
            exit
            sap 1/1/1:124 eth-ring 124 create
                description "SAP 1/1/1:124 on Ethernet Ring 124 "
                stp
                    shutdown
                exit
                egress
                exit
            exit
            sap 1/1/2:124 eth-ring 124 create
                description "SAP 1/1/2:124 on Ethernet Ring 124 "
                stp
                    shutdown
                exit
                egress
                exit
            exit
            no shutdown
        exit
    exit
#--------------------------------------------------
```

Example: EVPN PE node D configuration

The following is a sample configuration of an EVPN PE node, node D in Figure 47: Network topology of an access ring.

```
#--------------------------------------------------
echo "System Configuration"
#--------------------------------------------------
    system
        name "Dut-D"
---------snipped-------------
#--------------------------------------------------
echo "Ethernet Rings Configuration"
#--------------------------------------------------
    eth-ring 124
    exit
    eth-ring 124
        description "Ethernet Ring 124"
        guard-time 20
        path a 1/1/21 raps-tag 124
            description "Ethernet Ring : 124 Path : pathA"
            eth-cfm
                mep 5 domain 1 association 1243
                    ccm-enable
                    control-mep
                    control-sap-tag 724
                    no shutdown
                exit
            exit
            no shutdown
        exit
```

```
        no shutdown
    exit
#--------------------------------------------------
--------snipped-----------------
#--------------------------------------------------
echo "Service Configuration"
#--------------------------------------------------
    service
        sdp 42 mpls create
            far-end 10.20.1.2
            ldp
            path-mtu 1600
            keep-alive
                shutdown
            exit
            no shutdown
        exit
        sdp 43 mpls create
            far-end 10.20.1.3
            ldp
            path-mtu 1600
            keep-alive
                shutdown
            exit
            no shutdown
        exit
        sdp 45 mpls create
            far-end 10.20.1.5
            ldp
            path-mtu 1600
            keep-alive
                shutdown
            exit
            no shutdown
        exit
        customer 1 create
            description "Default customer"
        exit
        system
            bgp-evpn
                ethernet-segment "esPort1" create
                    esi 00:de:03:00:00:00:00:00:03
                    service-carving
                        mode auto
                    exit
                    multi-homing single-active no-esi-label
                    shutdown
                exit
            exit
        exit
        vpls 1 customer 1 svc-sap-type any create
            description "Default tls description for service id 1"
            split-horizon-group "vpls1" create
                description "Default description for SHG vpls1"
            exit
            bgp-evpn
                evi 1
                mpls
                    control-word
                    force-vlan-vc-forwarding
                    split-horizon-group "vpls1"
                    ingress-replication-bum-label
                    auto-bind-tunnel
                        resolution any
```

```
                    exit
                    no shutdown
                exit
            exit
            stp
                shutdown
            exit
            sap 1/1/21:1 eth-ring 124 create
                stp
                    shutdown
                exit
                egress
                exit
            exit
            no shutdown
        exit
        vpls 124 customer 1 vpn 124 svc-sap-type any create
            description "Default tls description for service id 124"
            stp
                shutdown
            exit
            sap 1/1/21:124 eth-ring 124 create
                description "SAP 1/1/21:124 on Ethernet Ring 124 "
                stp
                    shutdown
                exit
                egress
                exit
            exit
            no shutdown
        exit
    exit
#--------------------------------------------------
echo "Router (Service Side) Configuration"
#--------------------------------------------------
    router Base
#--------------------------------------------------
echo "BGP Configuration"
#--------------------------------------------------
        bgp
            connect-retry 1
            min-route-advertisement 1
            rapid-withdrawal
            bfd-enable
            group "bgpEvpn"
                peer-as 100
                bfd-enable
                neighbor 10.20.1.2
                    family evpn
                    peer-as 100
                    bfd-enable
                exit
                neighbor 10.20.1.3
                    family evpn
                    peer-as 100
                    bfd-enable
                exit
                neighbor 10.20.1.5
                    family evpn
                    peer-as 100
                    bfd-enable
                exit
            exit
            no shutdown
```

```
        exit
#-------------------------------------------------
```

4.3.7 Routing policies for BGP EVPN routes

Routing policies match on specific fields when importing or exporting EVPN routes. These matching fields are the following:

- communities (*comm-val*), extended communities (*ext-comm*), and large communities (*large-comm*)
- well-known communities (*well-known-comm*); **no-export** | **no-export-subconfed** | **no-advertise**
- family EVPN
- protocol BGP-VPN (this term also matches VPN-IPv4/6 routes)
- BGP attributes that are applicable to EVPN routes (such as AS-path, local-preference, next-hop)

4.4 Configuring an EVPN service with CLI

This section provides information to configure EVPN services using the CLI for 7210 SAS-R6 and 7210 SAS-R12.

4.4.1 EVPN-MPLS configuration examples

This section provides EVPN-MPLS configuration examples.

4.4.1.1 EVPN single-active multi-homing example

To use single-active multi-homing on PE-1 and PE-2 instead of all-active multi-homing perform the following:

- Change the LAG configuration to **multi-homing single-active**.

  The CE-12 is now configured with two different LAGs; therefore, the key, system ID, and system priority values must be different on PE-1 and PE-2.
- Change the Ethernet segment configuration to **multi-homing single-active**.

No changes are needed at the service level on any of the three PEs.

The following configuration example shows the differences between single-active multi-homing and all-active multi-homing.

Example: Single-active and all-active multi-homing

```
A:PE1# configure lag 1
A:PE1>config>lag# info
----------------------------------------------
        mode access
        encap-type dot1q
        port 1/1/2
        lacp active administrative-key 1 system-id 00:00:00:00:69:69
        no shutdown
```

```
-----------------------------------------------
A:PE1>config>lag# /configure service system bgp-evpn
A:PE1>config>service>system>bgp-evpn# info
 esi 00:de:01:00:00:00:00:00:00:01
                service-carving
                    mode auto
                exit
                multi-homing single-active
                lag 6
                no shutdown
-----------------------------------------------
A:PE2# configure lag 1
A:PE2>config>lag# info
-----------------------------------------------
        mode access
        encap-type dot1q
        port 1/1/3
        lacp active administrative-key 1 system-id 00:00:00:00:72:72
        no shutdown
-----------------------------------------------
A:PE2>config>lag# /configure service system bgp-evpn
A:PE2>config>service>system>bgp-evpn# info
 esi 00:de:01:00:00:00:00:00:00:01
                service-carving
                    mode auto
                exit
                multi-homing single-active
                lag 6
                no shutdown
```

4.5 EVPN command reference

This section describes the EVPN commands for 7210 SAS-R6 and 7210 SAS-R12.

4.5.1 Command hierarchies

- EVPN configuration commands
- EVPN show commands
- EVPN clear commands
- EVPN tools commands

4.5.1.1 EVPN configuration commands

Note: See VPLS services command reference for information about configuring commands in the **config>vpls>bgp** context.

```
config
    - service
        - system
            - [no] evpn-proxy-arp-nd
config
    - service
```

```
        -  vpls  service-id [customer customer-id] [create] [vpn vpn-id] [m-vpls]
        - no vpls  service-id
            - bgp-evpn
            - no bgp-evpn
                - evi value
                -  no evi
                -  [no] mac-advertisement
                -  mac-duplication
                    - detect  num-moves num-moves window minutes
                    - retry  minutes
                    - no retry
                -  mpls
                    -  auto-bind-tunnel
                        -  resolution {disabled | any | filter}
                        -  resolution-filter
                            - [no] bgp
                            - [no] ldp
                            - [no] rsvp
                            - [no] sr-isis
                            - [no] sr-ospf
                    - [no] control-word
                    - no force-vlan-vc-forwarding
                    - [no] ingress-replication-bum-label
                    - [no] shutdown
                    -  split-horizon-group  name
                    -  no split-horizon-group
            - [no] proxy-arp
                - age-time seconds
                - no age-time
                - dup-detect [anti-spoof-mac mac-address] window minutes num-moves count hold-
down minutes | max
                - [no] dynamic-arp-populate
                - [no] garp-flood-evpn
                - [no] send-refresh seconds
                - static ip-address ieee-address
                - no static ip-address
                - table-size table-size
                - [no] unknown-arp-request-flood-evpn
                - [no] shutdown
            - [no] proxy-nd
                - age-time seconds
                - no age-time
                - dup-detect [anti-spoof-mac mac-address] window minutes num-moves count hold-
down minutes | max
                - [no] dynamic-nd-populate
                - evpn-nd-advertise {host | router}
                - [no] host-unsolicited-na-flood-evpn
                - [no] router-unsolicited-na-flood-evpn
                - [no] send-refresh seconds
                - [no] static ip-address ieee-address {host | router}
                - table-size table-size
                - [no] unknown-ns-flood-evpn
                - [no] shutdown
```

```
config
    - service
        - system
            - bgp-evpn
                - ethernet-segment  name [create] [virtual]
                    - es-activation-timer seconds
                    - no es-activation-timer
                    - esi esi
                    - no esi
```

```
                    - lag lag-id
                    - no lag
                    - multi-homing single-active no-esi-label
                    - no multi-homing
                    - port port-id
                    - no port
                    - service-carving
                        - manual
                            - evi start [to to]
                            - no evi start
                        - mode {auto | manual | off}
                    - [no] shutdown
                - route-distinguisher rd
                - no route-distinguisher
config
    - redundancy
        - bgp-evpn-multi-homing
                - boot-timer  seconds
                - es-activation-timer  seconds
```

4.5.1.2 EVPN show commands

```
show
    - service
        - evpn-mpls
        - id service-id
            - bgp-evpn
            - evpn-mpls  [esi esi]
            - proxy-arp [ip-address] [detail]
            - proxy-nd [ip-address] [detail]
        - system
            - bgp-evpn
```

```
show
    - redundancy
        - bgp-evpn-multi-homing
```

4.5.1.3 EVPN clear commands

```
clear
    - service
        - id service-id
            - proxy-arp [duplicate] [dynamic]
            - proxy-nd [duplicate] [dynamic]
```

4.5.1.4 EVPN tools commands

```
tools
    - dump
        - service
            - proxy-arp
                - usage
            - proxy-nd
```

```
                - usage
```

4.5.2 Command descriptions

4.5.2.1 EVPN configuration commands

evpn-proxy-arp-nd

Syntax

[**no**] **evpn-proxy-arp-nd**

Context

config>service>system

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables proxy-ARP and proxy-ND capability per node.

When this command is enabled, the **proxy-arp** and **proxy-nd** commands are enabled for all services and cannot be disabled for individual services. Using the per-service CLI context and commands under the **proxy-arp** or **proxy-nd** command, users can configure the service-specific **proxy-arp** or **proxy-nd** command parameters. Only when the **evpn-proxy-arp-nd** command is enabled can the per-service CLI commands be used to configure **proxy-arp** or **proxy-nd** parameters.

When this command is disabled, it is not possible to enable the **proxy-arp** or **proxy-nd** command per service, and **proxy-arp** and **proxy-nd** is disabled for all EVPN services on the node.

The **no** form of this command disables proxy-ARP and proxy-ND capability per node.

Note: The **no** form of this command reverts all configured **proxy-arp** and **proxy-nd** command parameters to the default values and shuts down proxy-ARP and proxy-ND for all services.

Default

no evpn-proxy-arp-nd

vpls

Syntax

vpls *service-id* [**customer** *customer-id*] [**vpn** *vpn-id*] [**m-vpls**] [**name** *name*] [**create**]

no vpls *service-id*

Context

config>service

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command creates or edits a Virtual Private LAN Service (VPLS) 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.

A VPLS connects multiple customer sites together acting like a zero-hop, Layer 2 switched domain. A VPLS is always a logical full mesh.

If the **create** command is enabled in the **environment** context, the **create** keyword must be specified when the service is created. Specify the **customer** keyword and *customer-id* to associate the service with a customer. The *customer-id* must already exist (created using the **customer** command in the service context). After a service has been created with a customer association, it is not possible to edit the customer association. To edit the customer association, the service must be deleted and recreated with a new customer association.

After a service is created, the use of the **customer** *customer-id* is optional for navigating into the service configuration context. Attempting to edit a service with the incorrect *customer-id* specified results in an error.

More than one VPLS may be created for a single customer ID.

By default, no VPLS instances exist until they are explicitly created.

The **no** form of this command deletes the VPLS service instance with the specified *service-id*. The service cannot be deleted until all SAPs and SDPs defined within the service ID have been shutdown and deleted, and the service has been shutdown.

Parameters

service-id

Specifies the unique service identification number or string identifying the service in the service domain. This ID must be unique to this service and may not be used for any other service of any type. The *service-id*must be the same number used for every router on which this service is defined.

Values *service-id* — 1 to 2147483648

svc-name — a string up to 64 characters

customer *customer-id*

Specifies the customer ID number to be associated with the service. This parameter is required on service creation and optional for service editing or deleting.

Values 1 to 2147483647

vpn vpn-id

Specifies the VPN ID number which allows you to identify VPNs by a VPN identification number.

Values 1 to 2147483647

Default null (0)

m-vpls

Specifies a management VPLS.

bgp-evpn

Syntax

bgp-evpn

no bgp-evpn

Context

config>service>vpls

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

Commands in this context configure the BGP-EVPN parameters in the base instance.

The **no** form of this command disables BGP-EVPN.

evi

Syntax

evi *value*

no evi

Context

config>service>vpls>bgp-evpn

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command specifies a 2-byte EVPN instance that is unique in the system. It is used by the service-carving algorithm for multihoming and auto-deriving route target and route distinguishers.

If not specified, the value is zero and no route distinguisher or route targets are auto-derived from it. If the **evi** *value* is specified and no other route distinguisher or route target is configured in the service, the following rules apply:

- the route distinguisher is derived from <**system_ip**>:**evi**

- the route-target is derived from <**autonomous-system**>:**evi**

Note:
If VSI import and export policies are configured, the route target must be configured in the policies, and those values take precedence over the auto-derived route targets. The operational route target for a service is shown in the **show service id bgp** command.

The **no** form of this command reverts the **evi** *value* to zero.

Default

no evi

Parameters

value

Specifies the EVPN instance.

Values 1 to 65535

mpls

Syntax

mpls

Context

config>service>vpls>bgp-evpn

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

Commands in this context configure the BGP EVPN MPLS parameters.

auto-bind-tunnel

Syntax

auto-bind-tunnel

Context

config>service>vpls>bgp-evpn>mpls

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

Commands in this context configure automatic binding of a BGP-EVPN service using tunnels to MP-BGP peers.

The resolution mode must be configured to enable auto-bind resolution to tunnels in TTM. The following configurations are available.

- If **resolution** is explicitly set to **disabled**, the auto-binding to the tunnel is removed.
- If **resolution** is set to **any**, any tunnel type supported in the EVPN context is selected, following TTM preference.
- The **resolution-filter** option is used to specify one or more explicit tunnel types; only the specified tunnel types are selected again following the TTM preference.

The following tunnel types are supported in a BGP-EVPN MPLS context, in order of preference: RSVP, LDP, SR-ISIS, SR-OSPF, and BGP.

The rsvp value specifies that BGP searches for the best metric RSVP LSP to the address of the BGP next hop. This address can correspond to the system interface or to another loopback used by the BGP instance on the remote node. The LSP metric is provided by MPLS in the tunnel table. In the case of multiple RSVP LSPs with the same lowest metric, BGP selects the LSP with the lowest tunnel ID.

The ldp value specifies that BGP searches for an LDP LSP with a FEC prefix corresponding to the address of the BGP next hop.

The sr-isis (sr-ospf) value specifies that an SR tunnel to the BGP next hop is selected in the TTM from the lowest numbered ISIS (OSPF) instance.

The bgp value specifies BGP EVPN to search for a BGP LSP to the address of the BGP next hop. If the user does not enable the BGP tunnel type, the inter-area or inter-as prefixes is not resolved.

To activate the list of tunnel-types configured under **resolution-filter**, the **resolution** must be set to **filter**.

resolution

Syntax

resolution {**disabled** | **any** | **filter**}

Context

config>service>vpls>bgp-evpn>mpls>auto-bind-tunnel

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the resolution mode in the automatic binding of a BGP-EVPN MPLS service to tunnels to MP-BGP peers.

Default

resolution disabled

Parameters

disabled

Specifies to disable the automatic binding of a BGP-EVPN MPLS service to tunnels to MP-BGP peers.

any

Specifies to enable the binding to any tunnel type supported in a BGP-EVPN MPLS context following TTM preference.

filter

Specifies to enable the binding to the subset of tunnel types configured under **resolution-filter**.

resolution-filter

Syntax

resolution-filter

Context

config>service>vpls>bgp-evpn>mpls>auto-bind-tunnel

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

Commands in this context configure the subset of tunnel types that can be used in the resolution of BGP-EVPN routes within the automatic binding of BGP-EVPN MPLS service to tunnels to MP-BGP peers.

The following tunnel types are supported in a BGP-EVPN MPLS context, in order of preference: RSVP, LDP, Segment Routing (SR), BGP, and UDP.

bgp

Syntax

[**no**] **bgp**

Context

config>service>vpls>bgp-evpn>mpls>auto-bind-tunnel>resolution-filter

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command specifies the BGP tunnel type.

BGP EVPN searches for a BGP LSP to the address of the BGP next hop. If the user does not enable the BGP tunnel type, the inter-area or inter-as prefixes are resolved.

The **no** form of this command disables BGP as a tunnel type to consider.

Default

no bgp

ldp

Syntax

[**no**] **ldp**

Context

config>service>vpls>bgp-evpn>mpls>auto-bind-tunnel>resolution-filter

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command specifies the LDP tunnel type.

BGP searches for an LDP LSP with a FEC prefix corresponding to the address of the BGP next-hop.

The **no** form of this command disables LDP as a tunnel type to consider.

Default

no ldp

rsvp

Syntax

[**no**] **rsvp**

Context

config>service>vpls>bgp-evpn>mpls>auto-bind-tunnel>resolution-filter

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command specifies the RSVP-TE tunnel type.

BGP searches for the best metric RSVP LSP to the address of the BGP next hop. This address can correspond to the system interface or to another loopback used by the BGP instance on the remote node.

The LSP metric is provided by MPLS in the tunnel table. In the case of multiple RSVP LSPs with the same lowest metric, BGP selects the LSP with the lowest tunnel-id.

The **no** form of this command disables RSVP as a tunnel type to consider.

Default

no rsvp

sr-isis

Syntax

[**no**] **sr-isis**

Context

config>service>vpls>bgp-evpn>mpls>auto-bind-tunnel>resolution-filter

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command specifies the Segment Routing (SR) tunnel type programmed by an IS-IS instance in TTM.

The **no** form of this command disables SR-ISIS as a tunnel type to consider.

Default

no sr-isis

sr-ospf

Syntax

[**no**] **sr-ospf**

Context

config>service>vpls>bgp-evpn>mpls>auto-bind-tunnel>resolution-filter

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command specifies the SR tunnel type programmed by an OSPF instance in TTM.

The SR tunnel to the BGP next hop is selected in the TTM from the lowest numbered IS-IS (OSPF) instance.

The **no** form of this command disables SR-OSPF as a tunnel type to consider.

Default

no sr-ospf

shutdown

Syntax

shutdown

no shutdown

Context

config>service>vpls>bgp-evpn>mpls

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

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

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

Default

shutdown

mac-advertisement

Syntax

[**no**] **mac-advertisement**

Context

config>service>vpls>bgp-evpn

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables the advertisement in BGP of the learned MACs on SAPs and SDP bindings. When the **mac-advertisement** command is disabled, the local MACs are withdrawn in BGP.

The **no** form of this command disables **mac-advertisement**.

Default

mac-advertisement

mac-duplication

Syntax

mac-duplication

Context

config>service>vpls>bgp-evpn

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

Commands in this context configure the BGP EVPN MAC duplication parameters.

detect

Syntax

detect num-moves *num-moves* **window** *minutes*

Context

config>service>vpls>bgp-evpn>mac-duplication

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command modifies the default behavior of the **mac-duplication** feature, which is always enabled by default. The command specifies the number of moves (**num-moves**) to monitor within a period of time (**window**).

Default

detect num-moves 5 window 3

Parameters

num-moves

Specifies the number of MAC moves in a VPLS. The counter is incremented when a specified MAC is locally relearned in the FDB or flushed from the FDB because of the reception of a better remote EVPN route for that MAC.

Values 3 to 10

Default 5

minutes

Specifies the length of the window, in minutes.

Values 1 to 15

Default 3

retry

Syntax

retry *minutes*

no retry

Context

config>service>vpls>bgp-evpn>mac-duplication

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command specifies the timer after which the MAC in hold-down state is automatically flushed and the MAC duplication process starts again. This value is expected to be equal to two times or more than that of **window**.

If the **no** form of this command is configured and MAC duplication is detected, MAC updates for that MAC are held down until the user intervenes or a network event (that flushes the MAC) occurs.

Default

retry 9

Parameters

minutes

Specifies the BGP EVPN MAC duplication retry, in minutes.

Values 2 to 60

control-word

Syntax

[**no**] **control-word**

Context

config>service>vpls>bgp-evpn>mpls

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables the transmission and reception of the control word, as defined in RFC 7432, which helps avoid frame disordering.

This command is enabled or disabled for all EVPN-MPLS destinations at the same time.

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

Default

no control-word

force-vlan-vc-forwarding

Syntax

no force-vlan-vc-forwarding

Context

config>service>vpls>bgp-evpn>mpls

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command allows the system to preserve the VLAN ID and 802.1p bits of the service-delimiting qtag in a new tag added in the customer frame before sending it to the EVPN-MPLS destinations.

Note: When the **force-vlan-vc-forwarding** command is enabled, the VC VLAN ID is always set to 0.

This command is disabled on the 7210 SAS. It is set to the **no** form by default and cannot be enabled. If the ingress SAP/SDP binding is null-encapsulated, the output VLAN ID and pbits are zero.

Default

no force-vlan-vc-forwarding

ingress-replication-bum-label

Syntax

[**no**] **ingress-replication-bum-label**

Context

config>service>vpls>bgp-evpn>mpls

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the system to send a separate label for Broadcast, Unknown unicast and Multicast (BUM) traffic in a specified service. By default (**no ingress-replication-bum-label**), the same label is used for unicast and flooded BUM packets when forwarding traffic to remote PEs.

Saving labels may cause transient traffic duplication for all-active multihoming. If **ingress-replication-bum-label** is enabled, the system advertises two labels per EVPN VPLS instance, one for unicast and one for BUM traffic. The ingress PE uses the BUM label for flooded traffic to the advertising egress PE, which allows the egress PE to determine whether unicast traffic has been flooded by the ingress PE. Depending on the scale required in the network, the user may choose between saving label space or avoiding transient packet duplication sent to an all-active multi-homed CE for certain MACs.

The **no** form of this command uses the same label for unicast and flooded BUM packets.

Default

no ingress-replication-bum-label

split-horizon-group

Syntax

split-horizon-group *name*

no split-horizon-group

Context

config>service>vpls>bgp-evpn>mpls

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures an explicit split-horizon group for all BGP-EVPN MPLS destinations that can be shared by other SAPs and spoke-SDPs. The use of explicit split-horizon groups for EVPN-MPLS and spoke-SDPs allows the integration of VPLS and EVPN-MPLS networks.

If the **bgp-evpn mpls split-horizon-group** command is not used, the default split-horizon group (that contains all the EVPN destinations) is still used, but it is not possible to associate with it from SAPs/spoke-SDPs.

User-configured split-horizon groups can be configured within the service context. The same group name can be associated with SAPs, spoke-SDPs, pw-templates, pw-template-bindings, and EVPN-MPLS destinations.

The configuration of the **bgp-evpn mpls split-horizon-group** command is only allowed if **bgp-evpn>mpls** is shut down; no changes are allowed when **bgp-evpn>mpls** is **no shutdown**.

If the SAPs or spoke-SDPs (manual) are configured within the same split-horizon group as the EVPN-MPLS endpoints, MAC addresses are still learned but not advertised in BGP-EVPN. If an EVPN-MPLS provider tunnel is enabled in the service, the SAPs and SDP-bindings that share the same split-horizon group of the EVPN-MPLS provider-tunnel are brought operationally down if the point-to-multipoint tunnel is operationally up.

The **no** form of this command configures the EVPN-MPLS destinations to use the default split-horizon group.

Default

no split-horizon-group

Parameters

name

Specifies the split-horizon group name.

proxy-arp

Syntax

[**no**] **proxy-arp**

Context

config>service>vpls

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables proxy-ARP in an VPLS service.

On the 7210 SAS, users can enable or disable proxy-ARP commands for all EVPN services configured on the node; however, the option to enable or disable proxy-ARP per service is not available.

To enable or disable proxy-ARP capability, use the **config>service>system>evpn-proxy-arp-nd** command.

The **no** form of this command removes the proxy-ARP context.

Note: If the **config>service>system>evpn-proxy-arp-nd** command is configured, it must be disabled to run the **no proxy-arp** command. See Configuration guidelines for proxy-ARP and proxy-ND for more information.

Default

no proxy-arp

proxy-nd

Syntax

[**no**] **proxy-nd**

Context

config>service>vpls

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables proxy-ND in a VPLS service.

On the 7210 SAS, users can enable or disable proxy-ND commands for all EVPN services configured on the node; however, the option to enable or disable proxy-ND per service is not available.

To enable or disable proxy-ND capability, use the **config>service>system>evpn-proxy-arp-nd** command.

The **no** form of this command removes the proxy-ND context.

Note: If the **config>service>system>evpn-proxy-arp-nd** command is configured, the **no proxy-nd** command cannot be run. See Configuration guidelines for proxy-ARP and proxy-ND for more information.

Default

no proxy-nd

age-time

Syntax

age-time *seconds*

no age-time

Context

config>service>vpls>proxy-arp

config>service>vpls>proxy-nd

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command specifies the aging timer per proxy-ARP and proxy-ND entry for dynamic entries. When the aging expires, the entry is flushed. The age is reset when a new ARP, GARP, or NA for the same MAC-IP is received.

If the corresponding FDB MAC entry is flushed, the proxy-ARP or proxy-ND entry becomes inactive and subsequent ARP or NS lookups are treated as "missed". EVPN withdraws the IP-to-MAC if the entry becomes inactive. The **age-time** should be set at the **send-refresh** *seconds* value * 3 to ensure that no active entries are unnecessarily removed.

The **no** form of this command disables the aging timer.

Default

no age-time

Parameters

seconds

Specifies the aging time, in seconds.

Values 60 to 86400

dup-detect

Syntax

dup-detect [**anti-spoof-mac** *mac-address*] **window** *minutes* **num-moves** *count* **hold-down** [*minutes* | **max**]

Context

config>service>vpls>proxy-arp

config>service>vpls>proxy-nd

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables the mechanism that detects duplicate IPs and ARP/ND spoofing attacks. Attempts (relevant to dynamic and EVPN entry types) to add the same IP (different MAC) are monitored for **window** *minutes*. When *count* is reached within that **window**, the proxy-ARP or proxy-ND entry for the suspected IP is marked as duplicate. An alarm is also triggered. This condition is cleared when **hold-down** time expires (max does not expire) or a **clear** command is issued.

If the **anti-spoof-mac** keyword is configured, the proxy-ARP or proxy-ND MAC address of the offending entry is replaced with the configured anti-spoof *mac-address* and advertised in an unsolicited GARP/NA for local SAPs/SDP-bindings, and in EVPN to remote PEs. This mechanism assumes that the same **anti-spoof-mac** is configured in all the PEs for the same service, and that traffic with destination **anti-spoof-mac** received on SAPs/SDP-bindings are dropped. An ingress **mac-filter** may be configured to drop traffic to the **anti-spoof-mac**.

Default

dup-detect window 3 num-moves 5 hold-down 9

Parameters

window *minutes*

Specifies the window size, in minutes.

Values 1 to 15

Default 3

count

Specifies the number of moves required so that an entry is declared duplicate.

Values 3 to 10

Default 5

hold-down *minutes*

Specifies the hold-down time, in minutes, for a duplicate entry.

Values 2 to 60 | max

Default 9

mac-address

Specifies the MAC address to use as the optional anti-spoof-mac.

dynamic-arp-populate

Syntax

[**no**] **dynamic-arp-populate**

Context

config>service>vpls>proxy-arp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables the addition of dynamic entries to the proxy-ARP table.

When enabled, the system populates proxy-ARP entries from snooped GARP or ARP messages on SAPs/SDP-bindings. These entries are shown as dynamic.

When disabled, dynamic ARP entries are flushed from the proxy-ARP table. Enabling **dynamic-arp-populate** is only recommended in networks where this command is consistently configured in all PEs.

The **no** form of this command disables the addition of dynamic entries to the proxy-ARP table.

Default

no dynamic-arp-populate

dynamic-nd-populate

Syntax

[**no**] **dynamic-nd-populate**

Context

config>service>vpls>proxy-nd

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables the addition of dynamic entries to the proxy-ND table.

When enabled, the system populates proxy-ND entries from snooped Neighbor Advertisement (NA) messages on SAPs or SDP-bindings, in addition to the entries coming from EVPN (if the EVPN is enabled). These entries are shown as dynamic, and not as EVPN or static entries.

When disabled, dynamic ND entries are flushed from the proxy-ND table. Enabling **dynamic-nd-populate** is only recommended in networks where this command is consistently configured in all PEs.

The **no** form of this command disables the addition of dynamic entries to the proxy-ND table.

Default

no dynamic-nd-populate

evpn-nd-advertise

Syntax

evpn-nd-advertise {**host** | **router**}

Context

config>service>vpls>proxy-nd

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables the advertisement of static or dynamic entries that are learned as a host or router. Only one option (host or router) is possible in a specified service. This command also determines the R flag (host or router) when sending NA messages for existing EVPN entries in the proxy-ND table.

This command can only be modified if **proxy-nd** is shut down.

Default

evpn-nd-advertise router

Parameters

host

Keyword to enable the advertisement of static or dynamic entries that are learned as host.

router

Keyword to enable the advertisement of static or dynamic entries that are learned as routers.

garp-flood-evpn

Syntax

[**no**] **garp-flood-evpn**

Context

config>service>vpls>proxy-arp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command controls whether the system floods GARP-requests and GARP-replies to the EVPN. The GARPs impacted by this command are messages in which the sender IP is equal to the target IP and the MAC DA is broadcast.

The **no** form of this command only floods to local SAPs/SDP-bindings but not to EVPN destinations. The use of the **no** form is only recommended in networks where CEs are routers that are directly connected to the PEs. Networks using aggregation switches between the host/routers and the PEs should flood GARP messages in the EVPN to ensure that the remote caches are updated and the BGP does not miss the advertisement of these entries.

Default

garp-flood-evpn

host-unsolicited-na-flood-evpn

Syntax

[**no**] **host-unsolicited-na-flood-evpn**

Context

config>service>vpls>proxy-nd

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command controls whether the system floods host unsolicited Neighbor Advertisement (NA) messages to the EVPN. The NA messages with the following flag are impacted by this command:

- S=0
- R=0

The **no** form of this command only floods to local SAPs/SDP-bindings but not to the EVPN destinations. The use of the **no** form is only recommended in networks where CEs are routers that are directly connected to the PEs. Networks using aggregation switches between the host/routers and the PEs should flood unsolicited NA messages in the EVPN to ensure that the remote caches are updated and the BGP does not miss the advertisement of these entries.

Default

host-unsolicited-na-flood-evpn

router-unsolicited-na-flood-evpn

Syntax

[**no**] **router-unsolicited-na-flood-evpn**

Context

config>service>vpls>proxy-nd

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command controls whether the system floods router unsolicited NAs to EVPN. The NA messages impacted by this command are NA messages with the following flags:

- S=0
- R=1

The **no** form of this command only floods to local SAPs/SDP-bindings but not to EVPN destinations. This is only recommended in networks where CEs are routers directly connected to the PEs. Networks using aggregation switches between the host/routers and the PEs should flood unsolicited NA messages in EVPN to ensure that the remote caches are updated and the BGP does not miss the advertisement of these entries.

Default

router-unsolicited-na-flood-evpn

send-refresh

Syntax

send-refresh *seconds*

no send-refresh

Context

config>service>vpls>proxy-arp

config>service>vpls>proxy-nd

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables the system to send a refresh message at the configured time. A refresh message is an ARP-request message that uses 0s as the sender IP for the case of a proxy-ARP entry. For proxy-ND entries, a refresh is a regular NS message that uses the chassis MAC address as the MAC source address.

The **no** form of this command suppresses the refresh messages.

Default

no send-refresh

Parameters

seconds

Specifies the time to send a refresh message, in seconds.

Values 120 to 86400

static

Syntax

static *ip-address ieee-address*

no static *ip-address*

Context

config>service>vpls>proxy-arp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures static entries to be added to the table. A static MAC-IP entry requires the addition of the MAC address to the FDB as either learned or CStatic (conditional static MAC) to become active.

The **no** form of this command removes the specified static entry.

Parameters

ip-address

Specifies the IPv4 address for the static entry.

ieee-address

Specifies a 48-bit MAC address in the form xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx, where xx represents a hexadecimal number.

static

Syntax

static *ipv6-address ieee-address* {**host** | **router**}

no static *ipv6-address*

Context

config>service>vpls>proxy-nd

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures static entries to be added to the table. A static MAC-IP entry requires the addition of the MAC address to the FDB as either dynamic or CStatic (Conditional Static MAC) to become active. Along with the IPv6 and MAC address, the entry must also be configured as either host or router. This determines whether the received NS for the entry is replied with the R flag set to 1 (router) or 0 (host).

The **no** form of this command removes the specified static entry.

Parameters

ipv6-address

Specifies the IPv6 address for the static entry.

ieee-address

Specifies a 48-bit MAC address in the form xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx, where xx represents a hexadecimal number.

host

Specifies that the entry is type "host".

router

Specifies that the entry is type "router".

table-size

Syntax

table-size *table-size*

Context

config>service>vpls>proxy-arp

config>service>vpls>proxy-nd

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command adds a table-size limit per service. By default, the limit is 250; it can be set up to 16k entries per service. A non-configurable implicit high watermark of 95% and low watermark of 90% exists, per service and per system.

When those watermarks are reached, a syslog or trap is triggered. When the system or service limit is reached, entries for a specified IP can be replaced (a different MAC can be learned and added) but no new IP entries are added, regardless of the type (Static, evpn, dynamic). If the user attempts to change the *table-size* value to a value that cannot accommodate the number of existing entries, the attempt fails.

Default

table-size 250

Parameters

table-size

Specifies the table-size as the number of entries for the service.

Values 1 to 16384

unknown-arp-request-flood-evpn

Syntax

[**no**] **unknown-arp-request-flood-evpn**

Context

config>service>vpls>proxy-arp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command controls whether unknown ARP requests are flooded into the EVPN network. By default, the system floods ARP requests, including EVPN (with source squelching), if there is no active proxy-ARP entry for the requested IP.

The **no** form of this command only floods to local SAPs/SDP-bindings and not to EVPN destinations.

Default

unknown-arp-request-flood-evpn

unknown-ns-flood-evpn

Syntax

[**no**] **unknown-ns-flood-evpn**

Context

config>service>vpls>proxy-nd

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables unknown Neighbor Solicitation (NS) messages to be flooded into the EVPN network. By default, the system floods NS (with source squelching) to SAPs/SDP-bindings including EVPN, if there is no active proxy-ND entry for the requested IPv6.

The **no** form of this command only floods to local SAPs/SDP-bindings but not to EVPN destinations.

Default

unknown-ns-flood-evpn

shutdown

Syntax

[**no**] **shutdown**

Context

config>service>vpls>proxy-arp

config>service>vpls>proxy-nd

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables and disables the proxy-ARP and proxy-ND functionalities. ARP, GARP, and ND messages are snooped and redirected to the CPM for lookup in the proxy-ARP or proxy-ND table. The proxy-ARP or proxy-ND table is populated with IP-to-MAC pairs received from different sources (EVPN, static, dynamic). When the **shutdown** command is issued, the system stops snooping ARP or ND frames and the dynamic/EVPN dup proxy-ARP or proxy-ND table entries are flushed. All the static entries are kept in the table as "inactive", regardless of their previous "Status".

Note:
The **proxy-arp shutdown** and **no shutdown**, and **proxy-nd shutdown** and **no shutdown** commands cannot be executed if the **config>service>system>evpn-proxy-arp-nd** command is configured.

The **no** form of this command enables the proxy-ARP and proxy-ND functionalities.

Default

shutdown

ethernet-segment

Syntax

ethernet-segment *name* [**create**]

no ethernet-segment *name*

Context

config>service>system>bgp-evpn

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures an ES instance and its corresponding name.

The **no** form of this command deletes the specified ES.

Parameters

name

Specifies the ES name, up to 28 characters.

create

Keyword to create an ES.

es-activation-timer

Syntax

es-activation-timer *seconds*

no es-activation-timer

Context

config>service>system>bgp-evpn>ethernet-segment

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the ES activation timer for the specified **ethernet-segment**. The **es-activation-timer** delays the activation of a specified **ethernet-segment** on a specified PE that has been elected as DF (Designated Forwarder). Only when the **es-activation-timer** has expired, the SAP associated with an **ethernet-segment** can be activated (in case of single-active multi-homing) or added to the default-multicast-list (in case of all-active multi-homing).

The **no** form of this command specifies that the system uses the value in the **config>redundancy>bgp-evpn-multi-homing>es-activation-timer** context, if configured. Otherwise the system uses the default value of 3 seconds.

Default

no es-activation-timer

Parameters

seconds

Specifies the number of seconds for the **es-activation-timer**.

Values 0 to 100

Default 3

esi

Syntax

esi *value*

no esi

Context

config>service>system>bgp-evpn>ethernet-segment

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the 10-byte Ethernet segment identifier (ESI) associated with the Ethernet segment that is signaled in the BGP-EVPN routes. The ESI value cannot be changed unless the Ethernet segment is shut down. Reserved ESI values, 0 and MAX-ESI, are not allowed.

The **no** form of this command deletes the ESI from the Ethernet segment.

Default

no esi

Parameters

value

Specifies the 10-byte ESI in the form 00-11-22-33-44-55-66-77-88-99, using "-", ":", or " " as separators.

lag

Syntax

lag *lag-id*

no lag

Context

config>service>system>bgp-evpn>ethernet-segment

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures a lag ID associated with the ES When the **ethernet-segment** is configured as **all-active**, only a LAG can be associated with the ES. When the **ethernet-segment** is configured as **single-active**, a LAG or port can be associated with the ES. In either case, only one of the two objects can be configured in the ES. A specified LAG can be part of only one ES

The **no** form of this command removes the association of the Ethernet segment to LAG ports.

Default

no lag

Parameters

lag-id

Specifies the lag ID associated with the ES.

Values 1 to 800

multi-homing

Syntax

multi-homing single-active no-esi-label

no multi-homing

Context

config>service>system>bgp-evpn>ethernet-segment

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the multi-homing mode for the specified **ethernet-segment** as **single-active** multi-homing, as defined in RFC7432.

Note: The **esi-label** option cannot be enabled for **single-active**.

When **single-active no-esi-label** is specified, the system does not allocate an ESI label and advertise ESI label 0 to peers. The 7210 SAS does not use the ESI label received from a peer to send traffic to that peer.

The **multi-homing** command must be configured for the Ethernet segment to be enabled.

The **no** form of this command disables multi-homing on the Ethernet segment.

Default

no multi-homing

Parameters

single-active

Specifies single-active mode for the ES.

no-esi-label

Specifies that the system does not send an ESI label for **single-active** mode.

port

Syntax

port *port-id*

no port

Context

config>service>system>bgp-evpn>ethernet-segment

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures a port ID associated with the ES. If the **ethernet-segment** is configured as **single-active**, a LAG or port can be associated with the ES. In any case, only one of the two objects can be configured in the **ethernet-segment**. A specified port can be part of only one **ethernet-segment**. Only Ethernet ports can be added to an **ethernet-segment**.

The **no** form of this command removes the Ethernet segment association to all ports.

Default

no port

Parameters

port-id

Specifies the port ID associated with the ES.

Values *slot*/*mda*/*port* [.*channel*]

service-carving

Syntax

service-carving

Context

config>service>system>bgp-evpn>ethernet-segment

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

Commands in this context configure service-carving in the Ethernet segment. The service-carving algorithm determines the PE that is the Designated Forwarder (DF) in a specified ES and for a specific service.

manual

Syntax

manual

Context

config>service>system>bgp-evpn>eth-seg>service-carving

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

Commands in this context manually configure the service-carving algorithm; that is, configure the EVIs for which the PE is DF.

evi

Syntax

evi *start* [**to** *to*] **primary**

no evi *start*

Context

config>service>system>bgp-evpn>eth-seg>service-carving>manual

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the EVI ranges for which the PE is DF.

Note: Multiple individual EVI values and ranges are allowed. The PE is non-DF for the evi values not defined as **primary**.

The **no** form of this command removes the specified EVI range.

Parameters

start

Specifies the initial EVI value of the range for which the PE is DF.

Values 1 to 65535

to

Specifies the end EVI value of the range for which the PD is DF. If not configured, only the individual start value is considered.

Values 1 to 65535

primary

Specifies that the PE is DF for the configured EVI range.

mode

Syntax

mode {**manual** | **auto** | **off**}

Context

config>service>system>bgp-evpn>eth-seg>service-carving

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the **service-carving** mode. This determines how the DF is elected for a specified ES and service.

Default

mode auto

Parameters

auto

Specifies the service-carving algorithm defined in RFC 7432. The DF for the service is calculated based on the modulo function of the service (identified by either the EVI or the ISID) and the number of PEs.

manual

Specifies that the DF is elected based on the manual configuration added in the **service-carving>manual** context.

off

Specifies that all the services elect the same DF PE (assuming the same PEs are active for all the configured services). The PE with the lowest IP is elected as DF for the ES.

shutdown

Syntax

[**no**] **shutdown**

Context

config>service>system>bgp-evpn>ethernet-segment

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command changes the administrative status of the **ethernet-segment**.

The user can only configure **no shutdown** when **esi**, **multi-homing**, and **lag**/**port** are configured. If the ES or the corresponding **lag**/**port** are **shutdown**, the ES route and the AD per-ES routes are withdrawn. No changes are allowed when the **ethernet-segment** is **no shutdown**.

Default

shutdown

route-distinguisher

Syntax

route-distinguisher *rd*

no route-distinguisher

Context

config>service>system>bgp-evpn

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the route distinguisher (RD) that are signaled in EVPN Type 4 routes (Ethernet segment routes).

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

Default

no route-distinguisher

Parameters

rd

Specifies the route distinguisher in the following format.

ip-addr:*comm-val*

Values *ip-addr* — a.b.c.d

comm-val— 0 to 65535

Default system-ip: 0

redundancy

Syntax

redundancy

Context

config

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

Commands in this context configure the global redundancy parameters.

bgp-evpn-multi-homing

Syntax

bgp-evpn-multi-homing

Context

config>redundancy

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

Commands in this context configure the BGP-EVPN global timers.

boot-timer

Syntax

boot-timer *seconds*

Context

config>redundancy>bgp-evpn-multi-homing

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

When the PE boots up, the **boot-timer** allows the necessary time for the control plane protocols to come up before bringing up the Ethernet segments and running the DF algorithm.

The following considerations apply to the functionality:

- The boot-timer is configured at the system level. The configured value must provide enough time to allow the node and the cards (if available) to come up and BGP sessions to come up before exchanging ES routes and running the DF election for each EVI.
- The boot-timer is synchronized across CPMs and is relative to the System UP-time; therefore the boot-timer is not subject to change or reset upon CPM switchover.
- The boot-timer is never interrupted (however, the **es-activation-timer** can be interrupted if there is a new event triggering the DF election).
- The boot-timer runs per EVI on the ES's in the system. While **system-up-time>boot-timer** is true, the system does not run the DF election for any EVI. When the boot-timer expires, the DF election for the EVI is run and if the system is elected DF for the EVI, the **es-activation-timer** kicks in.
- The system does not advertise ES routes until the boot timer has expired. This guarantees that the peer ES PEs do not run the DF election until the PE is ready to become the DF, if required.

Default

boot-timer 10

Parameters

seconds

Specifies the number of seconds for the boot-timer.

Values 0 to 600

es-activation-timer

Syntax

es-activation-timer *seconds*

Context

config>redundancy>bgp-evpn-multi-homing

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the global Ethernet segment activation timer. The **es-activation-timer** delays the activation of a specified Ethernet segment on a specified PE that has been elected as the DF (Designated Forwarder). Only when the **es-activation-timer** has expired, can the SAP/SDP-binding associated with an Ethernet segment be activated (in case of single-active multi-homing) or added to the default-multicast-list (in case of all-active multi-homing).

The **es-activation-timer** configured at the Ethernet-segment level supersedes this global **es-activation-timer**.

Default

es-activation-timer 3

Parameters

seconds

Specifies the number of seconds for the **es-activation-timer**.

Values 0 to 100

4.5.2.2 EVPN show commands

evpn-mpls

Syntax

evpn-mpls

Context

show>service

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays the remote EVPN-MPLS tunnel endpoints in the system.

Output

The following output is an example of EVPN MPLS tunnel endpoint information, and Table 40: Output fields: EVPN MPLS tunnel endpoints describes the output fields.

Sample output

```
*A:Dut-B# show service evpn-mpls
===========================================================
EVPN MPLS Tunnel Endpoints
===========================================================
EvpnMplsTEP Address EVPN-MPLS Dest      ES Dest
-----------------------------------------------------------
10.20.1.3           1                   0
10.20.1.4           1                   0
10.20.1.5           1                   0
-----------------------------------------------------------
Number of EvpnMpls Tunnel Endpoints: 3
-----------------------------------------------------------
===========================================================
```

Table 40: Output fields: EVPN MPLS tunnel endpoints

Label	Description
EvpnMplsTEP	Displays the tunnel endpoint addresses
EVPN-MPLS Dest	Displays the number of EVPN-MPLS destinations
ES Dest	Displays the Ethernet segment destination

bgp-evpn

Syntax

bgp-evpn

Context

show>service>id

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays the **bgp-evpn** configured parameters for a specified service, including the administrative status of MPLS, the configuration for **mac-advertisement** and **unknown-mac-route**, as well as the **mac-duplication** parameters. The command shows the duplicate MAC addresses that **mac-duplication** has detected.

If the service is BGP-EVPN MPLS, the command also shows the parameters corresponding to EVPN-MPLS.

Output

The following output is an example of BGP EVPN information for a specified service, and Table 41: Output fields: service ID BGP-EVPN describes the output fields.

Sample output

```
*A:Dut-B# /show service id 1 bgp-evpn
===============================================================================
BGP EVPN Table
===============================================================================
MAC Advertisement  : Enabled
CFM MAC Advertise  : Disabled
MAC Dup Detn Moves : 5                  MAC Dup Detn Window: 3
MAC Dup Detn Retry : 9                  Number of Dup MACs : 0
EVI                : 1
-------------------------------------------------------------------------------
Detected Duplicate MAC Addresses             Time Detected
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
===============================================================================
===============================================================================
```

```
BGP EVPN MPLS Information
===============================================================================
Admin Status       : Enabled
Force Vlan Fwding  : Disabled           Control Word       : Disabled
Split Horizon Group: (Not Specified)
Ingress Rep BUM Lbl: Disabled           Max Ecmp Routes    : 0
Ingress Ucast Lbl  : 131069             Ingress Mcast Lbl  : 131069
===============================================================================
===============================================================================
BGP EVPN MPLS Auto Bind Tunnel Information
===============================================================================
Resolution         : any
Filter Tunnel Types: (Not Specified)
===============================================================================
```

Table 41: Output fields: service ID BGP-EVPN

Label	Description
BGP EVPN Table	
MAC Advertisement	Displays whether MAC advertisement is enabled or disabled
CFM MAC Advertise	Displays whether CFM MAC advertise is enabled or disabled
MAC Dup Detn Moves	Displays the number of moves that trigger MAC duplication detection
MAC Dup Detn Window	Displays the configured window size used for duplicate MAC detection
MAC Dup Detn Retry	Displays the retry timer value used for MAC duplication detection.
Number of Dup MACs	Displays the number of duplicate MAC addresses
EVI	Displays the EVPN instance ID
BGP EVPN MPLS Information	
Admin Status	Displays the administrative status of the EVPN MPLS
Force Vlan Fwding	Displays the status of force-vlan-forwarding
Control Word	Displays the status of control
Split Horizon Group	Displays the split-horizon group membership information
Ingress Rep BUM Lbl	Displays the label used for Ingress BUM replication
Max Ecmp Routes	Displays the maximum number of ECMP routes
Ingress Ucast Lbl	Displays the ingress unicast label
Ingress Mcast Lbl	Displays the ingress multicast label
BGP EVPN MPLS Auto Bind Tunnel Information	

Label	Description
Resolution	Displays the transport tunnel resolution filter used
Filter Tunnel Types	Displays auto-bind-tunnel resolution filter values, if applicable

evpn-mpls

Syntax

evpn-mpls

evpn-mpls esi *esi*

Context

show>service>id

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays the existing EVPN-MPLS destinations for a specified service and all related information. The command allows filtering based on **esi** (for EVPN multi-homing) to display the EVPN-MPLS destinations associated with an Ethernet Segment Identifier (ESI).

Parameters

esi

Specifies a 10-byte ESI by which to filter the displayed information. For example, ESI-0 | ESI-MAX or 00-11-22-33-44-55-66-77-88-99 with any of these separators ('-',':',' ')

Output

The following output is an example of EVPN MPLS information, and Table 42: Output fields: EVPN MPLS describes the output fields.

Sample output

```
*A:Dut-B# /show service id 1 evpn-mpls
===============================================================================
BGP EVPN-MPLS Dest
===============================================================================
TEP Address     Egr Label     Num. MACs   Mcast           Last Change
                 Transport
-------------------------------------------------------------------------------
10.20.1.3       131069        0           Yes             02/02/2014 15:29:40
                rsvp
10.20.1.4       131069        0           Yes             02/02/2014 15:29:33
                rsvp
10.20.1.5       131059        0           Yes             02/02/2014 15:29:42
                rsvp
-------------------------------------------------------------------------------
Number of entries : 3
```

```
-------------------------------------------------------------------------------
===============================================================================
===============================================================================
BGP EVPN-MPLS Ethernet Segment Dest
===============================================================================
Eth SegId                       Num. Macs              Last Change
-------------------------------------------------------------------------------
00:de:01:00:00:00:00:00:00:01   1                      02/02/2014 15:47:04
-------------------------------------------------------------------------------
Number of entries: 1
-------------------------------------------------------------------------------
*A:PE-1# show service id 2 evpn-mpls esi 00:10:00:00:00:00:00:00:00:00
```

Table 42: Output fields: EVPN MPLS

Label	Description
TEP Address	Displays the TEP address
Egr Label	Displays the egress label
Transport	Displays the transport type
Number of entries	Indicates the number of entries
Eth SegId	Displays the Ethernet segment ID
Transport:Tnl-Id	Displays the tunnel type and tunnel ID of the EVPN-MPLS entry
Transport:Tnl	Displays the transport tunnel
Num. MAC	Displays the number of MACs
Mcast	Displays the multicast information
Sup BCast Domain	Displays the Sup BCast Domain

proxy-arp

Syntax

proxy-arp [*ip-address*] [**detail**]

Context

show>service>id

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays, in a table, the existing proxy-ARP entries for a specified service. The table is populated by EVPN MAC routes that contain a MAC and an IP address, as well as static entries or dynamic entries from snooped ARP messages on access SAPs.

A 7210 SAS that receives an ARP request from a SAP performs a lookup in the proxy-ARP table for the service. If a match is found, the router replies to the ARP and does not allow ARP flooding in the VPLS service. If a match is not found, the ARP is flooded within the service if the configuration allows it.

The command allows for specific IP addresses to be displayed. Dynamic IP entries associated with a MAC list are displayed with the corresponding MAC list and resolve timers information.

Parameters

ip-address

Specifies an IP address.

Values a.b.c.d

detail

Displays detailed information.

Output

The following output is an example of proxy-ARP information for a specified service, and Table 43: Output fields: proxy-ARP describes the output fields.

Sample output

```
show service id 1 proxy-arp detail
-------------------------------------------------------------------------------
Proxy Arp
-------------------------------------------------------------------------------
Admin State       : enabled
Dyn Populate      : enabled
Age Time          : disabled            Send Refresh      : disabled
Table Size        : 16383               Total             : 2
Static Count      : 0                   EVPN Count        : 1
Dynamic Count     : 1                   Duplicate Count   : 0
Dup Detect
-------------------------------------------------------------------------------
Detect Window     : 3 mins              Num Moves         : 5
Hold down         : 9 mins
Anti Spoof MAC    : None
EVPN
-------------------------------------------------------------------------------
Garp Flood        : disabled            Req Flood         : enabled
-------------------------------------------------------------------------------
===============================================================================
VPLS Proxy Arp Entries
===============================================================================
IP Address          Mac Address         Type      Status    Last Update
-------------------------------------------------------------------------------
10.1.1.1            00:00:00:00:00:01   dyn       active    03/13/2020 10:25:39
10.1.1.10           00:00:00:00:00:11   evpn      active    03/13/2020 10:25:40
-------------------------------------------------------------------------------
Number of entries : 2
===============================================================================
```

Table 43: Output fields: proxy-ARP

Label	Description
Admin State	Displays the admin state: enabled or disabled
Dyn Populate	Displays the status of the ARP dynamic population
Age Time	Displays the configured ARP age timer
Send Refresh	Displays the configured ARP refresh timer
Table Size	Displays the configured ARP table size
Total	Displays the total table used count
Static Count	Displays the static ARP entries count
EVPN Count	Displays the count of ARP entries learned through the EVPN tunnel
Dynamic Count	Displays the count of ARP entries dynamically learned
Duplicate Count	Displays the count of ARP duplicate entries
Detect Window	Displays the configured window value for ARP duplicate detection
Num Moves	Displays the configured count for number of moves used for ARP duplicate detection
Hold Down	Displays the hold-down timer used by ARP duplicate detection
Anti Spoof MAC	Displays the MAC address configured for anti-spoof detection
Garp Flood	Displays the status for GARP flooding
Req Flood	Displays the status of ARP request flooding
IP Address	Displays the IP address of the proxy-ARP entry
Mac Address	Displays the MAC address of the proxy-ARP entry
Type	Displays the type of ARP entry
Status	Displays the status
Last Update	Displays the date and time of the last update

proxy-nd

Syntax

proxy-nd [*ipv6-address*] [**detail**]

Context

show>service>id

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays, in a table, the existing proxy-ND entries for a specified service. The table is populated by the EVPN MAC routes containing a MAC and an IPv6 address, as well as static entries or dynamic entries from snooped NA messages on access SAPs.

A 7210 SAS that receives a Neighbor Solicitation (NS) from a SAP performs a lookup in the proxy-ND table for the service. If a match is found, the router replies to the NS and does not allow NS flooding in the VPLS service. If a match is not found, the NS is flooded in the service, if the configuration allows it.

This command allows specific IPv6 addresses to be displayed. Dynamic IPv6 entries associated with a MAC list are shown with the corresponding MAC list and resolve timer information.

Parameters

ipv6-address

Specifies an IPv6 address.

Values ipv6-address:

x:x:x:x:x:x:x:x (eight 16-bit pieces)

x:x:x:x:x:x:d.d.d.d

where:

x - [0 to FFFF]H

d - [0 to 255]D

detail

Displays detailed information.

Output

The following output is an example of proxy-ND information for a specified service, and Table 44: Output fields: proxy-ND displays the output fields.

Sample output

```
A:Dut-C# show service id 1 proxy-nd detail
-------------------------------------------------------------------------------
Proxy ND
-------------------------------------------------------------------------------
```

```
Admin State       : enabled
Dyn Populate      : enabled
Age Time          : disabled            Send Refresh      : disabled
Table Size        : 250                 Total             : 1
Static Count      : 0                   EVPN Count        : 0
Dynamic Count     : 1                   Duplicate Count   : 0
Dup Detect
-------------------------------------------------------------------------------
Detect Window     : 3 mins              Num Moves         : 5
Hold down         : 9 mins
Anti Spoof MAC    : None
EVPN
-------------------------------------------------------------------------------
Unknown NS Flood  : enabled             ND Advertise      : Router
Rtr Unsol NA Flood: disabled            Host Unsol NA Fld : disabled
-------------------------------------------------------------------------------
===============================================================================
VPLS Proxy ND Entries
===============================================================================
IP Address               Mac Address       Type Status Rtr/ Last Update
                                                      Host
-------------------------------------------------------------------------------
2000::4                  00:00:00:00:00:04 dyn  active Rtr  01/14/2020 09:47:43
-------------------------------------------------------------------------------
Number of entries : 1*A:PE-2#  show service id 5 proxy-nd
```

Table 44: Output fields: proxy-ND

Label	Description
Admin State	Displays the admin state for proxy-ND: enabled or disabled
Dyn Populate	Displays the status for dynamic populate
Age Time	Displays the aging timer for ND entries
Send Refresh	Displays the refresh timer for ND entries
Table Size	Displays the proxy-ND table size
Total	Displays the count of learned ND entries
Static Count	Displays the count of static ND entries
EVPN Count	Displays the count of ND entries learned from the EVPN binding
Dynamic Count	Displays the count of dynamically learned ND entries
Duplicate Count	Displays the count of duplicate ND entries
Detect Window	Displays the configured value for window size used for duplicate detection
Num Moves	Displays the configured value for number of moves used in duplicate ND detection
Hold Down	Displays the value of the hold-down timer

Label	Description
Anti Spoof MAC	Displays the configured anti-spoof MAC address
Unknown NS Flood	Displays the state of unknown Neighbor Solicitation messages that are flooded to the EVPN network
ND Advertise	Displays the advertisement of static or dynamic entries that are learned as hosts or routers
Rtr Unsol NA Flood	Displays the state of system floods router unsolicited Neighbor Advertisements to EVPN
Host Unsol NA Fld	Displays the state of system floods host unsolicited Neighbor Advertisements to EVPN
IP Address	Displays the IP address of the proxy-ND entry
Mac Address	Displays the MAC address of the proxy-ND entry
Type	Displays the type of ND entry
Status	Displays the status of the ND entry
Last Update	Displays the date and time of the last update

system

Syntax

system

Context

show>service

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

Commands in this context configure the **system** BGP EVPN show command.

bgp-evpn

Syntax

bgp-evpn

Context

show>service>system

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command shows system BGP EVPN information.

Output

The following output is an example of system BGP EVPN information, and Table 45: Output fields: system BGP-EVPN describes the output fields.

Sample output

```
*A:Dut-B# /show service system bgp-evpn
===============================================================================
System BGP EVPN Information
===============================================================================
Evpn Route Dist.                      : <none>
Oper Route Dist.                      : 10.20.1.2:0
Oper Route Dist Type                  : default
===============================================================================
```

Table 45: Output fields: system BGP-EVPN

Label	Description
Evpn Route Dist.	Displays the EVPN route distinguisher
Oper Route Dist.	Displays address of the operational route distinguisher
Oper Route Dist Type	Displays the operational route distinguisher type

redundancy

Syntax

redundancy

Context

show

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

Commands in this context display the global redundancy parameters.

bgp-evpn-multi-homing

Syntax

bgp-evpn-multi-homing

Context

show>redundancy

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays information related to the EVPN global timers.

Output

The following output is an example of BGP EVPN multi-homing information, and Table 46: Output fields: BGP-EVPN multi-homing displays the output fields.

Sample output

```
*A:Dut-B# show redundancy bgp-evpn-multi-homing
===============================================================================
Redundancy BGP EVPN Multi-homing Information
===============================================================================
Boot-Timer              : 10 secs
Boot-Timer Remaining    : 0 secs
ES Activation Timer     : 3 secs
===============================================================================
```

Table 46: Output fields: BGP-EVPN multi-homing

Label	Description
Boot-Timer	Displays the value configured for the boot timer
Boot-Timer Remaining	Displays the amount of time remaining on the boot timer
ES Activation Timer	Displays the value configured for the ES activation timer

4.5.2.3 EVPN clear commands

proxy-arp

Syntax

proxy-arp [**duplicate**] [**dynamic**]

Context

clear>service>id

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command clears all entries in the proxy-ARP table if none of the optional parameters is specified. If the duplicate parameter is specified it clears all the duplicate entries in the proxy-ARP table. If the dynamic parameter is specified it clears all the dynamic entries in the proxy-ARP table.

Parameters

duplicate

Clears the proxy ARP duplicate entries.

dynamic

Clears the proxy ARP dynamic entries.

proxy-nd

Syntax

proxy-nd [**duplicate**] [**dynamic**]

Context

clear>service>id

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command clears all entries in the proxy-ND table if none of the optional parameters is specified. If the duplicate parameter is specified it clears all the duplicate entries in the hold-down state from the proxy-ND table. If the dynamic parameter is specified it clears all the dynamic entries in the hold-down state from the proxy-ND table.

Parameters

duplicate

Clears the proxy ND duplicate entries.

dynamic

Clears the proxy ND dynamic entries.

4.5.2.4 Tools commands

service

Syntax

service

Context

tools>dump

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures tools to display service dump information.

usage

Syntax

usage

Context

tools>dump>service>proxy-arp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command provides information about the usage and limit of the system-wide proxy-ARP table for all the services. The command also shows if the limit has been exceeded and a trap raised.

Output

The following output is an example of **tools dump service proxy-arp** usage information.

Sample output

```
*A:Dut# tools dump service proxy-arp usage
Proxy arp Usage
            Current Usage       :         10
            System Limit        :     16384
      High Usage Trap Raised:       No
            High Usage Threshold:         95 percent
            High Usage Clear Threshold:   90 percent
```

usage

Syntax

usage

Context

tools>dump>service>proxy-nd

Platforms

Supported on all 7210 SAS platforms as described in this document, except 7210 SAS-R6 IMM

Description

This command provides information about the usage and limit of the system-wide proxy-ND table for all the services. The command also shows if the limit has been exceeded and a trap raised.

Output

The following output is an example of **tools dump service proxy-nd** usage information.

Sample output

```
*A:Dut# tools dump service proxy-nd usage
Proxy nd Usage
            Current Usage       :        211
            System Limit        :     16384
       High Usage Trap Raised:       No
            High Usage Threshold:         95 percent
            High Usage Clear Threshold:   90 percent
```

5 Virtual Private LAN Service

This chapter provides information about Virtual Private LAN Service (VPLS), process overview, and implementation notes.

5.1 VPLS service overview

Virtual Private LAN Service (VPLS) is a class of virtual private network service that allows the connection of multiple sites in a single bridged domain over a provider-managed IP/MPLS network. The customer sites in a VPLS instance appear to be on the same LAN, regardless of their location. VPLS uses an Ethernet interface on the customer-facing (access) side which simplifies the LAN/WAN boundary and allows for rapid and flexible service provisioning. The 7210 SAS supports provisioning of access or uplink spokes to connect to the provider edge IP/MPLS routers.

VPLS provides a balance between point-to-point Frame Relay service and outsourced routed services (VPRN). VPLS enables each customer to maintain control of their own routing strategies. All customer routers in the VPLS service are part of the same subnet (LAN) which simplifies the IP addressing plan, especially when compared to a mesh constructed from many separate point-to-point connections. The VPLS service management is simplified because the service is not aware of nor participates in the IP addressing and routing.

A VPLS service provides connectivity between two or more SAPs on one (which is considered a local service) or more (which is considered a distributed service) service routers. The connection appears to be a bridged domain to the customer sites so protocols, including routing protocols, can traverse the VPLS service.

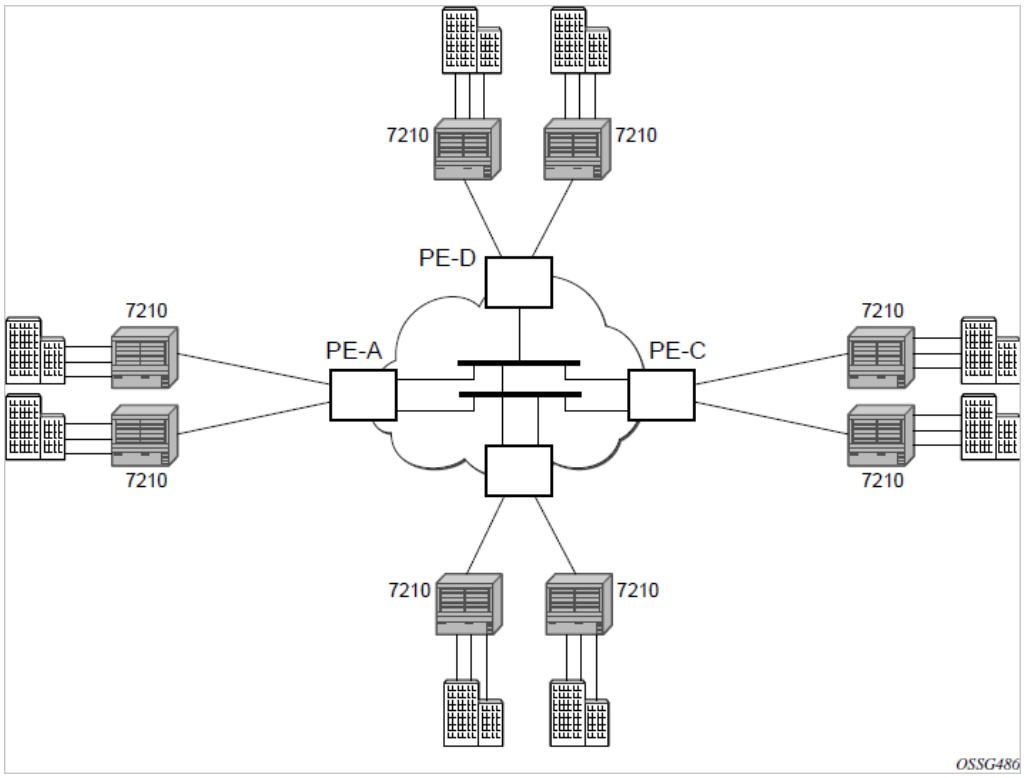
Other VPLS advantages include:

- VPLS is a transparent, protocol-independent service.
- There is no Layer 2 protocol conversion between LAN and WAN technologies.
- There is no need to design, manage, configure, and maintain separate WAN access equipment, therefore, eliminating the need to train personnel on WAN technologies such as Frame Relay.

5.1.1 VPLS packet walkthrough

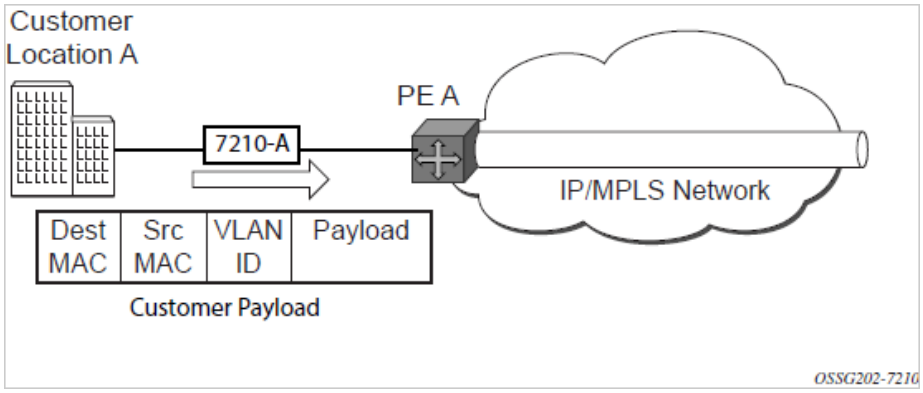
This section provides an example of VPLS processing of a customer packet sent across the network from site-A, which is connected to PE-Router-A through a 7210 SAS to site-C, which is connected through 7210 SAS to PE-Router-C (shown in the following figure) in an H-VPLS configuration. This section does not describe the processing on the PE routers, but only on 7210 SAS routers:

Figure 48: VPLS service architecture



1. 7210-A (shown in the following figure)
   a. Service packets arriving at are associated with a VPLS service instance based on the combination of the physical port and the IEEE 802.1Q tag (VLAN-ID) in the packet.

      Figure 49: Access port ingress packet format and lookup



   b. 7210-A learns the source MAC address in the packet and creates an entry in the FIB table that associates the MAC address to the service access point (SAP) on which it was received.
   c. The destination MAC address in the packet is looked up in the FIB table for the VPLS instance. There are two possibilities: either the destination MAC address has already been learned (known MAC address) or the destination MAC address is not yet learned (unknown MAC address). For a

Known MAC Address (Figure 50: Network port egress packet format and flooding Customer Location A).

d. If the destination MAC address has already been learned by 7210, an existing entry in the FIB table identifies the far-end PE-Router and the service VC-label (inner label) to be used before sending the packet to PE-Router-A.

e. The 7210 SAS chooses a transport LSP to send the customer packets to PE-Router-A. The customer packet is sent on this LSP when the IEEE 802.1Q tag is stripped and the service VC-label (inner label) and the transport label (outer label) are added to the packet. For an Unknown MAC Address (Figure 51: Network port egress packet format and flooding).

f. If the destination MAC address has not been learned, 7210 floods the packet to spoke-SDPs that are participating in the service.

Figure 50: Network port egress packet format and flooding Customer Location A

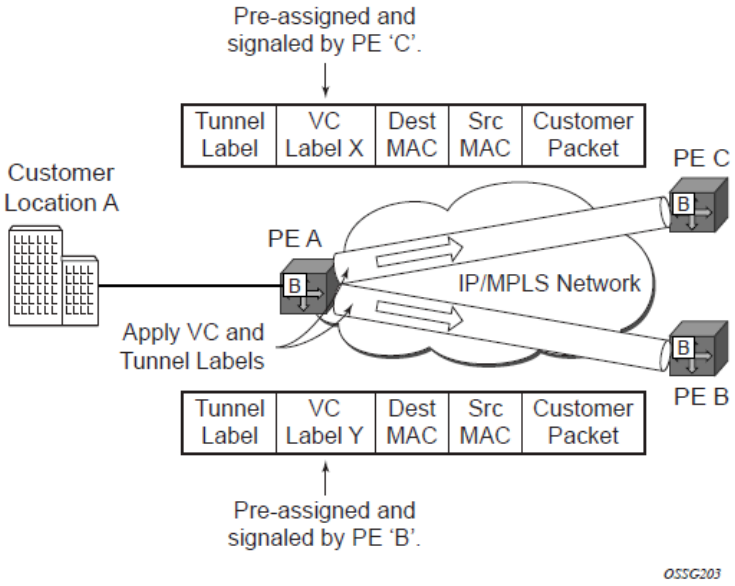
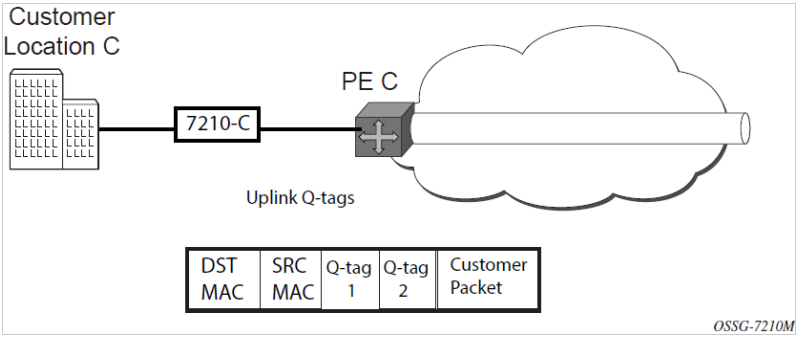


Figure 51: Network port egress packet format and flooding



2. Core Router Switching

All the core routers ('P' routers in IETF nomenclature) between PE-Router-A and PE-Router-B and PE-Router-C are Label Switch Routers (LSRs) that switch the packet based on the transport (outer) label of the packet until the packet arrives at far-end PE-Router. All core routers are unaware that this traffic is associated with a VPLS service.

3. 7210-C (Figure 49: Access port ingress packet format and lookup)
   a. 7210-C associates the packet with the VPLS instance based on the VC label in the received packet after the stripping of the tunnel label.
   b. 7210-C learns the source MAC address in the packet and creates an entry in the FIB table that associates the MAC address to the spoke-SDP on which the packet was received.
   c. The destination MAC address in the packet is looked up in the FIB table for the VPLS instance. Again, there are two possibilities: either the destination MAC address has already been learned (known MAC address) or the destination MAC address has not been learned on the access side of 7210-C (unknown MAC address).
   d. If the destination MAC address has been learned by an existing entry in the FIB table identifies the local access port and the IEEE 802.1Q tag to be added before sending the packet to customer Location-C. The egress Q tag may be different from the ingress Q tag.
   e. If the destination MAC address has not been learned, 7210 floods the packet to all the access SAPs that are participating in the service.

5.2 VPLS features

This section describes VPLS features.

5.2.1 VPLS enhancements

The Nokia VPLS implementation includes several enhancements beyond basic VPN connectivity. The following VPLS features can be configured individually for each VPLS service instance:

- Extensive MAC and IP filter support (up to Layer 4). Filters can be applied on a per SAP basis.
- Forwarding Information Base (FIB) management features including:
  - Configurable FIB size limit
  - FIB size alarms
  - MAC learning disable
  - Discard unknown
  - Separate aging timers for locally and remotely learned MAC addresses.
- Ingress rate limiting for broadcast, multicast, and destination unknown flooding on a per SAP basis.
- Implementation of Spanning Tree Protocol (STP) parameters on a per VPLS, per SAP and per spoke-SDP basis.
- Optional SAP and spoke-SDP redundancy to protect against node failure.
- IGMP snooping on a per-SAP and SDP basis.

5.2.2 VPLS over MPLS

The VPLS architecture proposed in *draft-ietf-ppvpn-vpls-ldp-0x.txt* specifies the use of provider equipment (PE) that is capable of learning, bridging, and replication on a per-VPLS basis. The PE routers that participate in the service are connected using MPLS Label Switched Path (LSP) tunnels in a full-mesh composed of mesh SDPs or based on an LSP hierarchy (Hierarchical VPLS (H-VPLS)) composed of mesh SDPs and spoke SDPs. The 7210 SAS supports only H-VPLS.

Multiple VPLS services can be offered over the same set of LSP tunnels. Signaling specified in *RFC 4905* is used to negotiate a set of ingress and egress VC labels on a per-service basis. The VC labels are used by the PE routers for de-multiplexing traffic arriving from different VPLS services over the same set of LSP tunnels.

H-VPLS is provided over MPLS by:

- connecting the 7210 SAS-R6 and 7210 SAS-R12 to bridging-capable provider edge (PE) routers through a spoke-SDP. The PE routers are connected using a full mesh of LSPs.
- negotiating per-service VC labels using draft-Martini encapsulation
- replicating unknown and broadcast traffic in a service domain
- enabling MAC learning over tunnel and access ports (see VPLS MAC learning and packet forwarding).
- using a separate forwarding information base (FIB) per VPLS service

5.2.3 VPLS MAC learning and packet forwarding

The 7210 SAS edge devices perform the packet replication required for broadcast and multicast traffic across the bridged domain. MAC address learning is performed by the 7210 SAS device to reduce the amount of unknown destination MAC address flooding.

Each 7210 SAS maintains a Forwarding Information Base (FIB) for each VPLS service instance and learned MAC addresses are populated in the FIB table of the service. All traffic is switched based on MAC addresses and forwarded between all participating nodes using the LSP tunnels. Unknown destination packets (for example, the destination MAC address has not been learned) are forwarded on all LSPs to all participating nodes for that service until the target station responds and the MAC address is learned by the 7210 SAS associated with that service.

5.2.4 Configuration notes for VPLS forwarding

The 7210 SAS-R6 and 7210 SAS-R12 devices, uses the packet header fields that computes the hash for unicast traffic to be sent out of a SAP configured over a LAG and forwards it over the member ports of the LAG. For unknown unicast, broadcast and multicast traffic, it does not compute a hash and forwards all traffic out of the primary port of the LAG. For more information, see the *7210 SAS-Mxp, R6, R12, S, Sx, T Interface Configuration Guide*.

5.2.5 IGMP snooping in VPLS service

Note: This section provides information about IGMP snooping support in a VPLS service. It does not apply to routed VPLS (R-VPLS) services. IGMP snooping can also be enabled for routed VPLS services. See Routed VPLS and IGMPv3 snooping for details.

In Layer 2 switches, multicast traffic is treated like an unknown MAC address or broadcast frame, which causes the incoming frame to be flooded out (broadcast) on every port within a VLAN. Although this is acceptable behavior for unknowns and broadcast frames, this flooded multicast traffic may result in wasted bandwidth on network segments and end stations, as IP multicast hosts can join and be interested in only specific multicast groups.

IGMP snooping entails using information in Layer 3 protocol headers of multicast control messages to determine the processing at Layer 2. By doing so, an IGMP snooping switch provides the benefit of conserving bandwidth on those segments of the network in which no node has expressed interest in receiving packets addressed to the group address.

IGMP snooping can be enabled in the context of VPLS services. The IGMP snooping feature allows for optimization of the multicast data flow to only those SAPs or SDPs that are members of the group. The system builds a database of group members per service by listening to IGMP queries and reports from each SAP or SDP, as follows:

- When the switch receives an IGMP report from a host for a particular multicast group, the switch adds the host port number to the forwarding table entry.
- When it receives an IGMP leave message from a host, it removes the host port from the table entry, if no other group members are present. It also deletes entries if it does not receive periodic IGMP membership reports from the multicast clients.

The following are IGMP snooping features:

- IGMP v1, v2, and v3 are supported (RFC 1112, *Host Extensions for IP Multicasting*, and RFC 2236, *Internet Group Management Protocol, Version 2*).
- IGMP snooping can be enabled and disabled on individual VPLS service instances.
- IGMP snooping can be configured on individual SAPs that are part of a VPLS service. When IGMP snooping is enabled on a VPLS service, all its contained SAPs and SDPs automatically have snooping enabled.
- Fast leave terminates the multicast session immediately instead of using the standard group-specific query to check if other group members are present on the network.
- SAPs and SDPs can be statically configured as multicast router ports. This allows the operator to control the set of ports to which IGMP membership reports are forwarded.
- Static multicast group membership on a per SAP and as per SDP basis can be configured.
- The maximum number of multicast groups (static and dynamic) that a SAP or SDP can join can be configured. An event is generated when the limit is reached.
- The maximum number of multicast groups (static and dynamic) that a VPLS instance simultaneously supports can be configured.
- Proxy summarization of IGMP messages reduces the number of IGMP messages processed by upstream devices in the network.
- IGMP filtering allows a subscriber to a service or the provider to block, receive, or transmit permission (or both) to individual hosts or a range of hosts. The following types of filters can be defined:

– Filter group membership that report from a particular host or range of hosts. This filtering is performed by importing an appropriately-defined routing policy into the SAP or SDP.
– Filters that prevent a host from transmitting multicast streams into the network. The operator can define a data-plane filter (ACL) that drops all multicast traffic, and apply this filter to a SAP or SDP.

5.2.5.1 Configuration guidelines for IGMP snooping in VPLS service

The following IGMP snooping considerations apply:

- Layer 2 multicast is supported in VPLS services.
- IGMP snooping is not supported for VCs (either VC-Ether or VC-VLAN) with control-word enabled.
- IGMP snooping fast leave processing can be enabled only on SAPs and SDPs. IGMP snooping proxy summarization is enabled by default on SAPS and SDPs and cannot be disabled. Proxy summarization and fast leave processing are supported only on SDPs whose VC are configured to use vc-type ether and do not have control-word enabled.
- IGMP filtering using policies is available on SAPs and SDPs. It is supported only on SDPs whose VC are configured to use vc-type ether and do not have control-word enabled.
- Dynamic learning is only supported on SDPs whose VC are configured to use vc-type ether and do not have control-word enabled.
- SDPs that are configured to use VC of type vc-vlan that need to be router ports must be configured statically. Multicast group memberships for such SDPs must be configured statically. Dynamic learning is not available for these SDPs.
- IGMP snooping is not supported for control word-enabled SDPs.

5.2.6 Multicast VLAN Registration (MVR) support in VPLS service

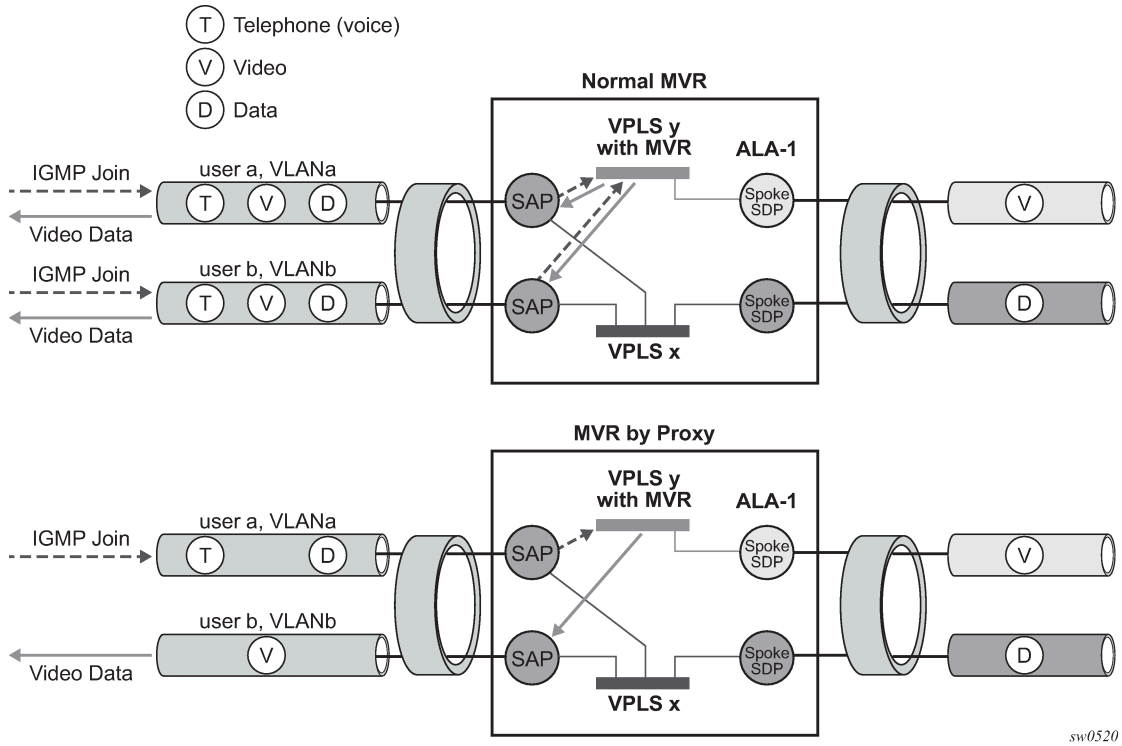
Multicast VPLS Registration (MVR) is a bandwidth optimization method for multicast in a broadband services network. MVR allows a subscriber on a port to subscribe and unsubscribe to a multicast stream on one or more network-wide multicast VPLS instances.

MVR assumes that subscribers join and leave multicast streams by sending IGMP join and leave messages. The IGMP leave and join message are sent inside the VPLS to which the subscriber port is assigned. The multicast VPLS is shared in the network while the subscribers remain in separate VPLS services. Using MVR, users on different VPLS cannot exchange any information between them, but still multicast services are provided.

On the MVR VPLS, IGMP snooping must be enabled. On the user VPLS, IGMP snooping and MVR work independently. If IGMP snooping and MVR are both enabled, MVR reacts only to join and leave messages from multicast groups configured under MVR. Join and leave messages from all other multicast groups are managed by IGMP snooping in the local VPLS. This way, potentially several MVR VPLS instances could be configured, each with its own set of multicast channels.

MVR by proxy — In some situations, the multicast traffic should not be copied from the MVR VPLS to the SAP on which the IGMP message was received (standard MVR behavior) but to another SAP. This is called MVR by proxy and is shown in the following figure.

Figure 52: MVR and MVR by proxy



5.2.6.1 Configuration guidelines for MVR in VPLS service

In a MVR configuration, the **svc-sap-type** of the VPLS service that is the source (also known as MVR VPLS service) and the **svc-sap-type** of the VPLS service that is the sink (also known as user VPLS service) should match.

5.2.7 Layer 2 forwarding table management

The following sections describe VPLS features related to management of the Forwarding Information Base (FIB).

5.2.7.1 FIB size

MAC FIB size limits is a required MAC table management feature for each instance of a SAP or spoke-SDP within a particular VPLS service instance. It allows users to specify the maximum number of MAC FIB entries that are learned locally for a SAP or remotely for a spoke-SDP. If the configured limit is reached, then no new addresses are learned from the SAP or spoke-SDP until at least one FIB entry is aged out or cleared, as follows:

- When the limit is reached on a SAP, packets with unknown source MAC addresses are still forwarded (this default behavior can be changed by configuration). By default, if the destination MAC address is known, it is forwarded based on the FIB, and if the destination MAC address is unknown, it is flooded.

Alternatively, if discard unknown is enabled at the VPLS service level, unknown destination MAC addresses are discarded.

- The log event SAP MAC limit reached is generated when the limit is reached. When the condition is cleared, the log event SAP MAC Limit Reached Condition Cleared is generated.
- Disable learning at the VPLS service level allows users to disable the dynamic learning function on the service. Disable Learning is supported at the SAP and spoke-SDP level as well.
- Disable aging allows users to turn off aging for learned MAC addresses. It is supported at the VPLS service level, SAP level and spoke-SDP level.

5.2.7.2 FIB size alarms

The size of the VPLS FIB can be configured with a low watermark and a high watermark, expressed as a percentage of the total FIB size limit. If the actual FIB size grows above the configured high watermark percentage, an alarm is generated. If the FIB size falls below the configured low watermark percentage, the alarm is cleared by the system.

5.2.7.3 Local and remote aging timers

Like a Layer 2 switch, learned MACs within a VPLS instance can be aged out if no packets are sourced from the MAC address for a specified period of time (the aging time). In each VPLS service instance, there are independent aging timers for locally learned MAC and remotely learned MAC entries in the forwarding database (FIB). A local MAC address is a MAC address associated with a SAP because it ingressed on a SAP. A remote MAC address is a MAC address received by an SDP from another router for the VPLS instance. The local-age timer for the VPLS instance specifies the aging time for locally learned MAC addresses, and the remote-age timer specifies the aging time for remotely learned MAC addresses.

In general, the remote-age timer is set to a longer period than the local-age timer to reduce the amount of flooding required for destination unknown MAC addresses. The aging mechanism is considered a low priority process. In most situations, the aging out of MAC addresses can happen in within tens of seconds beyond the age time. To minimize overhead, local MAC addresses on a LAG port and remote MAC addresses, in some circumstances, can take up to two times their respective age timer to be aged out.

5.2.7.4 Disable MAC aging

The MAC aging timers can be disabled which prevents any learned MAC entries from being aged out of the FIB. When aging is disabled, it is still possible to manually delete or flush learned MAC entries. Aging can be disabled for learned MAC addresses on a SAP or a spoke-SDP of a VPLS service instance.

5.2.7.5 Disable MAC learning

When MAC learning is disabled for a service, new source MAC addresses are not entered in the VPLS FIB. MAC learning can be disabled for individual SAPs or spoke-SDPs.

5.2.7.6 Unknown MAC discard

Unknown MAC discard is a feature which discards all packets ingressing the service where the destination MAC address is not in the FIB. The normal behavior is to flood these packets to all end points in the service.

Unknown MAC discard can be used with the disable MAC learning and disable MAC aging options to create a fixed set of MAC addresses allowed to ingress and traverse the service.

5.2.7.7 VPLS and rate limiting

Traffic that is flooded throughout the VPLS can be rate limited on SAP ingress through the use of service ingress QoS policies. In a service ingress QoS policy, individual meters can be defined per forwarding class to provide rate-limiting/policing of broadcast traffic, MAC multicast traffic and unknown destination MAC traffic.

5.2.7.8 MAC move

The MAC move feature is useful to protect against undetected loops in a VPLS topology as well as the presence of duplicate MACs in a VPLS service.

If two clients in the VPLS have the same MAC address, the VPLS experiences a high relearn rate for the MAC. When MAC move is enabled, the 7210 SAS-R6 or 7210 SAS-R12 shuts down the SAP or spoke-SDP and creates an alarm event when the threshold is exceeded.

MAC move allows sequential order port blocking. By configuration, some VPLS ports can be configured as "non-blockable" which allows simple level of control which ports are being blocked during loop occurrence.

5.2.7.8.1 Split horizon SAP groups and split horizon spoke-SDP groups

Within the context of VPLS services, a loop-free topology inside a fully meshed VPLS core is achieved by applying a split-horizon forwarding concept.The packets received from a mesh SDP are never forwarded to other mesh SDPs within the same service. The advantage of this approach is that no protocol is required to detect loops within the VPLS core network.

In applications such as DSL aggregation, it is useful to extend this split-horizon concept also to groups of SAPs or spoke-SDPs. This extension is referred to as a split horizon SAP group. Traffic arriving on a SAP or a spoke-SDP within a split horizon group is not forwarded to other SAPs and spoke SDPs configured in the same split horizon group, but is forwarded to other SAPs/spoke-SDPs, which are not part of the split horizon group.

5.2.7.8.2 Configuration guidelines for use of split horizon group in a VPLS service

On all 7210 SAS platforms, except for 7210 SAS-R6 and 7210 SAS-R12 IMM-b, mesh SDPs cannot be configured in a service which uses split horizon group. Conversely, if a service has a mesh-SDP configured, split horizon group cannot be used in the same service. On 7210 SAS-R6 and 7210 SAS-R12 IMM-b, SHG can be configured along with spoke-SDP and mesh-SDP.

5.2.8 VPLS and Spanning Tree Protocol

The Nokia VPLS service provides a bridged or switched Ethernet Layer 2 network. Equipment connected to SAPs forward Ethernet packets into the VPLS service. The participating in the service learns where the customer MAC addresses reside, on ingress SAPs.

Unknown destinations, broadcasts, and multicasts are flooded to all other SAPs in the service. If SAPs are connected together, either through misconfiguration or for redundancy purposes, loops can form and flooded packets can keep flowing through the network. The Nokia implementation of the Spanning Tree Protocol (STP) is designed to remove these loops from the VPLS topology. This is done by putting one or several SAPs in the discarding state.

The Nokia implementation of the Spanning Tree Protocol (STP) incorporates some modifications to make the operational characteristics of VPLS more effective.

The STP instance parameters allow the balancing between resiliency and speed of convergence extremes. Modifying particular parameters can affect the behavior. For information about command usage, descriptions, and CLI syntax, see Configuring a VPLS service with CLI.

5.2.8.1 Spanning tree operating modes

Per VPLS instance, a preferred STP variant can be configured. The STP variants supported are:

- rstp - Rapid Spanning Tree Protocol (RSTP) compliant with IEEE 802.1D-2004 - default mode
- dot1w - compliant with IEEE 802.1w
- comp-dot1w - operation as in RSTP but backwards compatible with IEEE 802.1w (this mode allows interoperability with some MTU types)
- mstp - compliant with the Multiple Spanning Tree Protocol specified in IEEE 802.1Q-REV/D5.0-09/2005. This mode of operation is only supported in an mVPLS

While the 7210 SAS initially uses the mode configured for the VPLS, it dynamically falls back (on a per-SAP basis) to STP (IEEE 802.1D-1998) based on the detection of a BPDU of a different format. A trap or log entry is generated for every change in spanning tree variant.

Some older 802.1W compliant RSTP implementations may have problems with some of the features added in the 802.1D-2004 standard. Interworking with these older systems is improved with the comp-dot1w mode. The differences between the RSTP mode and the comp-dot1w mode are:

- The RSTP mode implements the improved convergence over shared media feature, for example, RSTP transitions from discarding to forwarding in 4 seconds when operating over shared media. The comp-dot1w mode does not implement this 802.1D-2004 improvement and transitions conform to 802.1w in 30 seconds (both modes implement fast convergence over point-to-point links).
- In the RSTP mode, the transmitted BPDUs contain the port's designated priority vector (DPV) (conforms to 802.1D-2004). Older implementations may be confused by the DPV in a BPDU and may fail to recognize an agreement BPDU correctly. This would result in a slow transition to a forwarding state (30 seconds). For this reason, in the comp-dot1w mode, these BPDUs contain the port's port priority vector (conforms to 802.1w).

The 7210 SAS supports BDPU encapsulation formats, and can dynamically switch between the following supported formats (on a per-SAP basis):

- IEEE 802.1D STP
- Cisco PVST

5.2.8.2 Multiple Spanning Tree

The Multiple Spanning Tree Protocol (MSTP) extends the concept of the IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) by allowing grouping and associating VLANs to Multiple Spanning Tree Instances (MSTI). Each MSTI can have its own topology, which provides architecture enabling load balancing by providing multiple forwarding paths. At the same time, the number of STP instances running in the network is significantly reduced as compared to Per VLAN STP (PVST) mode of operation. Network fault tolerance is also improved because a failure in one instance (forwarding path) does not affect other instances.

The 7210 SAS implementation of Management VPLS (mVPLS) is used to group different VPLS instances under single RSTP instance. Introducing MSTP into the mVPLS allows the following:

- interoperation with traditional Layer 2 switches in access network
- provides an effective solution for dual homing of many business Layer 2 VPNs into a provider network

5.2.8.2.1 Configuration notes for Spanning Tree Protocol, L2PT and BPDU translation

The 7210 SAS-R6 and 7210 SAS-R12 devices, reserves some entries in the L2 FIB table for use with xSTP, L2PT and BPDU translation. A fixed amount of such resources are available per node. The user has an option to allocate these resources to services, where they plan to use one of these protocols, at service creation time. This is achieved with the new CLI parameter **allow-l2pt-xstp-bpdu** [**enable** | **disable**]. This is a mandatory parameter that the user must configure if they plan to enable one of these protocols in the service. The software fails any attempt to enable these protocols if this parameter has not been configured for the service.

5.2.8.3 MSTP for QinQ SAPs

MSTP runs in a MVPLS context and can control SAPs from source VPLS instances. QinQ SAPs are supported. The outer tag is considered by MSTP as part of VLAN range control

5.2.8.4 Enhancements to the Spanning Tree Protocol

To interconnect 7210 SAS devices (PE devices) across the backbone, service tunnels (SDPs) are used. These service tunnels are shared among multiple VPLS instances. The Nokia implementation of the Spanning Tree Protocol (STP) incorporates some enhancements to make the operational characteristics of VPLS more effective. The implementation of STP on the router is modified to guarantee that service tunnels is not blocked in any circumstance without imposing artificial restrictions on the placement of the root bridge within the network. The modifications introduced are fully compliant with the 802.1D-2004 STP specification.

When running MSTP, spoke-SDPs cannot be configured. Also, ensure that all bridges connected by mesh SDPs are in the same region. If not, the mesh is prevented from becoming active (trap is generated).

To achieve this, all mesh SDPs are dynamically configured as either root ports or designated ports. The PE devices participating in each VPLS mesh determine (using the root path cost learned as part of the normal protocol exchange) which of the 7210 SAS devices is closest to the root of the network. This PE device is internally designated as the primary bridge for the VPLS mesh. As a result of this, all network ports on the primary bridges are assigned the designated port role and therefore remain in the forwarding state.

The second part of the solution ensures that the remaining PE devices participating in the STP instance see the SDP ports as a lower cost path to the root instead of a path that is external to the mesh. Internal to the PE nodes participating in the mesh, the SDPs are treated as zero cost paths toward the primary bridge. As a consequence, the path through the mesh are seen as lower cost than any alternative and the PE node designates the network port as the root port. This ensures that network ports always remain in forwarding state.

A combination of the preceding features ensure that network ports are never blocked and maintain interoperability with bridges external to the mesh that are running STP instances.

5.2.8.4.1 L2PT termination

L2PT is used to transparently transport protocol data units (PDUs) of Layer 2 protocols such as STP, CDP, DTP, VTP, PAGP, and UDLD. This allows running these protocols between customer CPEs without involving backbone infrastructure.

The 7210 SAS routers allow transparent tunneling of PDUs across the VPLS core. However, in some network designs, the VPLS PE is connected to CPEs through a legacy Layer 2 network instead of having direct connections. In such environments termination of tunnels through such infrastructure is required.

L2PT tunnels protocol PDUs by overwriting MAC destination addresses at the ingress of the tunnel to a proprietary MAC address such as 01-00-0c-cd-cd-d0. At the egress of the tunnel, this MAC address is then overwritten back to MAC address of the respective Layer 2 protocol.

The 7210 SAS nodes support L2PT termination for STP BPDUs. More specifically:

- At ingress of every SAP which is configured as L2PT termination, all PDUs with a MAC destination address, 01-00-0c-cd-cd-d0 are intercepted and their MAC destination address are overwritten to MAC destination address used for the corresponding protocol. The type of protocol can be derived from LLC and SNAP encapsulation.
- In egress direction, PDUs of the corresponding protocol received on all VPLS ports are intercepted and L2PT encapsulation is performed for SAPs configured as L2PT termination points. Because of the implementation reasons, PDU interception and redirection to CPM can be performed only at ingress. Therefore, to comply with the preceding requirement, as soon as at least 1 port of a specific VPLS service is configured as L2PT termination port, redirection of PDUs to CPM is set on all other ports (SAPs) of the VPLS service.

L2PT termination can be enabled only if STP is disabled in a context of the specific VPLS service.

5.2.8.4.2 BPDU translation

VPLS networks are typically used to interconnect different customer sites using different access technologies such as Ethernet and bridged-encapsulated ATM PVCs. Typically, different Layer 2 devices can support different types of STP and even if they are from the same vendor. In some cases, it is necessary to provide BPDU translation to provide an interoperable e2e solution.

To address these network designs, BPDU format translation is supported on 7210 SAS devices. If enabled on a specific SAP, the system intercepts all BPDUs destined for that interface and perform required format translation such as STP-to-PVST or PVST-to-STP.

Similarly, BPDU interception and redirection to the CPM is performed only at ingress meaning that as soon as at least 1 port within a specific VPLS service has BPDU translation enabled, all BPDUs received on any of the VPLS ports are redirected to the CPM.

BPDU translation involves all encapsulation actions that the datapath would perform for a specific outgoing port (such as adding VLAN tags depending on the outer SAP and adding or removing all the required VLAN information in a BPDU payload.

This feature can be enabled on a SAP only if STP is disabled in the context of the specific VPLS service.

5.2.8.4.3 L2PT and BPDU translation

L2PT termination for only STP (Spanning Tree Protocol) and PVST (Per VLAN Spanning Tree Protocol), Cisco Discovery Protocol (CDP), Digital Trunking Protocol (DTP), Port Aggregation Protocol (PAgP), Uni-directional Link Detection (UDLD), Virtual Trunk Protocol (VTP), STP (Spanning Tree Protocol) and PVST (per-VLAN Spanning Tree protocol) are supported on 7210 SAS devices.

These protocols automatically pass the other protocols tunneled by L2PT toward the CPM and all carry the same specific Cisco MAC.

The existing L2PT limitations apply:

- The protocols apply only to VPLS.
- The protocols cannot be used while running STP on the same VPLS as soon as one SAP has L2PT/ BPDU translation enabled.
- Forwarding occurs on the CPM and uses CPU processing cycles.

5.2.9 VPLS redundancy

The VPLS standard (RFC 4762, *Virtual Private LAN Services Using LDP Signaling*) includes provisions for hierarchical VPLS, using point-to-point spoke SDPs. Two applications have been identified for spoke SDPs:

- to connect to Multi-Tenant Units (MTUs) to PEs in a metro area network
- to interconnect the VPLS nodes of two networks

In both applications the spoke SDPs serve to improve the scalability of VPLS. While node redundancy is implicit in non-hierarchical VPLS services (using a full mesh of SDPs between PEs), node redundancy for spoke SDPs needs to be provided separately. In VPLS services, only two spoke-SDPs are allowed in an endpoint.

Nokia routers have implemented special features for improving the resilience of hierarchical VPLS instances, in both MTU and inter-metro applications.

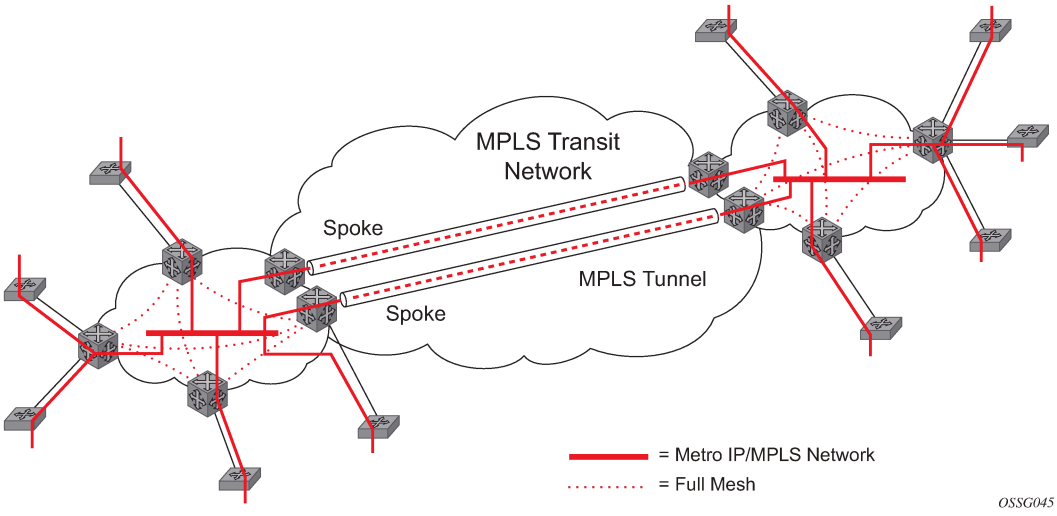
5.2.9.1 Spoke-SDP redundancy for metro interconnection

When two or more meshed VPLS instances are interconnected by redundant spoke SDPs (as shown in Figure 53: H-VPLS with spoke redundancy), a loop in the topology results. To remove such a loop from the topology, Spanning Tree Protocol (STP) can be run over the SDPs (links) which form the loop such that one of the SDPs is blocked. As running STP in each and every VPLS in this topology is not efficient, the node includes functionality which can associate a number of VPLSes to a single STP instance running over the redundant-SDPs. Node redundancy is therefore achieved by running STP in one VPLS, and applying the conclusions of this STP to the other VPLS services. The VPLS instance running STP is referred to as the "management VPLS" or mVPLS.

In the case of a failure of the active node, STP on the management VPLS in the standby node changes the link states from disabled to active. The standby node then broadcasts a MAC flush LDP control message in each of the protected VPLS instances, so that the address of the newly active node can be relearned by all PEs in the VPLS.

It is possible to configure two management VPLS services, where both VPLS services have different active spokes (this is achieved by changing the path-cost in STP). By associating different user VPLSes with the two management VPLS services, load balancing across the spokes can be achieved.

Figure 53: H-VPLS with spoke redundancy



5.2.9.2 Spoke-SDP-based redundant access

This feature provides the ability to have a node deployed as MTUs (Multi-Tenant Unit Switches) to be multi-homed for VPLS to multiple routers deployed as PEs without requiring the use of mVPLS.

In the configuration example shown in Figure 53: H-VPLS with spoke redundancy, the MTUs have spoke-SDPs to two PEs devices. One is designated as the primary and one as the secondary spoke-SDP. This is based on a precedence value associated with each spoke. If the primary and secondary spoke-SDPs have the same precedence value, the spoke-SDP with lower ID functions as the primary SDP.

The secondary spoke is in a blocking state (both on receive and transmit) as long as the primary spoke is available. When the primary spoke becomes unavailable (because of link failure, PEs failure, and so on), the MTU immediately switches traffic to the backup spoke and starts receiving/sending traffic to/from the standby spoke. Optional revertive operation (with configurable switch-back delay) is applicable only when one of the spokes is configured with precedence of primary. If not, this action does not take place. Forced manual switchover is also supported.

To speed up the convergence time during a switchover, MAC flush is configured. The MTUs generates a MAC flush message over the newly unblocked spoke when a spoke change occurs. As a result, the PEs receiving the MAC flush then flush all MACs associated with the impacted VPLS service instance and forward the MAC flush to the other PEs in the VPLS network if **propagate-mac-flush** is enabled.

5.2.9.3 Inter-domain VPLS resiliency using multi-chassis endpoints

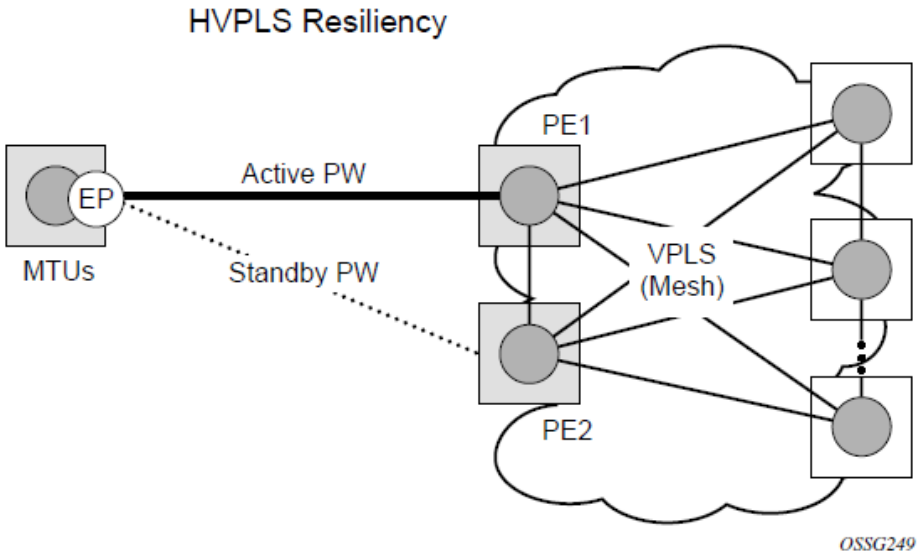
Note: MC-EP is not supported on 7210 SAS platforms. This section provides an example of how 7210 SAS devices can be used as MTU devices in an MC-EP solution. In this solution the 7750 SR routers provide the MC-EP functionality.

Inter-domain VPLS refers to a VPLS deployment where sites may be located in different domains. An example of inter-domain deployment can be where different Metro domains are interconnected over a Wide Area Network (Metro1-WAN-Metro2) or where sites are located in different autonomous systems (AS1-ASBRs-AS2).

Multi-chassis endpoint (MC-EP) provides an alternate solution that does not require RSTP at the gateway VPLS PEs while still using pseudowires to interconnect the VPLS instances located in the two domains.

MC-EP expands the single chassis endpoint based on active/standby pseudowires for VPLS shown in the following figure. In the solution shown by the following figure, 7210 devices are used as MTUs.

Figure 54: H-VPLS resiliency based on AS pseudowires



The active/standby pseudowire solution is appropriate for the scenario when only one VPLS PE (MTU-s) needs to be dual-homed to two core PEs (PE1 and PE2).

5.2.10 VPLS access redundancy

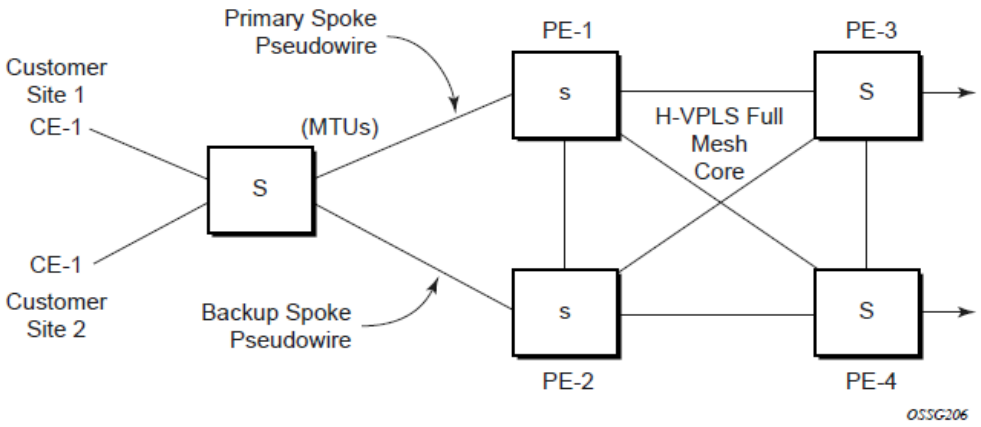
A second application of hierarchical VPLS is using that are MPLS-enabled which must have spoke-SDPs to the closest PE node. To protect against failure of the PE node, an MTU can be dual-homed.

The following are several mechanisms that can be used to resolve a loop in an access circuit, however from operation perspective they can be subdivided into STP-based access, with or without mVPLS.

5.2.10.1 STP-based redundant access to VPLS

In configuration shown in the following figure, STP is activated on the MTU and two PEs to resolve a potential loop.

Figure 55: Dual homed MTU-s in two-tier hierarchy H-VPLS



To remove such a loop from the topology, Spanning Tree Protocol (STP) can be run over the SDPs (links) which form the loop such that one of the SDPs is blocked. Running STP in every VPLS in this topology is not efficient as the node includes functionality which can associate a number of VPLSes to a single STP instance running over the redundant SDPs. Node redundancy is therefore achieved by running STP in one VPLS. Therefore, this applies the conclusions of this STP to the other VPLS services.

The VPLS instance running STP is referred to as the management VPLS or mVPLS. In the case of a failure of the active node, STP on the management VPLS in the standby node changes the link states from disabled to active. The standby node then broadcasts a MAC flush LDP control message in each of the protected VPLS instances, so that the address of the newly active node can be relearned by all PEs in the VPLS. It is possible to configure two management VPLS services, where both VPLS services have different active spokes (this is achieved by changing the path-cost in STP). By associating different user VPLSes with the two management VPLS services, load balancing across the spokes can be achieved.

In this configuration the scope of STP domain is limited to MTU and PEs, while any topology change needs to be propagated in the whole VPLS domain.

This is done by using "MAC-flush" messages defined by RFC 4762, *Virtual Private LAN Services Using LDP Signaling*. In the case where STP acts as a loop resolution mechanism, every Topology Change Notification (TCN) received in a context of STP instance is translated into an LDP-MAC address withdrawal message (also referred to as a MAC-flush message) requesting to clear all FDB entries except the ones learned from the originating PE. Such messages are sent to all PE peers connected through SDPs (mesh and spoke) in the context of VPLS services which are managed by the specific STP instance.

5.2.10.2 Redundant access to VPLS without STP

The Nokia implementation also alternative methods for providing a redundant access to Layer 2 services, such as MC-LAG. Also in this case, the topology change event needs to be propagated into VPLS topology to provide fast convergence.

Figure 53: H-VPLS with spoke redundancy show a dual-homed connection to VPLS service (PE-A, PE-B, PE-C, PE-D) and operation in case of link failure (between PE-C and L2-B). Upon detection of a link failure PE-C sends MAC-Address-Withdraw messages, which indicates to all LDP peers that they should flush all MAC addresses learned from PE-C. This leads to a broadcasting of packets addressing affected hosts and relearning process in case an alternative route exists.

Note that the message described here is different from the message described in previous section and in RFC 4762, *Virtual Private LAN Services Using LDP Signaling*. The difference is in the interpretation and action performed in the receiving PE. According to the standard definition, upon receipt of a MAC withdraw message, all MAC addresses, except the ones learned from the source PE, are flushed,

This section specifies that all MAC addresses learned from the source are flushed. This message has been implemented as an LDP address message with vendor-specific type, length, value (TLV), and is called the flush-mine message.

The advantage of this approach (as compared to RSTP based methods) is that only MAC-affected addresses are flushed and not the full forwarding database. While this method does not provide a mechanism to secure alternative loop-free topology, the convergence time is dependent on the speed of the specific CE device opening alternative links (L2-B switch in Figure 57) as well as on the speed PE routers flush their FDB.

In addition, this mechanism is effective only if PE and CE are directly connected (no hub or bridge) as it reacts to physical failure of the link.

5.2.11 MAC flush message processing

The previous sections described operation principle of several redundancy mechanisms available in context of VPLS service. All of them rely on MAC flush message as a tool to propagate topology change in a context of the specific VPLS. This section aims to summarize basic rules for generation and processing of these messages.

As described on respective sections, the 7210 SAS supports two types of MAC flush message, flush-all-but-mine and flush-mine. The main difference between these messages is the type of action they signal. Flush-all-but-mine requests clearing of all FDB entries which were learned from all other LDP peers except the originating PE. This type is also defined by RFC 4762 as an LDP MAC address withdrawal with an empty MAC address list.

Flush-all-mine message requests clearing all FDB entries learned from originating PE. This means that this message has exactly other effect then flush-all-but-mine message. This type is not included in RFC 4762 definition and it is implemented using vendor specific TLV.

The advantages and disadvantages of the individual types should be apparent from examples in the previous section. The description here focuses on summarizing actions taken on reception and conditions individual messages are generated.

Upon reception of MAC flush messages (regardless the type) SR-Series PE takes following actions:

- Clears FDB entries of all indicated VPLS services conforming the definition.
- Propagates the message (preserving the type) to all LDP peers, if "propagate-mac-flush” flag is enabled at corresponding VPLS level.

The flush-all-but-mine message is generated under following conditions:

- The flush-all-but-mine message is received from LDP peer and propagate-mac-flush flag is enabled. The message is sent to all LDP peers in the context of VPLS service it was received in.

- TCN message in a context of STP instance is received. The flush-all-but-mine message is sent to all LDP-peers connected with spoke and mesh SDPs in a context of VPLS service controlled by the specific STP instance (based on mVPLS definition). The message is sent only to LDP peers which are not part of STP domain, which means corresponding spoke and mesh SDPs are not part of mVPLS.
- Flush-all-but-mine message is generated when switch over between spoke SDPs of the same endpoint occurs. The message is sent to LDP peer connected through newly active spoke-SDP.

The flush-mine message is generated under following conditions:

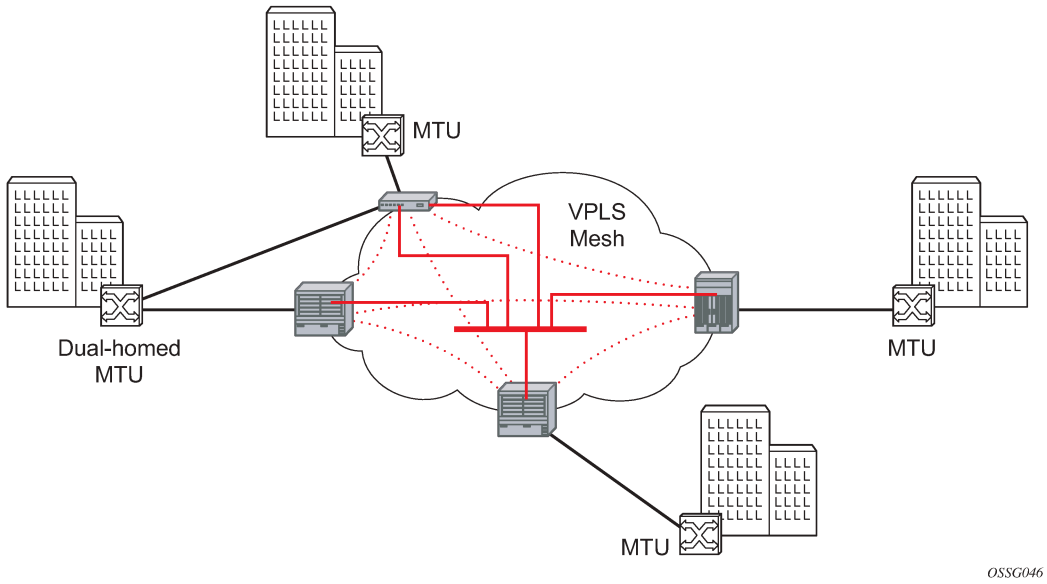
- The flush-mine message is received from LDP peer and **propagate-mac-flush** flag is enabled. The message is sent to all LDP peers in the context of VPLS service it was received.
- The flush-mine message is generated when a SAP or SDP transitions from operationally up to an operationally down state and **send-flush-on-failure** flag is enabled in the context of the specific VPLS service. The message is sent to all LDP peers connected in the context of the specific VPLS service. Note, that enabling **send-flush-on-failure** the flag is blocked in VPLS service managed by mVPLS. This is to prevent both messages from being sent at the same time.
- The flush-mine message is generated when an MC-LAG SAP transitions from an operationally up state to an operationally down state. The message is sent to all LDP peers connected in the context of the specific VPLS service.

5.2.11.1 MAC flush with STP

A second application of Hierarchical VPLS is in the use of Multi Tenant Units (MTU). MTUs are typically not MPLS-enabled, and therefore have Ethernet links to the closest PE node (see Figure 56: H-VPLS with SAP redundancy). To protect against failure of the PE node, an MTU could be dual-homed and therefore have two SAPs on two PE nodes. To resolve the potential loop, STP is activated on the MTU and the two PEs.

Like in the preceding scenario, STP only needs to run in a single VPLS instance, and the results of the STP calculations are applied to all VPLSs on the link. Equally, the standby node broadcasts MAC flush LDP messages in the protected VPLS instances when it detects that the active node has failed.

Figure 56: H-VPLS with SAP redundancy



5.2.11.2 Selective MAC flush

When using STP as described previously is not appropriate, the "Selective MAC flush" feature can be used instead.

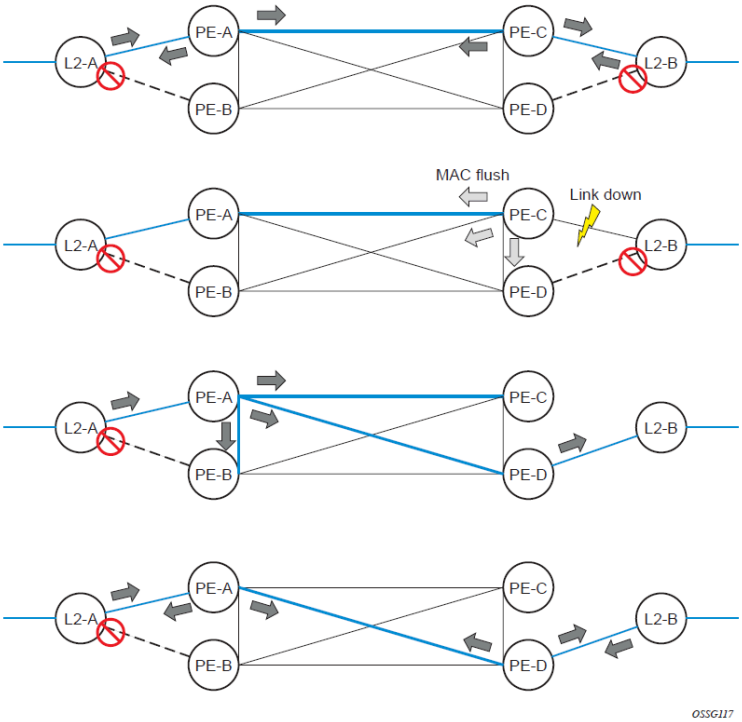
In this scenario, the 7210 SAS that detects a port failure sends out a flush-all-from-ME LDP message to all PEs in the VPLS. The PEs receiving this LDP message removes all MAC entries originated by the sender from the indicated VPLS.

A drawback of this approach is that selective MAC flush does not signal that a backup path was found, only that the previous path is no longer available. In addition, the selective MAC Flush mechanism is effective only if the CE and PE are directly connected (no intermediate hubs or bridges) as it reacts only to a physical failure of the link. Consequently, Nokia recommends using the MAC flush with STP method described previously where possible.

5.2.11.3 Dual homing to a VPLS service

The following figure shows a dual-homed connection to VPLS service (PE-A, PE-B, PE-C, PE-D) and operation in case of link failure (between PE-C and L2-B). Upon detection of a link failure PE-C sends MAC-Address-Withdraw messages, which indicates to all LDP peers that they should flush all MAC addresses learned from PE-C. This leads to a broadcasting of packets addressing affected hosts and relearning process in case an alternative route exists.

Figure 57: Dual homed CE connection to VPLS



Note that the message described here is different from the message described in draft-ietf-l2vpn-vpls-ldp-xx.txt, *Virtual Private LAN Services over MPLS*. The difference is in the interpretation and action performed in the receiving PE. According the draft definition, upon receipt of a MAC-withdraw message, all MAC addresses, except the ones learned from the source PE, are flushed, This section specifies that all MAC addresses learned from the source are flushed. This message has been implemented as an LDP address message with vendor-specific type, length, value (TLV), and is called the flush-all-from-ME message.

The draft definition message is currently used in management VPLS which is using RSTP for recovering from failures in Layer 2 topologies. The mechanism described in this document represent an alternative solution.

The advantage of this approach (as compared to RSTP based methods) is that only MAC-affected addresses are flushed and not the full forwarding database. While this method does not provide a mechanism to secure alternative loop-free topology, the convergence time is dependent on the speed of the specific CE device opening alternative links (L2-B switch in Figure 57: Dual homed CE connection to VPLS) as well as on the speed PE routers flush their FDB.

In addition, this mechanism is effective only if PE and CE are directly connected (no hub or bridge) as it reacts to physical failure of the link.

5.2.12 VPLS service considerations

This section describes various 7210 SAS service features and any special capabilities or considerations as they relate to VPLS services.

5.2.12.1 SAP encapsulations

VPLS services are designed to carry Ethernet frame payloads, so it can provide connectivity between any SAPs that pass Ethernet frames. The following SAP encapsulations are supported on the VPLS service:

- Ethernet null
- Ethernet Dot1q
- Ethernet Dot1q Default
- Ethernet Dot1q Explicit Null

5.2.12.2 VLAN processing

The SAP encapsulation definition on Ethernet ingress ports defines which VLAN tags are used to determine the service that the packet belongs:

1. **null encapsulation defined on ingress**

   Any VLAN tags are ignored and the packet goes to a default service for the SAP

2. **dot1q encapsulation defined on ingress**

   Only first VLAN tag is considered.

3. **dot1q Default encapsulation defined on ingress**

   Tagged packets not matching any of the configured VLAN encapsulations would be accepted. This is like a default SAP for tagged packets.

4. **dot1q Explicit Null encapsulation defined on ingress**

   Any untagged or priority tagged packets are accepted.

5.3 BGP Auto-Discovery for LDP VPLS

BGP Auto Discovery (BGP AD) for LDP VPLS is a framework for automatically discovering the endpoints of a Layer 2 VPN offering an operational model similar to that of an IP VPN. This model allows carriers to leverage existing network elements and functions, including but not limited to, route reflectors and BGP policies to control the VPLS topology.

BGP AD is an excellent complement to an already established and well deployed Layer 2 VPN signaling mechanism target LDP providing one touch provisioning for LDP VPLS where all the related PEs are discovered automatically. The service provider may make use of existing BGP policies to regulate the exchanges between PEs in the same, or in different, autonomous system (AS) domains. The addition of BGP AD procedures does not require carriers to uproot their existing VPLS deployments and to change the signaling protocol.

5.3.1 BGP AD overview

The BGP protocol establishes neighbor relationships between configured peers. An open message is sent after the completion of the three-way TCP handshake. This open message contains information about the BGP peer sending the message. This message contains Autonomous System Number (ASN), BGP

version, timer information and operational parameters, including capabilities. The capabilities of a peer are exchanged using two numerical values: the Address Family Identifier (AFI) and Subsequent Address Family Identifier (SAFI). These numbers are allocated by the Internet Assigned Numbers Authority (IANA). BGP AD uses AFI 65 (L2VPN) and SAFI 25 (BGP VPLS).

5.3.2 Information model

Following is the establishment of the peer relationship, the discovery process begins as soon as a new VPLS service instance is provisioned on the PE.

Two VPLS identifiers are used to indicate the VPLS membership and the individual VPLS instance:

- **VPLS-ID**

  Membership information, unique network wide identifier; same value assigned for all VPLS switch instances (VSIs) belonging to the same VPLS; encodable and carried as a BGP extended community in one of the following formats:

  – a two-octet AS specific extended community

  – an IPv4 address specific extended community

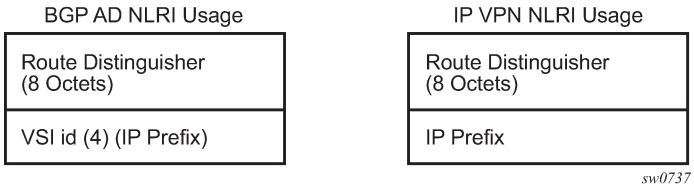
- **VSI-ID**

  The unique identifier for each individual VSI, built by concatenating a route distinguisher (RD) with a 4 bytes identifier (usually the system IP of the VPLS PE); encoded and carried in the corresponding BGP NLRI.

To advertise this information, BGP AD employs a simplified version of the BGP VPLS NLRI where just the RD and the next 4 bytes are used to identify the VPLS instance. There is no need for Label Block and Label Size fields as T-LDP takes care of signaling the service labels later on.

The format of the BGP AD NLRI is very similar with the one used for IP VPN, as shown in the following figure. The system IP may be used for the last 4 bytes of the VSI-ID further simplifying the addressing and the provisioning process.

Figure 58: BGP AD NLRI versus IP VPN NLRI



Network Layer Reachability Information (NLRI) is exchanged between BGP peers indicating how to reach prefixes. The NLRI is used in the Layer 2 VPN case to tell PE peers how to reach the VSI instead of specific prefixes. The advertisement includes the BGP next hop and a route target (RT). The BGP next hop indicates the VSI location and is used in the next step to determine which signaling session is used for pseudowire signaling. The RT, also coded as an extended community, can be used to build a VPLS full mesh or a H-VPLS hierarchy through the use of BGP import or export policies.

BGP is only used to discover VPN endpoints and the corresponding far end PEs. It is not used to signal the pseudowire labels. This task remains the responsibility of targeted-LDP (T-LDP).

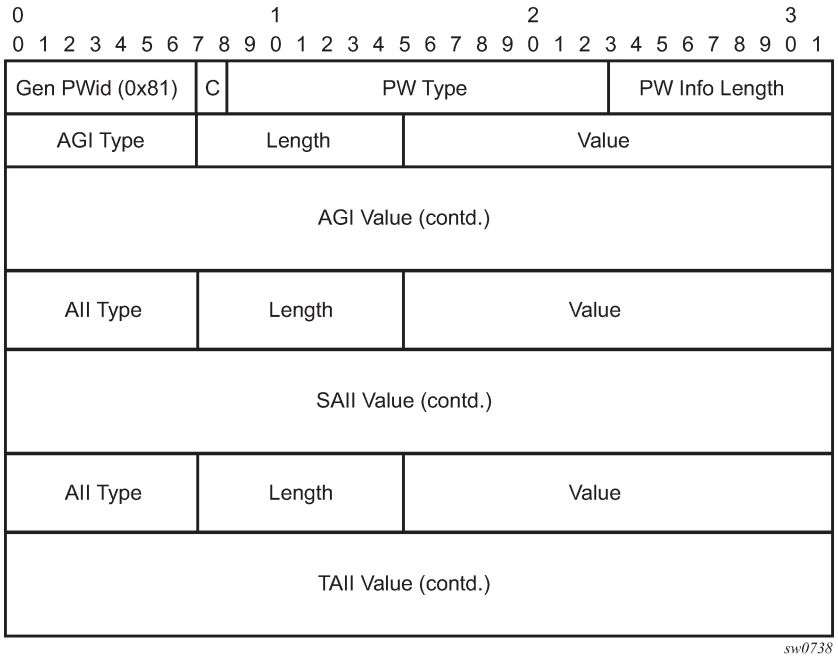
5.3.3 FEC element for T-LDP signaling

Two LDP FEC elements are defined in RFC 4447, *PW Setup & Maintenance Using LDP*. The original pseudowire-ID FEC element 128 (0x80) employs a 32-bit field to identify the virtual circuit ID and it was used extensively in the initial VPWS and VPLS deployments. The simple format is easy to understand but it does not provide the required information model for BGP Auto-Discovery function. To support BGP AD and other new applications a new Layer 2 FEC element, the generalized FEC (0x81) is required.

The generalized pseudowire-ID FEC element has been designed for auto discovery applications. It provides a field, the address group identifier (AGI), that is used to signal the membership information from the VPLS-ID. Separate address fields are provided for the source and target address associated with the VPLS endpoints called the Source Attachment Individual Identifier (SAII) and respectively, Target Attachment Individual Identifier (TAII). These fields carry the VSI-ID values for the two instances that are to be connected through the signaled pseudowire.

The detailed format for FEC 129 is shown in the following figure.

Figure 59: Generalized pseudowire-ID FEC element



Each of the FEC fields are designed as a sub-TLV equipped with its own type and length providing support for new applications. To accommodate the BGP AD information model the following FEC formats are used:

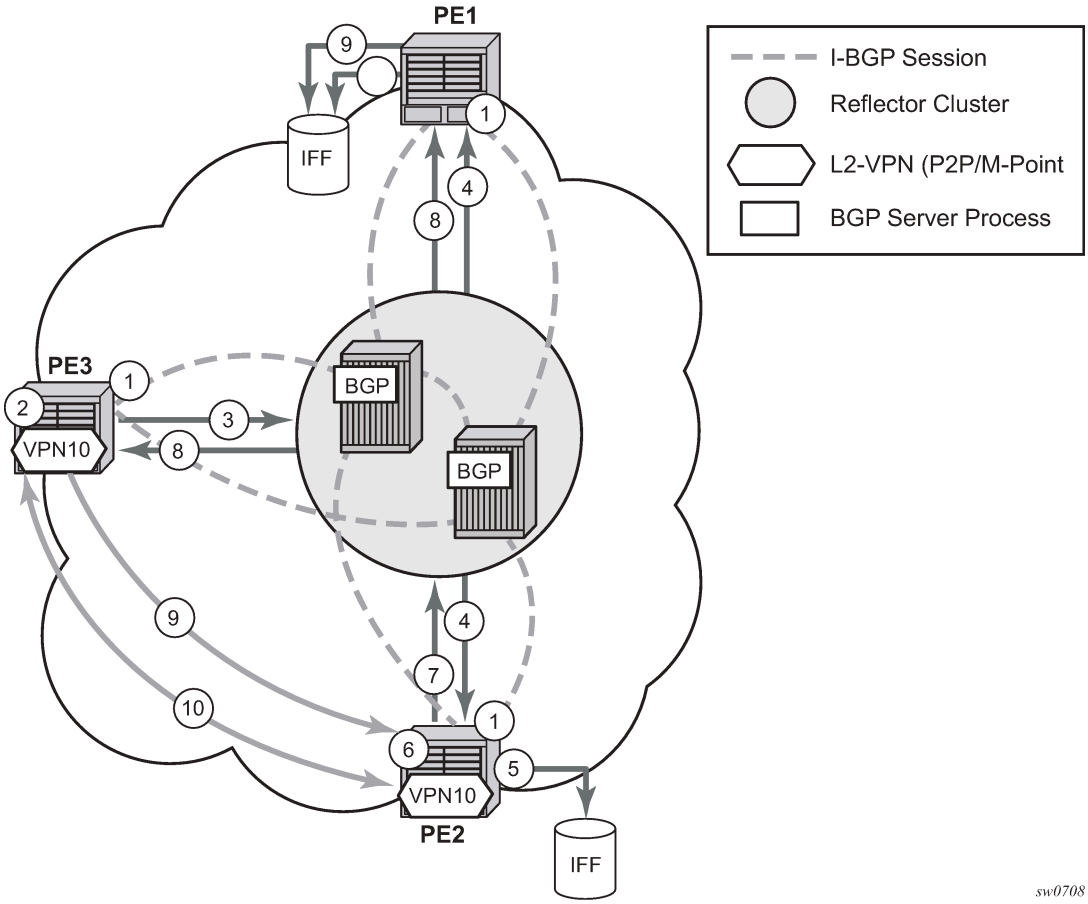
- AGI (type 1) is identical in format and content with the BGP extended community attribute used to carry the VPLS-ID value.
- Source AII (type 1) is a 4-byte value that carries the local VSI-id (outgoing NLRI minus the RD).
- Target AII (type 1) is a 4-byte value that carries the remote VSI-ID (incoming NLRI minus the RD).

5.3.4 BGP-AD and Target LDP (T-LDP) interaction

BGP is responsible for discovering the location of VSIs that share the same VPLS membership. LDP protocol is responsible for setting up the pseudowire infrastructure between the related VSIs by exchanging service specific labels between them.

When the local VPLS information is provisioned in the local PE, the related PEs participating in the same VPLS are identified through BGP AD exchanges. A list of far-end PEs is generated and triggers the creation, if required, of the necessary T-LDP sessions to these PEs and the exchange of the service specific VPN labels. The steps for the BGP AD discovery process and LDP session establishment and label exchange are shown in the following figure.

Figure 60: BGP-AD and T-LDP interaction



Key:

1. Establish I-BGP connectivity RR.
2. Configure VPN (10) on edge node (PE3).
3. Announce VPN to RR using BGP-AD.
4. Send membership update to each client of the cluster.
5. LDP exchange or inbound FEC filtering (IFF) of non-match or VPLS down.

6. Configure VPN (10) on edge node (PE2).
7. Announce VPN to RR using BGP-AD.
8. Send membership update to each client of the cluster.
9. LDP exchange or inbound FEC filtering (IFF) of non-match or VPLS down.
10. Complete LDP bidirectional pseudowire establishment FEC 129.

5.3.5 SDP usage

Service Access Points (SAP) are linked to transport tunnels using Service Distribution Points (SDP). The service architecture of the 7210 platform allows services to be abstracted from the transport network.

MPLS transport tunnels are signaled using the Resource Reservation Protocol (RSVP-TE) or by the Label Distribution Protocol (LDP). The capability to automatically create an SDP only exists for LDP based transport tunnels. Using a manually provisioned SDP is available for both RSVP-TE and LDP transport tunnels. See the *7210 SAS-Mxp, R6, R12, S, Sx, T MPLS Guide* for more information about MPLS, LDP, and RSVP.

5.3.6 Automatic creation of SDPs

When BGP AD is used for LDP VPLS and LDP is used as the transport tunnel there is no requirement to manually create an SDP. The LDP SDP can be automatically instantiated using the information advertised by BGP AD. This simplifies the configuration on the service node.

Enabling LDP on the IP interfaces connecting all nodes between the ingress and the egress, builds transport tunnels based on the best IGP path. LDP bindings are automatically built and stored in the hardware. These entries contain an MPLS label pointing to the best next hop along the best path toward the destination.

When two endpoints need to connect and no SDP exists, a new SDP is automatically constructed. New services added between two endpoints that already have an automatically created SDP are immediately used. No new SDP is constructed. The far-end information is gleaned from the BGP next hop information in the NLRI. When services are withdrawn with a BGP_Unreach_NLRI, the automatically established SDP remains up as long as at least one service is connected between those endpoints. An automatically created SDP is removed and the resources released when the only or last service is removed.

5.3.7 Manually provisioned SDP

The carrier is required to manually provision the SDP if they create transport tunnels using RSVP-TE. Operators have the option to choose a manually configured SDP, if they use LDP as the tunnel signaling protocol. The functionality is the same regardless of the signaling protocol.

Creating a BGP-AD enabled VPLS service on an ingress node with the manually provisioned SDP option causes the Tunnel Manager to search for an existing SDP that connects to the far-end PE. The far-end IP information is gleaned from the BGP next hop information in the NLRI. If a single SDP exists to that PE, it is used. If no SDP is established between the two endpoints, the service remains down until a manually configured SDP becomes active.

When multiple SDPs exist between two endpoints, the tunnel manager selects the appropriate SDP. The algorithm preferred SDPs with the best (lower) metric. Should there be multiple SDPs with equal metrics,

the operational state of the SDPs with the best metric is considered. If the operational state is the same, the SDP with the higher SDP ID is used. If an SDP with a preferred metric is found with an operational state that is not active, the tunnel manager flags it as ineligible and restarts the algorithm.

5.3.8 Automatic instantiation of pseudowires (SDP bindings)

The choice of manual or auto provisioned SDPs has limited impact on the amount of required provisioning. Most of the savings are achieved through the automatic instantiation of the pseudowire infrastructure (SDP bindings). This is achieved for every auto-discovered VSIs through the use of the pseudowire template concept. Each VPLS service that uses BGP AD contains the "pw-template-binding" option defining specific Layer 2 VPN parameters. This command references a "pw-template" which defines the pseudowire parameters. The same "pwtemplate" may be referenced by multiple VPLS services. As a result, changes to these pseudowire templates have to be treated with great care as they may impact many customers at the same time.

The Nokia implementation provides for safe handling of pseudowire templates. Changes to the pseudowire templates are not automatically propagated. Tools are provided to evaluate and distribute the changes. The following command is used to distribute changes to a "pw-template" at the service level to one or all services that use that template.

tools perform service id 300 eval-pw-template 1 allow-service-impact

If the service ID is omitted, then all services are updated. The type of change made to the "pwtemplate" influences how the service is impacted:

1. Adding or removing a split-horizon-group causes the router to destroy the original object and recreate using the new value.
2. Changing parameters in the **vc-type** {**ether** | **vlan**} command requires LDP to resignal the labels.

Both of these changes affect the services. Other changes are not service affected.

5.3.9 Mixing statically configured and auto-discovered pseudowires in a VPLS service

The services implementation allows for manually provisioned and auto-discovered pseudowire (SDP bindings) to coexist in the same VPLS instance (for example, both FEC128 and FEC 129 are supported). This allows for gradual introduction of auto discovery into an existing VPLS deployment.

As FEC 128 and 129 represent different addressing schemes, it is important to make sure that only one is used at any point in time between the same two VPLS instances. Otherwise, both pseudowires may become active causing a loop that may adversely impact the correct functioning of the service. Nokia recommends that the FEC128 pseudowire be disabled as soon as the FEC129 addressing scheme is introduced in a portion of the network. Alternatively, RSTP may be used during the migration as a safety mechanism to provide additional protection against operational errors.

5.3.10 Resiliency schemes

The use of BGP-AD on the network side, or in the backbone, does not affect the different resiliency schemes Nokia has developed in the access network. This means that both Multi-Chassis Link Aggregation (MC-LAG) and Management-VPLS (M-VPLS) can still be used.

BGP-AD may coexist with Hierarchical-VPLS (H-VPLS) resiliency schemes (for example, dual homed MTU-s devices to different PE-rs nodes) using existing methods (M-VPLS and statically configured Active or Standby pseudowire endpoint).

If provisioned SDPs are used by BGP AD, M-VPLS may be employed to provide loop avoidance. However, it is currently not possible to auto-discover active or standby pseudowires and to instantiate the related endpoint.

5.4 Routed VPLS

Routed VPLS (R-VPLS) allows a VPLS instance to be associated with an IP interface.

Within an R-VPLS service, traffic with a destination MAC matching that of the associated IP interface is routed based on the IP forwarding table; all other traffic is forwarded based on the VPLS forwarding table.

In network mode, R-VPLS service can be associated with an IPv4 interface and supports static routing and other routing protocols. It can be used to provide a service to the customer or for in-band management of the node.

5.4.1 IES or VPRN IP interface binding

A standard IP interface within an existing IES or VPRN service context may be bound to a service name. A VPLS service only supports binding for a single IP interface.

While an IP interface may only be bound to a single VPLS service, the routing context containing the IP interface (IES or VPRN) may have other IP interfaces bound to other VPLS service contexts. That is, R-VPLS allows the binding of IP interfaces in IES or VPRN services to be bound to VPLS services.

5.4.2 Assigning a service name to a VPLS service

When a service name is applied to any service context, the name and service ID association is registered with the system. A service name cannot be assigned to more than one service ID. Special consideration is made for a service name that is assigned to a VPLS service that has the **configure>service>vpls>allow-ip-int-binding** command enabled. If a name is applied to the VPLS service while the flag is set, the system scans the existing IES services for an IP interface that is bound to the specified service name. If an IP interface is found, the IP interface is attached to the VPLS service associated with the name. Only one interface can be bound to the specified name.

If the allow-ip-int-binding command is not enabled on the VPLS service, the system does not attempt to resolve the VPLS service name to an IP interface. As soon as the allow-ip-int-binding flag is configured on the VPLS, the corresponding IP interface is adhered and become operational up. There is no need to toggle the shutdown or no shutdown command.

If an IP interface is not currently bound to the service name used by the VPLS service, no action is taken at the time of the service name assignment.

5.4.3 Service binding requirements

When the defined service name is created on the system, the system checks to ensure that the service type is VPLS. If the created service type is VPLS, the IP interface is eligible to enter the operationally upstate.

5.4.3.1 Bound service name assignment

When a bound service name is assigned to a service within the system, the system first checks to ensure the service type is VPLS. Secondly the system ensures that the service is not already bound to another IP interface through the service name. If the service type is not VPLS or the service is already bound to another IP interface through the service ID, the service name assignment fails.

A single VPLS instance cannot be bound to two separate IP interfaces.

5.4.3.2 Binding a service name to an IP interface

An IP interface within an IES or VPRN service context may be bound to a service name at anytime. Only one interface can be bound to a service. When an IP interface is bound to a service name and the IP interface is administratively up, the system scans for a VPLS service context using the name and takes the following actions:

- If the name is not currently in use by a service, the IP interface is placed in an operationally down: Non-existent service name or inappropriate service type state.
- If the name is currently in use by a non-VPLS service or the wrong type of VPLS service, the IP interface is placed in the operationally down: Non-existent service name or inappropriate service type state.
- If the name is currently in use by a VPLS service without the allow-ip-int-binding flag set, the IP interface is placed in the operationally down: VPLS service allow-ip-intbinding flag not set state. There is no need to toggle the shutdown or no shutdown command.
- If the name is currently in use by a valid VPLS service and the allow-ip-int-binding flag is set, the IP interface is eligible to be placed in the operationally up state depending on other operational criteria being met.

5.4.4 Routed VPLS specific ARP cache behavior

In typical routing behavior, the system uses the IP route table to select the egress interface, an ARP entry is used forward the packet to the appropriate Ethernet MAC. With routed VPLS, the egress IP interface may be represented by multiple egress (VPLS service SAPs).

The following table describes how the ARP cache and MAC FIB entry states interact.

Table 47: Routing behavior in R-VPLS and interaction ARP cache and MAC FIB

ARP cache entry	MAC FIB entry	Routing or system behavior
ARP Cache Miss (No Entry)	Known or Unknown	Triggers a request to control plane ARP processing module, to send out an ARP request, out of all the SAPs. (also known as virtual ports) of the VPLS instance.
ARP Cache Hit	Known	Forward to specific VPLS virtual port or SAP.
	Unknown	This behavior cannot happen typically in 7210 SAS, as and when a L2 entry is removed from the FDB, the matching MAC address is also removed from the ARP cache.

5.4.4.1 The allow-ip-int-binding VPLS flag

The **allow-ip-int-binding** flag on a VPLS service context is used to inform the system that the VPLS service is enabled for routing support. The system uses the setting of the flag as a key to determine what type of ports the VPLS service may span.

The system also uses the flag state to define which VPLS features are configurable on the VPLS service to prevent enabling a feature that is not supported when routing support is enabled.

5.4.5 Routed VPLS SAPs only supported on standard Ethernet ports

The **allow-ip-int-binding** flag is set (routing support enabled) on a VPLS service. SAPs within the service can be created on standard Ethernet ports.

5.4.5.1 LAG port membership constraints

If a LAG has a non-supported port type as a member, a SAP for the routing-enabled VPLS service cannot be created on the LAG. When one or more routing enabled VPLS SAPs are associated with a LAG, a non-supported Ethernet port type cannot be added to the LAG membership.

5.4.5.2 VPLS feature support and restrictions

When the **allow-ip-int-binding** flag is set on a VPLS service, the following features cannot be enabled (the flag also cannot be enabled while any of these features are applied to the VPLS service):

- In network mode, SDPs used in spoke or mesh SDP bindings cannot be configured.
- In network mode, the VPLS service type must be R-VPLS; no other VPLS service is allowed.
- MVR from an R-VPLS SAP to another SAP is not supported.
- Default QinQ SAPs are not supported in an R-VPLS service.

- The **allow-ip-int-binding** command cannot be used in a VPLS service that is acting as the G.8032 control instance.
- IPv4 filters (ingress and egress) can be used with R-VPLS SAPs. Additionally IP ingress override filters are supported, which affects the behavior of the IP filters attached to the R-VPLS SAPs.
- MAC filters (ingress and egress) are not supported for use with R-VPLS SAPs.
- A VPLS IP interface is not allowed in an R-VPLS service, and an R-VPLS service/SAP cannot be configured with a VPLS IP interface.
- In network mode, the R-VPLS service can be configured only with access SAPs or with SAPs on hybrid ports (applies only to the 7210 SAS-R6 and 7210 SAS-R12).
- In network mode, the VPLS service can use the following **svc-sap-type** values: any, null-star, and dot1q-preserve.
- G.8032 or MVPLS/STP based protection mechanisms can be used with an R-VPLS service. A separate G.8032 control instance or a separate MVPLS/STP instance must be used and the R-VPLS SAPs must be associated with these control instances such that the R-VPLS SAP forwarding state is driven by the control instance protocols
- IP multicast is not supported in an R-VPLS service.
- IGMP snooping is supported in an R-VPLS service for 7210 SAS-R6 and 7210 SAS-R12.
- DHCP snooping is not supported for the SAPs configured in an R-VPLS service. Instead, DHCP relay can be enabled on the IES service associated with the R-VPLS service.
- In network mode, an R-VPLS SAP drops packets received with extra tags. That is, if a packet is received on a R-VPLS SAP, with number of tags greater than the SAP tags to which it is mapped, then it is dropped. This is true for all supported encapsulations (that is, null, dot1q, and QinQ encapsulations) of the port. For example, double-tagged packets received on a dot1q SAP configured in a R-VPLS service is dropped on ingress.

5.4.6 VPLS SAP ingress IP filter override

When an IP Interface is attached to a VPLS service context, the VPLS SAP provisioned IP filter for ingress routed packets may be optionally overridden to provide special ingress filtering for routed packets. This allows different filtering for routed packets and non-routed packets. The filter override is defined on the IP interface bound to the VPLS service name. A separate override filter may be specified for IPv4 packet types.

If a filter for a specific packet type (IPv4) is not overridden, the SAP specified filter is applied to the packet (if defined).

The following tables list ACL lookup behavior with and without ingress override filter attached to an IES interface in a R-VPLS service.

Table 48: ACL lookup behavior with ingress override filter attached to an IES interface in an R-VPLS service

Type of traffic	SAP ingress IPv4 filter	SAP egress IPv4 filter	Ingress override IPv4 filter
Destination MAC != IES IP interface MAC	Yes	Yes	No

Type of traffic	SAP ingress IPv4 filter	SAP egress IPv4 filter	Ingress override IPv4 filter
Destination MAC = IES IP interface MAC and Destination IP on same subnet as IES interface	No	No	Yes
Destination MAC = IES IP interface MAC and destination IP not on same subnet as IES IP interface and route to destination IP does not exist	No	No	No
Destination MAC = IES IP interface MAC and destination IP not on same subnet as IES IP interface and route to destination IP exists	No	No	Yes
Destination MAC = IES IP interface MAC and IP TTL = 1	No	No	No
Destination MAC = IES IP interface MAC and IPv4 packet with Options	No	No	No
Destination MAC = IES IP interface MAC and IPv4 Multicast packet	No	No	No

Table 49: ACL lookup behavior without ingress override filter attached to an IES interface in an R-VPLS service

Type of traffic	SAP ingress IPv4 filter	SAP egress IPv4 filter
Destination MAC != IES IP interface MAC	Yes	Yes
Destination MAC = IES IP interface MAC and Destination IP on same subnet as IES IP interface	Yes	No
Destination MAC = IES IP interface MAC and destination IP not on same subnet as IES IP interface and route to destination IP does not exist	No	No
Destination MAC = IES IP interface MAC and destination IP not on same subnet as IES IP interface and route to destination IP exists	Yes	No
Destination MAC = IES IP interface MAC and IP TTL = 1	No	No
Destination MAC = IES IP interface MAC and IPv4 packet with Options	No	No
Destination MAC = IES IP interface MAC and IPv4 Multicast packet	No	No

5.4.6.1 QoS support for VPLS SAPs and IP interface in a routed VPLS service

The following information describes QoS support for VPLSs SAPs and IP interface in a routed VPLS service:

- SAP ingress classification (IPv4 and MAC criteria) is supported for SAPs configured in the service. SAP ingress policies cannot be associated with IES IP interface.
- On 7210 SAS-R6 and 7210 SAS-R12, when the node is operating in SAP based queuing mode, unicast traffic sent out of R-VPLS SAPs uses SAP based egress queues while BUM traffic sent out of R-VPLS SAPs uses per port egress queues. When the 7210 SAS-R6 and 7210 SAS-R12 node is operating in port based queuing mode, both unicast and BUM traffic sent out of R-VPLS SAPS uses per port egress queues. For more information, refer to the *7210 SAS-Mxp, R6, R12, S, Sx, T Quality of Service Guide*.
- Port based Egress Marking is supported for both routed packets and bridged packets. The existing access egress QoS policy can be used for Dot1p marking and DSCP marking.

5.4.6.2 Routed VPLS supported routing related protocols

In network mode, R-VPLS is supported in both the base routing instances (IES) and VPRN services. IPv4 addressing is supported for IES and VPRN IP interfaces associated with an R-VPLS service. The following table lists the support available for routing protocols on IP interfaces bound to a VPLS service in network mode.

Table 50: Routing protocols on IP interfaces bound to a VPLS service

Services	Network
Static-routing	Supported
BGP	Supported
OSPF	Supported
ISIS	Supported
BFD	Supported
VRRP	Supported
ARP and Proxy-Arp	Both are supported
DHCP Relay[14]	Supported

5.4.6.3 Spanning tree and split horizon

An R-VPLS context supports all spanning tree capabilities that a non-routed VPLS service supports. Service-based SHGs are not supported in an R-VPLS context.

5.4.7 Routed VPLS and IGMPv3 snooping

This feature (IGMPv3 snooping in R-VPLS) extends IGMP snooping to a routed VPLS service. On 7210 SAS, VPLS services that use MPLS uplinks (network mode) support IGMP snooping with IGMP v1

[14] DHCP relay can be configured for the IES interface associated with the Routed VPLS service. DHCP snooping cannot be configured on the VPLS SAPs in the routed VPLS Service.

and v2 only. That is, IGMP v3 is not supported, which means that only Layer 2 multicast is supported. To support source-based IP multicast, support for IGMPv3 is needed. To provide source-based IP multicast, support for IGMP snooping v1, v2, and v3 is added to routed VPLS service. The IGMPv3 snooping in R-VPLS feature gives customers an option to use a routed VPLS service without a configured IP interface association to deliver IP multicast traffic in access Layer 2 networks. Users also have an option to configure MVR service.

IGMPv3 snooping in R-VPLS is supported only for IES (not for VPRNs).

For information about IGMP snooping in the context of VPLS, see IGMP snooping in VPLS service.

5.4.7.1 Configuration guidelines and restrictions for IGMP snooping in R-VPLS

The following items apply to IGMP snooping in R-VPLS and should be included with the regular VPLS multicast configuration guidelines (see Configuration guidelines for IGMP snooping in VPLS service and Routed VPLS supported functionality and restrictions):

- R-VPLS without an IP interface association can be used to emulate VPLS service with support for IGMPv3 snooping.
- R-VPLS with or without IP interface association can be used for IGMPv3 snooping. If enabling MVR on the service then the service should not have an IP interface association.
- IGMPv3 snooping can be enabled in the context of the R-VPLS (both with and without MVR). It cannot be enabled in regular VPLS service. Regular VPLS service supports IGMP v1 and v2 only.
- MVR can be configured in an R-VPLS without an IP interface association. It can be used to leak multicast traffic to a user R-VPLS service with an IP interface configuration. Therefore, a user R-VPLS can be used to forward both unicast and multicast services.

In addition, the following list of guidelines and restrictions pertain to IGMP snooping in an R-VPLS service:

- R-VPLS service can only have a single SAP per port configured in a service. That is, two SAPs on the same port cannot be configured in the same service.
- Spoke SDPs and mesh SDPs cannot be configured in an R-VPLS service.
- On 7210 SAS devices, on ingress of a port, multicast traffic can be processed in the context of either **igmp-snooping** (Layer 2 Ethernet multicast with IGMP v1 or v2 snooping) or **l3-multicast** (either multicast in an Layer 3 service or IGMP snooping in an R-VPLS), but not both. That is, it is not possible to configure SAPs on the port such that one SAP is a receiver for multicast traffic to be processed by IGMP snooping, and another SAP is a receiver for multicast traffic to be processed by IP multicast in the context of Layer 3 service or R-VPLS. An option per port is available using the **configure>port>ethernet>multicast-ingress** {**l2-mc** | **ip-mc**} command to enable one or the other. See the *7210 SAS-Mxp, R6, R12, S, Sx, T Interface Configuration Guide* for more information about this command. By default, IGMP snooping is enabled to be backward compatible. Users need to explicitly change the IGMP snooping configuration to allow processing of received multicast traffic as IP multicast in the context of Layer 3 service or R-VPLS.
- If a VPLS SAP is configured on the same port as the port on which IP multicast is enabled, then multicast traffic received on the SAP is dropped. Unicast, broadcast, and unknown-unicast packets received on the SAP are forwarded appropriately. This behavior is true only for VPLS SAPs and does not apply to VPLS SDPs, Epipe SAPs, and Epipe SDPs.
- With R-VPLS multicast, a port on which receivers are present can be configured to perform either Layer 2 multicast replication (that is, no IP TTL decrement and no source MAC replacement) or Layer 3 multicast replication (that is, IP TTL is decremented and source MAC is replaced with 7210 SAS

chassis MAC or IP interface MAC). An option to use either Layer 2 or Layer 3 multicast replication is available using the **configure>port>ethernet>multicast-egress** {**l2-switch** | **l3-forward**} command. See the *7210 SAS-Mxp, R6, R12, S, Sx, T Interface Configuration Guide* for more information about this command. All SAPs on the port have the same behavior.

- An MVR R-VPLS must be configured without an IP interface and supports Layer 2 forwarding of both unicast and multicast traffic (that is, no IP forwarding).
- A user R-VPLS can be configured with an IP interface and supports Layer 2 forwarding of both unicast and multicast (with (S,G) IP multicast replications) and supports Layer 3 forwarding of unicast traffic.
- On 7210 SAS-R6, when using SAP-based egress queues and scheduler, R-VPLS BUM traffic uses per port egress queues—not per SAP egress queues.
- In an MVR configuration, the **svc-sap-type** of the R-VPLS service that is the source (also known as MVR R-VPLS service) and the **svc-sap-type** of the R-VPLS service that is the sink (also known as user R-VPLS service) should match.
- On 7210 SAS-R6 and 7210 SAS-R12, the MVR R-VPLS service configured with IGMPv3 snooping shares resources with TWAMP. An increase in one decreases the amount of resources available for the other. Contact your Nokia representative for more information about scaling of these features.

5.4.8 Routed VPLS supported functionality and restrictions

Routed VPLS supported functionality and restrictions for network mode are specified as follows:

- Static ARP cannot be configured with an IES IP interface that is associated with an R-VPLS, though static MAC can be configured in an R-VPLS service.
- In network mode, both static routing and dynamic routing protocols are supported.
- Whenever a VPLS FIB entry is removed because of user action, aging or mac-move, the corresponding ARP entry whose MAC address matches that of the MAC in the FIB is removed from the ARP cache.
- In network mode, R-VPLS is supported in both the base routing instance (IES) and VPRN services. IPv4 addressing is supported for IES and VPRN IP interfaces associated with an R-VPLS service.
- IPv6 addressing support is not available for IES interfaces associated with an R-VPLS service.
- In both network modes, multiple SAPs configured on the same port cannot be part of the same R-VPLS Service. That is, a single service can only be configured with a single SAP on a specific port.
- Service MTU configuration is not supported in the R-VPLS service.
- In network mode, in any service (that is, svc-sap-type set to any), null SAP accepts only untagged packets. Tagged packets received are dropped.
- In network mode, MPLS protocols (For example: RSVP, LDP) cannot be enabled on R-VPLS IP interface
- In network mode, MPLS-TP cannot use R-VPLS, IES, and IP interface.
- In network mode, R-VPLS SAPS can be configured on a MC-LAG LAG.
- The discard-unknown feature is not supported in the VPLS service associated with R-VPLS (only on 7210 SAS-R6 and 7210 SAS-R12).
- In the saved configuration file, for the R-VPLS service, the R-VPLS service instance appears twice; one appearance for service creation and one with all the other configuration parameters. This is required to resolve references to the R-VPLS service and to execute the configuration without any errors.

- Service-based SHGs are not supported in an R-VPLS service.

5.5 Configuring a VPLS service with CLI

This section provides information to configure VPLS services using the command line interface.

5.5.1 Basic configuration

The following fields require specific input (there are no defaults) to configure a basic VPLS service:

- Customer ID (see Configuring customer accounts).
- For a local service, configure two SAPs, specifying local access ports and encapsulation values.
- For a distributed service, configure a SAP and an SDP for each far-end node.

Example: VPLS service on ALA-1

```
*A:ALA-1>config>service>vpls# info
----------------------------------------------
...
        vpls 9001 customer 6 create
            description "Local VPLS"
            stp
                shutdown
            exit
            sap 1/2/2:0 create
                description "SAP for local service"
            exit
            sap 1/1/5:0 create
                description "SAP for local service"
            exit
            no shutdown
----------------------------------------------
*A:ALA-1>config>service>vpls#
*A:ALA-1>config>service# info
----------------------------------------------
...
       vpls 7 customer 7 create
            stp
                shutdown
            exit
            sap 1/1/21 create
            exit
            sap lag-1:700 create
            exit
            no shutdown
        exit
...
----------------------------------------------
*A:ALA-1>config>service#
```

Example: Distributed VPLS service between ALA-1, ALA-2, and ALA-3

```
*A:ALA-1>config>service# info
----------------------------------------------
...
        vpls 9000 customer 6 create
```

```
            shutdown
            description "This is a distributed VPLS."
            stp
                shutdown
            exit
            sap 1/1/5:16 create
                description "VPLS SAP"
            exit
            spoke-sdp 2:22 create
            exit
        exit
...
-------------------------------------------
*A:ALA-1>config>service#

*A:ALA-2>config>service# info
-------------------------------------------
...
        vpls 9000 customer 6 create
            description "This is a distributed VPLS."
            stp
                shutdown
            exit
            sap 1/1/5:16 create
                description "VPLS SAP"
            exit
            spoke-sdp 2:22 create
            exit
            no shutdown
        exit
...
-------------------------------------------
*A:ALA-2>config>service#

*A:ALA-3>config>service# info
-------------------------------------------
...
        vpls 9000 customer 6 create
            description "This is a distributed VPLS."
            stp
                shutdown
            exit
            sap 1/1/3:33 create
                description "VPLS SAP"
            exit
            spoke-sdp 2:22 create
            exit
            no shutdown
        exit
...
-------------------------------------------
*A:ALA-3>config>service#
```

5.5.2 Common configuration tasks

About this task

This section provides a brief overview of the tasks that must be performed to configure both local VPLS services and provides the CLI commands.

For VPLS services:

Procedure

Step 1. Associate VPLS service with a customer ID.

Step 2. Define SAPs:

- Select nodes and ports.
- Optional - select QoS policies other than the default (configured in **config>qos** context).
- Optional — select filter policies (configured in **config>filter** context).
- Optional — select accounting policy (configured in **config>log** context).

Step 3. Modify STP default parameters (optional) (see VPLS and Spanning Tree Protocol).

Step 4. Enable service.

5.5.3 Configuring VPLS components

5.5.3.1 Creating a VPLS service

Use the following syntax to create a VPLS service.

```
   config>service# vpls service-id [customer customer-id] [create] [vpn vpn-id] [m-vpls]
description description-string
   no shutdown
```

Example: Configured VPLS service

```
*A:ALA-1>config>service>vpls# info
----------------------------------------------
...
        vpls 1000 customer 1 create
            description "This is a VPLS with NULL SAP"
            stp
                shutdown
            exit
            no shutdown
        exit
        vpls 2000 customer 6 create
            description "This is a Distributed VPLS with DOT1Q SAP"
            stp
                shutdown
            exit
            no shutdown
        exit
...
----------------------------------------------
*A:ALA-1>config>service>vpls#
```

5.5.3.1.1 Enabling MAC move

The **mac-move** feature is useful to protect against undetected loops in your VPLS topology as well as the presence of duplicate MACs in a VPLS service. For example, if two clients in the VPLS have the same

MAC address, the VPLS experiences a high relearn rate for the MAC and shuts down the SAP when the threshold is exceeded.

Use the following syntax to configure **mac-move** parameters.

```
config>service# vpls service-id [customer customer-id] [vpn vpn-id] [m-vpls]
    mac-move
    move-frequency frequency
    retry-timeout timeout
    no shutdown
```

Example: MAC move information

```
*A:ALA-1# show service id 6 all
....
*A:ALA-1#
-------------------------------------------------------------------------------
Forwarding Database specifics
-------------------------------------------------------------------------------
Service Id        : 1150               Mac Move          : Disabled
Mac Move Rate     : 2                  Mac Move Timeout  : 10
Table Size        : 1000               Total Count       : 1000
Learned Count     : 1000               Static Count      : 0
Remote Age        : 900                Local Age         : 300
High WaterMark    : 95%                Low Watermark     : 90%
Mac Learning      : Enabl              Discard Unknown   : Dsabl
Mac Aging         : Enabl              Relearn Only      : True
===============================================================================
....
*A:ALA-1#
```

5.5.3.1.2 Configuring STP bridge parameters in a VPLS

Modifying some of the Spanning Tree Protocol parameters allows the operator to balance STP between resiliency and speed of convergence extremes. Modifying particular parameters, mentioned as follows, must be done in the constraints of the following two formulae:

2 x (*Bridge_Forward_Delay* - 1.0 seconds) >= *Bridge_Max_Age*

Bridge_Max_Age >= 2 x (*Bridge_Hello0_Time* + 1.0 seconds)

STP always uses the locally configured values for the first three parameters (Admin State, Mode and Priority).

For the parameters Max Age, Forward Delay, Hello Time and Hold Count, the locally configured values are only used when this bridge has been elected root bridge in the STP domain, otherwise the values received from the root bridge are used. The exception to this rule is: when STP is running in RSTP mode, the Hello Time is always taken from the locally configured parameter. The other parameters are only used when running mode MSTP.

5.5.3.1.2.1 Bridge STP admin state

The administrative state of STP at the VPLS level is controlled by the shutdown command.

When STP on the VPLS is administratively disabled, any BPDUs are forwarded transparently through the 7210 SAS-R6 and 7210 SAS-R12. When STP on the VPLS is administratively enabled, but the administrative state of a SAP is down, BPDUs received on such a SAP are discarded.

```
config>service>vpls service-id# stp
    no shutdown
```

5.5.3.1.2.2 Mode

To be compatible with the different iterations of the IEEE 802.1D standard, the 7210 SAS-R6 and 7210 SAS-R12 support several variants of the Spanning Tree protocol:

- **rstp**

  Rapid Spanning Tree Protocol (RSTP) compliant with IEEE 802.1D-2004 - default mode.

- **dot1w**

  compliant with IEEE 802.1w

- **comp-dot1w**

  operation as in RSTP but backwards compatible with IEEE 802.1w (this mode was introduced for interoperability with some MTU types).

- **mstp**

  compliant with the Multiple Spanning Tree Protocol specified in IEEE 802.1Q REV/D5.0-09/2005. This mode of operation is only supported in an mVPLS.

- **pmstp**

  compliant with the Multiple Spanning Tree Protocol specified in IEEE 802.1Q REV/D3.0-04/2005 but with some changes to make it backwards compatible to 802.1Q 2003 edition and IEEE 802.1w.

See section Spanning tree operating modes for details on these modes.

```
config>service>vpls service-id# stp
    mode {rstp | comp-dot1w | dot1w | mstp | pmstp}
```

Default: rstp

5.5.3.1.2.3 Bridge priority

The **bridge-priority** command is used to populate the priority portion of the bridge ID field within outbound BPDUs (the most significant 4 bits of the bridge ID). It is also used as part of the decision process when determining the best BPDU between messages received and sent.

All values are truncated to multiples of 4096, conforming with IEEE 802.1t and 802.1D-2004.

```
config>service>vpls service-id# stp
    priority bridge-priority
```

Range: 1 to 65535

Default: 32768

Restore Default: no priority

5.5.3.1.2.4 Max age

The **max-age** command indicates how many hops a BPDU can traverse the network starting from the root bridge. The message age field in a BPDU transmitted by the root bridge is initialized to 0. Each other bridge takes the message_age value from BPDUs received on their root port and increment this value by 1. The message_age therefore reflects the distance from the root bridge. BPDUs with a message age exceeding max-age are ignored.

STP uses the max-age value configured in the root bridge. This value is propagated to the other bridges by the BPDUs. The default value of **max-age** is 20. This parameter can be modified within a range of 6 to 40, limited by the standard STP parameter interaction formulae.

```
config>service>vpls service-id# stp
    max-age max-info-age
```

Range: 6 to 40 seconds

Default: 20 seconds

Restore Default: no max-age

5.5.3.1.2.5 Forward delay

RSTP, as defined in the IEEE 802.1D-2004 standards, transitions to the forwarding state by a handshaking mechanism (rapid transition), without any waiting times. If handshaking fails (such as on shared links, as follows), the system falls back to the timer-based mechanism defined in the original STP (802.1D-1998) standard.

A shared link is a link with more than two Ethernet bridges (for example, a shared 10/100BaseT segment). The port-type command is used to configure a link as point-to-point or shared (see section SAP link type).

For timer-based transitions, the 802.1D-2004 standard defines an internal variable forward-delay, which is used in calculating the default number of seconds that a SAP spends in the discarding and learning states when transitioning to the forwarding state. The value of the forward-delay variable depends on the STP operating mode of the VPLS instance:

- In **rstp** mode, but only when the SAP has not fallen back to legacy STP operation, the value configured by the **hello-time** command is used.
- In all other situations, the value configured by the **forward-delay** command is used.

```
config>service>vpls service-id# stp
forward-delay seconds
```

Range: 4 to 30 seconds

Default: 15 seconds

Restore Default: no forward-delay

5.5.3.1.2.6 Hello time

The **hello-time** command configures the Spanning Tree Protocol (STP) hello time for the Virtual Private LAN Service (VPLS) STP instance.

The *seconds* parameter defines the default timer value that controls the sending interval between BPDU configuration messages by this bridge, on ports where this bridge assumes the designated role.

The active hello time for the spanning tree is determined by the root bridge (except when the STP is running in RSTP mode, then the hello time is always taken from the locally configured parameter).

The configured hello-time value can also be used to calculate the bridge forward delay, see Forward delay.

```
config>service>vpls service-id# stp
    hello-time hello-time
```

Range: 1 to 10 seconds

Default: 2 seconds

Restore Default: no hello-time

5.5.3.1.2.7 Hold count

The **hold-count** command configures the peak number of BPDUs that can be transmitted in a period of one second.

```
config>service>vpls service-id# stp
    hold-count count-value
```

Range: 1 to 10

Default: 6

Restore Default: no hold-count

5.5.3.1.2.8 MST instances

You can create up to 15 MST-instances. They can range from 1 to 4094. By changing path-cost and priorities, you can make sure that each instance forms its own tree within the region, therefore making sure different VLANs follow different paths.

You can assign non overlapping VLAN ranges to each instance. VLANs that are not assigned to an instance are implicitly assumed to be in instance 0, which is also called the CIST. This CIST cannot be deleted or created.

The parameter that can be defined per instance are **mst-priority** and **vlan-range**:

- **mst-priority**

  The bridge-priority for this specific mst-instance. It follows the same rules as bridge-priority. For the CIST, the bridge-priority is used.

- **vlan-range**

  The VLANs are mapped to this specific mst-instance. If no VLAN-ranges are defined in any mst-instances, then all VLANs are mapped to the CIST.

5.5.3.1.2.9 MST max hops

The mst-max-hops command defines the maximum number of hops the BPDU can traverse inside the region. Outside the region max-age is used.

5.5.3.1.2.10 MST name

The MST name defines the name that the operator gives to a region. Together with MST revision and the VLAN to MST-instance mapping, it forms the MST configuration identifier. Two bridges that have the same MST configuration identifier form a region if they exchange BPDUs.

5.5.3.1.2.11 MST revision

The MST revision together with MST-name and VLAN to MST-instance mapping define the MST configuration identifier. Two bridges that have the same MST configuration identifier form a region if they exchange BPDUs.

5.5.3.2 Configuring a VPLS SAP

A default QoS policy is applied to each ingress SAP. Additional QoS policies can be configured in the **config>qos** context. There are no default filter policies. Filter policies are configured in the **config>filter** context and must be explicitly applied to a SAP.

5.5.3.2.1 Local VPLS SAPs

To configure a local VPLS service, enter the **sap** *sap-id* command twice with different port IDs in the same service configuration.

Example: Local VPLS configuration

```
*A:ALA-1>config>service# info
----------------------------------------------
       vpls 1150 customer 1 create
            fdb-table-size 1000
            fdb-table-low-wmark 5
            fdb-table-high-wmark 80
            local-age 60
            stp
                shutdown
            exit
            sap 1/1/1:1155 create
            exit
            sap 1/1/2:1150 create
            exit
            no shutdown
        exit
----------------------------------------------
*A:ALA-1>config>service#
```

5.5.3.2.2 Distributed VPLS SAPs

To configure a distributed VPLS service, you must configure service entities on originating and far-end nodes. You must use the same service ID on all ends (for example, create a VPLS service ID 9000 on ALA-1, ALA-2, and ALA-3). A distributed VPLS consists of a SAP on each participating node and an SDP bound to each participating node.

For SDP configuration information, see Configuring an SDP. For SDP binding information, see Configuring SDP bindings .

Example: VPLS SAP configuration

```
*A:ALA-3>config>service# info
----------------------------------------------
      vpls 1150 customer 1 create
            fdb-table-size 1000
            fdb-table-low-wmark 5
            fdb-table-high-wmark 80
            local-age 60
            stp
                shutdown
            exit
            sap 1/1/1:1155 create
            exit
            sap 1/1/2:1150 create
            exit
            no shutdown
        exit
----------------------------------------------
*A:ALA-3>config>service#
```

5.5.3.2.3 Configuring SAP-specific STP parameters

When a VPLS has STP enabled, each SAP within the VPLS has STP enabled by default.

5.5.3.2.3.1 SAP STP administrative state

The administrative state of STP within a SAP controls how BPDUs are transmitted and handled when received. The allowable states are:

- **SAP Admin Up**

  The default administrative state is *up* for STP on a SAP. BPDUs are handled in the normal STP manner on a SAP that is administratively up.

- **SAP Admin Down**

  An administratively down state allows a service provider to prevent a SAP from becoming operationally blocked. BPDUs do not originate out the SAP toward the customer.

- If STP is enabled on VPLS level, but disabled on the SAP, received BPDUs are discarded. Discarding the incoming BPDUs allows STP to continue to operate within the VPLS service while ignoring the down SAP. The specified SAP is always in an operationally forwarding state.

Note: The administratively down state allows a loop to form within the VPLS.

```
config>service>vpls>sap>stp#
    [no] shutdown
```

Range: shutdown or no shutdown

Default: no shutdown (SAP admin up)

5.5.3.2.3.2 SAP virtual port number

The virtual port number uniquely identifies a SAP within configuration BPDUs. The internal representation of a SAP is unique to a system and has a reference space much bigger than the 12 bits definable in a configuration BPDU. STP takes the internal representation value of a SAP and identifies it with it's own virtual port number that is unique to every other SAP defined on the VPLS. The virtual port number is assigned at the time that the SAP is added to the VPLS.

Because the order in which SAPs are added to the VPLS is not preserved between reboots of the system, the virtual port number may change between restarts of the STP instance. To achieve consistency after a reboot, the virtual port number can be specified explicitly.

```
config>service>vpls>sap# stp
    port-num number
```

Range: 1 — 2047

Default: (automatically generated)

Restore Default: no port-num

5.5.3.2.3.3 SAP priority

SAP priority allows a configurable "tie breaking" parameter to be associated with a SAP. When configuration BPDUs are being received, the configured SAP priority is used in some circumstances to determine whether a SAP is designated or blocked.

In traditional STP implementations (802.1D-1998), this field is called the port priority and has a value of 0 to 255. This field is coupled with the port number (0 to 255 also) to create a 16 bit value. In the latest STP standard (802.1D-2004) only the upper 4 bits of the port priority field are used to encode the SAP priority. The remaining 4 bits are used to extend the port ID field into a 12 bit virtual port number field. The virtual port number uniquely references a SAP within the STP instance. See SAP virtual port number for details on the virtual port number.

STP computes the actual SAP priority by taking the configured priority value and masking out the lower four bits. The result is the value that is stored in the SAP priority parameter. For example, if a value of 0 was entered, masking out the lower 4 bits would result in a parameter value of 0. If a value of 255 was entered, the result would be 240.

The default value for SAP priority is 128. This parameter can be modified within a range of 0 to 255, 0 being the highest priority. Masking causes the values actually stored and displayed to be 0 to 240, in increments of 16.

```
config>service>vpls>sap>stp#
```

```
    priority stp-priority
```

Range: 0 to 255 (240 largest value, in increments of 16)

Default: 128

Restore Default: no priority

5.5.3.2.3.4 SAP path cost

The SAP path cost is used by STP to calculate the path cost to the root bridge. The path cost in BPDUs received on the root port is incremental with the configured path cost for that SAP. When BPDUs are sent out other egress SAPs, the newly calculated root path cost is used.

STP suggests that the path cost is defined as a function of the link bandwidth. Because SAPs are controlled by complex queuing dynamics, in the the STP path cost is a purely static configuration.

The default value for SAP path cost is 10. This parameter can be modified within a range of 1 to 65535, 1 being the lowest cost.

```
config>service>vpls>sap>stp#
    path-cost sap-path-cost
```

Range: 1 to 200000000

Default: 10

Restore Default: no path-cost

5.5.3.2.3.5 SAP edge port

The SAP **edge-port** command is used to reduce the time it takes a SAP to reach the forwarding state when the SAP is on the edge of the network, and therefore has no further STP bridge to handshake with.

The **edge-port** command is used to initialize the internal OPER_EDGE variable. At any time, when OPER_EDGE is false on a SAP, the normal mechanisms are used to transition to the forwarding state (see Forward delay). When OPER_EDGE is true, STP assumes that the remote end agrees to transition to the forwarding state without actually receiving a BPDU with an agreement flag set.

The OPER_EDGE variable is dynamically set to false if the SAP receives BPDUs (the configured **edge-port** value does not change). The OPER_EDGE variable is dynamically set to true if auto-edge is enabled and STP concludes there is no bridge behind the SAP.

When STP on the SAP is administratively disabled and re-enabled, the OPER_EDGE is reinitialized to the value configured for **edge-port**.

Valid values for SAP **edge-port** are enabled and disabled with disabled being the default.

```
config>service>vpls>sap>stp#
    [no] edge-port
```

Default: **no edge-port**

5.5.3.2.3.6 SAP auto edge

The SAP **edge-port** command is used to instruct STP to dynamically decide whether the SAP is connected to another bridge.

If auto-edge is enabled, and STP concludes there is no bridge behind the SAP, the OPER_EDGE variable is dynamically set to true. If auto-edge is enabled, and a BPDU is received, the OPER_EDGE variable is dynamically set to true (see SAP edge port).

Valid values for SAP auto-edge are enabled and disabled with enabled being the default.

```
config>service>vpls>sap>stp#
    [no] auto-edge
```

Default: auto-edge

5.5.3.2.3.7 SAP link type

The SAP **link-type** parameter instructs STP on the maximum number of bridges behind this SAP. If there is only a single bridge, transitioning to forwarding state is based on handshaking (fast transitions). If more than two bridges are connected by a shared media, their SAPs should all be configured as shared, and timer-based transitions are used.

Valid values for SAP link-type are shared and pt-pt with pt-pt being the default.

```
config>service>vpls>sap>stp#
    link-type {pt-pt|shared}
```

Default: link-type pt-pt

Restore Default: no link-type

5.5.3.2.3.8 MST instances

The SAP mst-instance command is used to create MST instances at the SAP level. MST instance at a SAP level can be created only if MST instances are defined at the service level.

The parameters that can be defined per instance are **mst-path-cost** and **mst-port-priority**:

- **mst-path-cost**

  Specifies path-cost within a specific MST instance. The path-cost is proportional to link speed.

- **mst-port-priority**

  Specifies the port priority within a specific MST instance.

5.5.3.2.4 STP SAP operational states

The operational state of STP within a SAP controls how BPDUs are transmitted and handled when received.

5.5.3.2.4.1 Operationally disabled

Operationally disabled is the normal operational state for STP on a SAP in a VPLS that has any of the following conditions:

- VPLS state administratively down
- SAP state administratively down
- SAP state operationally down

If the SAP enters the operationally up state with the STP administratively up and the SAP STP state is up, the SAP transitions to the STP SAP discarding state.

When, during normal operation, the router detects a downstream loop behind a SAP, BPDUs can be received at a very high rate. To recover from this situation, STP transitions the SAP to disabled state for the configured forward-delay duration.

5.5.3.2.4.2 Operationally discarding

A SAP in the discarding state only receives and sends BPDUs, building the local correct STP state for each SAP while not forwarding actual user traffic. The duration of the discarding state is described in section Forward delay.

Note: In previous versions of the STP standard, the discarding state was called a blocked state.

5.5.3.2.4.3 Operationally learning

The learning state allows population of the MAC forwarding table before entering the forwarding state. In this state, no user traffic is forwarded.

5.5.3.2.4.4 Operationally forwarding

Configuration BPDUs are sent out a SAP in the forwarding state. Layer 2 frames received on the SAP are source learned and destination forwarded according to the FIB. Layer 2 frames received on other forwarding interfaces and destined for the SAP are also forwarded.

5.5.3.2.4.5 SAP BPDU encapsulation state

IEEE 802.1d (referred as dot1d) and Cisco per-VLAN Spanning Tree (PVST) BPDU encapsulations are supported on a per SAP basis. The STP is associated with a VPLS service like PVST is per VLAN. The difference between the two encapsulations is in the Ethernet and LLC framing and a type-length-value (TLV) field trailing the BPDU.The encapsulation format cannot be configured by the user; the system automatically determines the encapsulation format based on the BPDUs received on the port.

The following table shows differences between Dot1d and PVST Ethernet BPDU encapsulations based on the interface encap-type field:

Table 51: SAP BPDU encapsulation states

Field	dot1d encap-type null	dot1d encap-type dot1q	PVST encap-type null	PVST encap-type dot1q
Destination MAC	01:80:c2:00:00:00	01:80:c2:00:00:00	N/A	01:00:0c:cc:cc:cd
Source MAC	Sending Port MAC	Sending Port MAC	N/A	Sending Port MAC
EtherType	N/A	0x81 00	N/A	0x81 00
Dot1p and CFI	N/A	0xe	N/A	0xe
Dot1q	N/A	VPLS SAP ID	N/A	VPLS SAP encap value
Length	LLC Length	LLC Length	N/A	LLC Length
LLC DSAP SSAP	0x4242	0x4242	N/A	0xaaaa (SNAP)
LLC CNTL	0x03	0x03	N/A	0x03
SNAP OUI	N/A	N/A	N/A	00 00 0c (Cisco OUI)
SNAP PID	N/A	N/A	N/A	01 0b
CONFIG	Standard 802.1d	Standard 802.1d	N/A	Standard 802.1d
TLV: Type & Len	N/A	N/A	N/A	58 00 00 00 02
TLV: VLAN	N/A	N/A	N/A	VPLS SAP encap value
Padding	As Required	As Required	N/A	As Required

Each SAP has a Read-Only operational state that shows which BPDU encapsulation is currently active on the SAP. The states are:

- **Dot1d**

  This state specifies that the switch is currently sending IEEE 802.1d standard BPDUs. The BPDUs are tagged or non-tagged based on the encapsulation type of the egress interface and the encapsulation value defined in the SAP. A SAP defined on an interface with encapsulation type dot1q continues in the dot1d BPDU encapsulation state until a PVST encapsulated BPDU is received, in which case the SAP converts to the PVST encapsulation state. Each received BPDU must be properly IEEE 802.1q tagged if the interface encapsulation type is defined as dot1q. PVST BPDUs are silently discarded if received when the SAP is on an interface defined with encapsulation type null.

- **PVST**

  This state specifies that the switch is currently sending proprietary encapsulated BPDUs. PVST BPDUs are only supported on Ethernet interfaces with the encapsulation type set to dot1q. The SAP continues in the PVST BPDU encapsulation state until a dot1d encapsulated BPDU is received, in which case, the SAP reverts to the dot1d encapsulation state. Each received BPDU must be properly IEEE 802.1q tagged with the encapsulation value defined for the SAP. PVST BPDUs are silently discarded if received when the SAP is on an interface defined with a null encapsulation type.

Dot1d is the initial and only SAP BPDU encapsulation state for SAPs defined on Ethernet interface with encapsulation type set to null.

5.5.3.2.5 Configuring VPLS SAPs with per service split horizon

To configure a VPLS service with a split horizon group, add the **split-horizon-group** parameter when creating the SAP. Traffic arriving on a SAP within a split horizon group is not copied to other SAPs in the same split horizon group.

Example: VPLS with split horizon enabled

```
*A:ALA-1>config>service# info
----------------------------------------------
...
vpls 800 customer 6001 vpn 700 create
description "VPLS with split horizon for DSL"
stp
shutdown
exit
sap 1/1/3:100 split-horizon-group DSL-group1 create
description "SAP for residential bridging"
exit
sap 1/1/3:200 split-horizon-group DSL-group1 create
description "SAP for residential bridging"
exit
split-horizon-group DSL-group1
description "Split horizon group for DSL"
exit
no shutdown
exit
...
----------------------------------------------
*A:ALA-1>config>service#
```

5.5.3.3 Configuring SDP bindings

VPLS provides scaling and operational advantages. A hierarchical configuration eliminates the need for a full mesh of VCs between participating devices. Hierarchy is achieved by enhancing the base VPLS core mesh of VCs with access VCs (spoke) to form two tiers. Spoke SDPs are generally created between Layer 2 switches and placed at the Multi-Tenant Unit (MTU). The PE routers are placed at the service provider's Point of Presence (POP). Signaling and replication overhead on all devices is considerably reduced.

A spoke-SDP is treated like the equivalent of a traditional bridge port where flooded traffic received on the spoke-SDP is replicated on all other "ports" (other spoke SDPs or SAPs) and not transmitted on the port it was received (unless a split horizon group was defined on the spoke-SDP, see section Configuring VPLS spoke SDPs with split horizon).

A spoke-SDP connects a VPLS service between two sites and, in its simplest form, could be a single tunnel LSP. A set of ingress and egress VC labels are exchanged for each VPLS service instance to be transported over this LSP. The PE routers at each end treat this as a virtual spoke connection for the VPLS service in the same way as the PE-MTU connections. This architecture minimizes the signaling overhead and avoids a full mesh of VCs and LSPs between the two metro networks.

A VC-ID can be specified with the SDP-ID. The VC-ID is used instead of a label to identify a virtual circuit. The VC-ID is significant between peer SRs on the same hierarchical level. The value of a VC-ID is conceptually independent from the value of the label or any other datalink specific information of the VC.

5.5.3.3.1 Configuring VPLS spoke SDPs with split horizon

To configure spoke SDPs with a split horizon group, add the split-horizon-group parameter when creating the spoke-SDP. Traffic arriving on a SAP or spoke-SDP within a split horizon group is not copied to other SAPs or spoke SDPs in the same split horizon group.

Example: VPLS with split horizon enabled

```
*A:ALA-1>config>service# info
----------------------------------------------
...
vpls 800 customer 6001 vpn 700 create
description "VPLS with split horizon for DSL"
stp
shutdown
exit
spoke-sdp 51:15 split-horizon-group DSL-group1 create
exit
split-horizon-group DSL-group1
description "Split horizon group for DSL"
exit
no shutdown
exit
...
----------------------------------------------
*A:ALA-1>config>service#
```

5.5.4 Configuring VPLS redundancy

This section describes the service management tasks.

5.5.4.1 Creating a management VPLS for SAP protection

About this task

This section provides a brief overview of the tasks that must be performed to configure a management VPLS for SAP protection and provides the CLI commands, see Figure 61: Example configuration for protected VPLS SAP. The following tasks should be performed on both nodes providing the protected VPLS service.

Before configuring a management VPLS, first read VPLS redundancy for an introduction to the concept of management VPLS and SAP redundancy:

Procedure

Step 1. Create an SDP to the peer node.

Step 2. Create a management VPLS.

Step 3. Define a SAP in the m-vpls on the port. Note that the port must be dot1q. The SAP corresponds to the (stacked) VLAN on the 7210 SAS-R6 and 7210 SAS-R12 in which STP is active.

Step 4. Optionally modify STP parameters for load balancing (see Configuring load balancing with management VPLS).

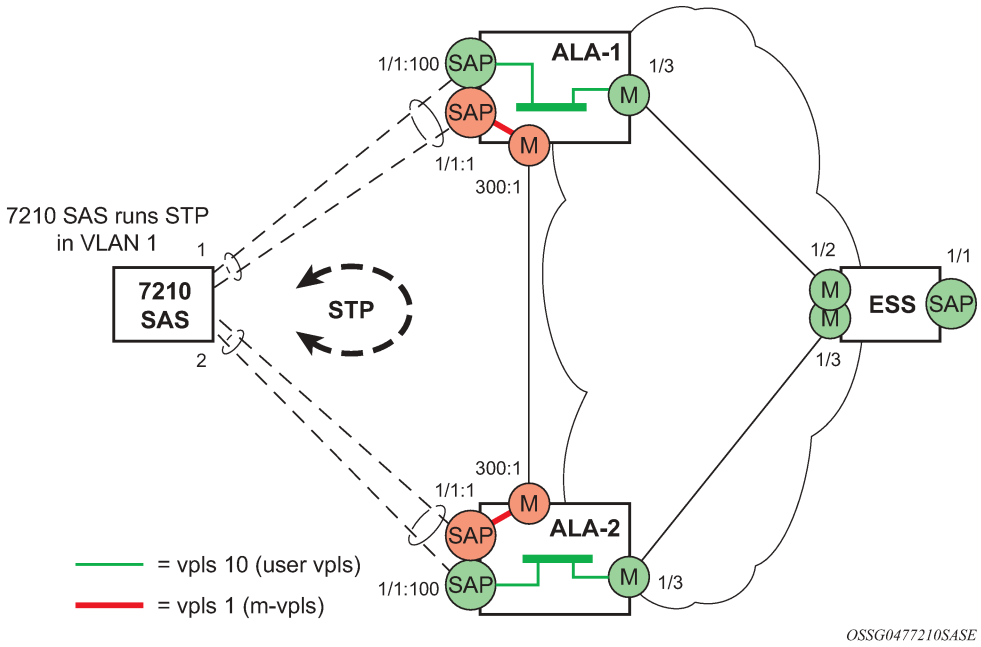
Step 5. Create an SDP in the m-vpls using the SDP defined in Step 1. Ensure that this SDP runs over a protected LSP.

Step 6. Enable the management VPLS service and verify that it is operationally up.

Step 7. Create a list of VLANs on the port that are to be managed by this management VPLS.

Step 8. Create one or more user VPLS services with SAPs on VLANs in the range defined by Step 6.

Figure 61: Example configuration for protected VPLS SAP



Example: Creating a management VPLS for SAP protection

Use the following commands to create a management VPLS for SAP protection.

```
config>service# vpls service-id [customer customer-id] [create] [m-vpls]
    description description-string
    sap sap-id create
    managed-vlan-list
        range vlan-range
            stp
            no shutdown
```

The following example shows output for a configured management VPLS.

```
*A:ALA-1>config>service# info
----------------------------------------------
        vpls 2000 customer 6 m-vpls create
            stp
                no shutdown
            exit
            sap 1/1/1:100 create
            exit
            sap 1/1/2:200 create
            exit
```

```
            sap 1/1/3:300 create
               managed-vlan-list
                  range 1-50
            exit
            no shutdown
        exit
----------------------------------------------
*A:ALA-1>config>service#
```

5.5.4.2 Creating a management VPLS for spoke-SDP protection

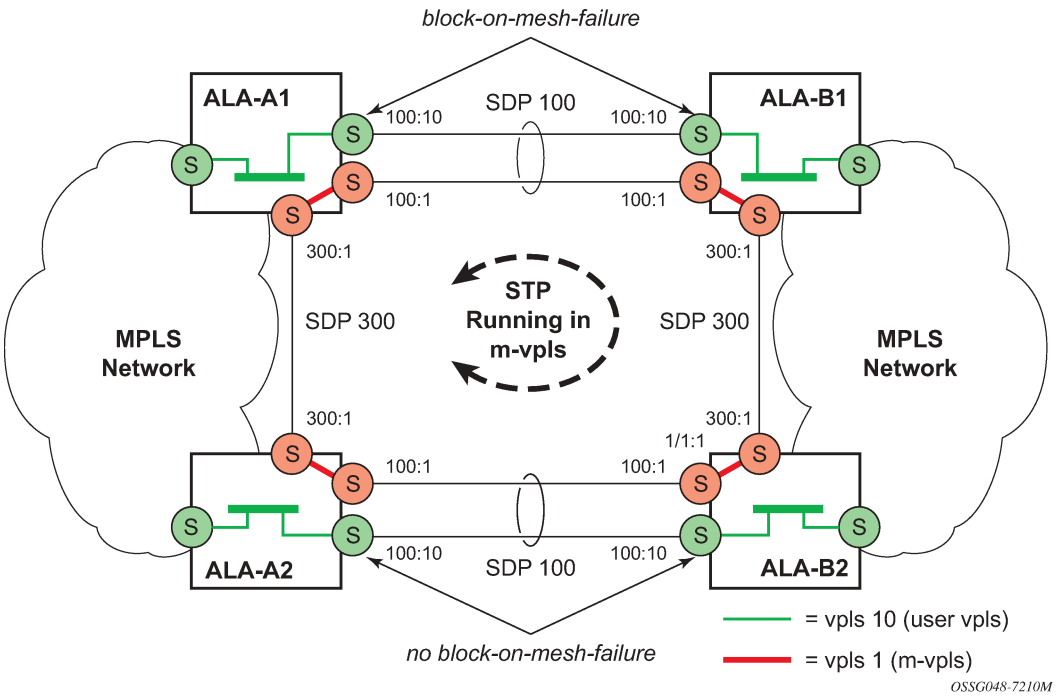
This section provides a brief overview of the tasks that must be performed to configure a management VPLS for spoke-SDP protection and provides the CLI commands, see Figure 62: Example configuration for protected VPLS spoke-SDP. The following tasks should be performed on all four nodes providing the protected VPLS service.

Before configuring a management VPLS, please first read Configuring a VPLS SAP for an introduction to the concept of management VPLS and spoke-SDP redundancy:

1. Create an SDP to the local peer node (node ALA-A2 in the following example).
2. Create an SDP to the remote peer node (node ALA-B1 in the following example).
3. Create a management VPLS.
4. Create a spoke-SDP in the m-vpls using the SDP defined in Step 1. Ensure that this mesh spoke-SDP runs over a protected LSP (see following note).
5. Enable the management VPLS service and verify that it is operationally up.
6. Create a spoke-SDP in the m-vpls using the SDP defined in Step 2. Optionally, modify STP parameters for load balancing.
7. Create one or more user VPLS services with spoke SDPs on the tunnel SDP defined by Step 2.

As long as the user spoke SDPs created in step 7are in this same tunnel SDP with the management spoke-SDP created in step 6, the management VPLS protect them.

Figure 62: Example configuration for protected VPLS spoke-SDP



Use the following CLI syntax to create a management VPLS for spoke-SDP protection:

```
config>service# sdp sdp-id mpls create
    far-end ip-address
    lsp lsp-name
    no shutdown
vpls service-id customer customer-id [m-vpls] create
    description description-string
    spoke-sdp sdp-id:vc-id create
    stp
    no shutdown
```

Example: VPLS configuration output

```
*A:ALA-A1>config>service# info
----------------------------------------------
...
       sdp 100 mpls create
            far-end 10.0.0.30
            lsp "toALA-B1"
            no shutdown
       exit
       sdp 300 mpls create
            far-end 10.0.0.20
            lsp "toALA-A2"
            no shutdown
       exit
       vpls 101 customer 1 m-vpls create
            spoke-sdp 100:1 create
            exit
            spoke-sdp 300:1 create
            exit
```

```
            stp
            exit
            no shutdown
        exit
...
----------------------------------------------
*A:ALA-A1>config>service#
```

5.5.4.3 Configuring a BGP-auto-discovery

```
config>service# sdp-template sdp-template-id
config>service# l2-auto-bind policy-id [use-provisioned-sdp]
```

BGP-AD automatically creates SDP-bindings using a template to configure SDP-binding configuration parameters. L2-auto-bind is a command used to initiate a template that is used by BGP-AD for PW instantiation under related VPLS instances.

The template may be referenced in the "service vpls bgp-ad" object and used subsequently to instantiate PWs to a remote PE and VSI instance advertised through BGP Auto-Discovery. Changes to these dynamically created objects cannot be performed directly through CLI or SNMP. There are two possible methods to initiate the change:

- Configure a new "l2-auto-bind" association under service>vpls>bgp-ad. This method is used when the existing policy is used by multiple VPLS services and only one or a few require the change.
- Change the parameters of the current template. This method is used when a change in parameter is required for the majority of VPLS services that use the template.

Changes are not automatically propagated to the instantiated objects and must be done through one of two tool commands:

```
tools>perform>service# eval-pw-template policy-id [allow-service-impact]
tools>perform>service>id# eval-pw-template policy-id [allow-service-impact]
```

This command forces evaluation of changes that were made in the l2-auto-bind template indicated in the command. This command can be applied to an individual VPLS service or all VPLS services that reference the template if no service is specified.

The parameters are divided into three classes:

- class 1 - modified at create time only
- class 2 - modified only when the object is administratively shutdown
- class 3 - no restrictions

Parameters that fall into class 1 destroy existing objects and recreate objects with the new values. Parameters in class 2 momentarily shutdown the object, change the parameter, then re-enable the object. Class 3 can be changed without affecting the operational status of the objects of service.

For the l2-auto-bind template, the parameters are treated as follows:

- class 1 - adding or removing a split-horizon-group, switching between a manual and auto SDP
- class 2 - changing the **vc-type** {**ether** | **vlan**}
- class 3 - all other changes

The keyword allow-service-impact enables service impacting changes. If this keyword is not configured, an error message is generated if the parameter changes are service impacting.

5.5.4.4 Configuring load balancing with management VPLS

With the concept of management VPLS, it is possible to load balance the user VPLS services across the two protecting nodes. This is done by creating two management VPLS instances, where both instances have different active spokes (by changing the STP path-cost). When different user VPLS services are associated with either the two management VPLS services, the traffic is split across the two spokes.

Load balancing can be achieved in both the SAP protection and spoke-SDP protection scenarios. Figure 63: Example configuration for load balancing across two protected VPLS spoke SDPs shows an example with the following configuration.

- Dut-C - spoke-SDP

```
mvpls 100
MVPLS M1
Dut-A – Spoke SDP 1201:100 (STP blocked); 1401:100
Dut-B – Spoke SDP 1201:100; 2301:100
```

- Dut-C - Spoke-SDP 1401:100; 2301:100

```
uvpls 101
UVPLS U1
Dut-A – Spoke SDP 1201:101; 1401:101
Dut-B – Spoke SDP 1201:101; 2301:101
```

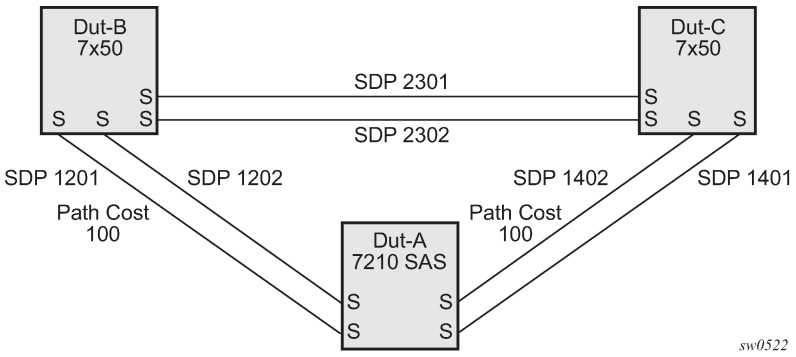
- Dut-C - Spoke-SDP 1401:101; 2301:101

```
mvpls 200
MVPLSM2
Dut-A – Spoke SDP 1202:200; 1402:200 (STP blocked)
Dut-B – Spoke SDP 1202:200; 2302:200
```

- Dut-C - Spoke-SDP 1402:200; 2302:200

```
uvpls 201
UVPLS U2
Dut-A – Spoke SDP 1202:201; 1402:201
Dut-B – Spoke SDP 1202:201; 2302:201
Dut-C – Spoke SDP 1402:201; 2302:201
```

Figure 63: Example configuration for load balancing across two protected VPLS spoke SDPs



Use the following syntax to create a load balancing across two management VPLS instances:

```
config>service# sdp sdp-id mpls create
    far-end ip-address
    lsp lsp-name
    no shutdown
vpls service-id customer customer-id [m-vpls] create
    description description-string
    spoke-sdp sdp-id:vc-id create
    stp
        path-cost
    stp
    no shutdown
```

The following examples show configurations for load balancing across two protected VPLS spoke SDPs.

Example: ALA-B configuration

The configuration on ALA-B (7210), the upper left node is shown as follows. It is configured such that it becomes the root bridge for MVPLS 100 and MVPLS 200.

```
# MVPLS 100 configs

*A:ALA-B# configure service vpls 100
*A:ALA-B>config>service>vpls# info
----------------------------------------------
            description "Default tls description for service id 100"
            stp
                priority 0
                no shutdown
            exit
            spoke-sdp 1201:100 create
            exit
            spoke-sdp 2301:100 create
            exit
            no shutdown
----------------------------------------------
*A:ALA-B>config>service>vpls#

# UVPLS 101 configs

*A:ALA-B>config>service# vpls 101
*A:ALA-B>config>service>vpls# info
----------------------------------------------

            description "Default tls description for service id 101"
            spoke-sdp 1201:101 create
            exit
            spoke-sdp 2301:101 create
            exit
            no shutdown
----------------------------------------------
*A:ALA-B>config>service>vpls#

# MVPLS 200 configs

*A:ALA-B# configure service vpls 200
*A:ALA-B>config>service>vpls# info
----------------------------------------------
            description "Default tls description for service id 200"
            stp
                priority 0
                no shutdown
```

```
            exit
            spoke-sdp 1202:200 create
            exit
            spoke-sdp 2302:200 create
            exit
            no shutdown
-----------------------------------------------
*A:ALA-B>config>service>vpls#


# UVPLS 201 configs
*A:ALA-B>config>service# vpls 201
*A:ALA-B>config>service>vpls# info
-----------------------------------------------

            description "Default tls description for service id 201"
            spoke-sdp 1202:201 create
            exit
            spoke-sdp 2302:201 create
            exit
            no shutdown
-----------------------------------------------
*A:ALA-B>config>service>vpls#
```

Example: ALA-C configuration

The configuration on ALA-C (7210), the upper right node is shown as follows.

```
# MVPLS 100 configs

*A:ALA-C# configure service vpls 100
*A:ALA-C>config>service>vpls# info
-----------------------------------------------

            description "Default tls description for service id 100"
            stp
                priority 4096
                no shutdown
            exit
            spoke-sdp 1401:100 create
            exit
            spoke-sdp 2301:100 create
            exit
            no shutdown
-----------------------------------------------
*A:ALA-C>config>service>vpls#


# UVPLS 101 configs

*A:ALA-C>config>service# vpls 101
*A:ALA-C>config>service>vpls# info
-----------------------------------------------

            description "Default tls description for service id 101"
            spoke-sdp 1401:101 create
            exit
            spoke-sdp 2301:101 create
            exit
            no shutdown
-----------------------------------------------
```

```
*A:ALA-C>config>service>vpls#
```

```
# MVPLS 200 configs

*A:ALA-C# configure service vpls 200
*A:ALA-C>config>service>vpls# info
----------------------------------------------
            description "Default tls description for service id 200"
            stp
                priority 4096
                no shutdown
            exit
            spoke-sdp 1402:200 create
            exit
            spoke-sdp 2302:200 create
            exit
            no shutdown
----------------------------------------------
*A:ALA-C>config>service>vpls#


# UVPLS 201 configs

*A:ALA-C>config>service# vpls 201
*A:ALA-C>config>service>vpls# info
----------------------------------------------

            description "Default tls description for service id 201"
            spoke-sdp 1402:201 create
            exit
            spoke-sdp 2302:201 create
            exit
            no shutdown
----------------------------------------------
*A:ALA-C>config>service>vpls#
```

5.5.4.5 Configuring selective MAC Flush

Use the following syntax to enable selective MAC Flush in a VPLS.

```
config>service# vpls service-id
    send-flush-on-failure
```

Use the following syntax to disable selective MAC Flush in a VPLS.

```
config>service# vpls service-id
    no send-flush-on-failure
```

5.5.5 Configuring IGMPv3 snooping in RVPLS

IGMPv3 snooping in RVPLS is supported only for IES (not for VPRNs).

Use the following syntax to configure IGMPv3 snooping in routed VPLS bound to an IES.

```
config>service# vpls service-id customer customer-id [svc-sap-type {any}] [b-vpls | i-vpls | r-
vpls] create
```

```
config>service>vpls# service-name service-name
config>service>vpls# allow-ip-int-bind
config>service>vpls>allow-ip-int-bind# exit
config>service>vpls# igmp-snooping
config>service>vpls>igmp-snooping# no shutdown
config>service>vpls# exit
config>service>vpls# sap sap-id create
config>service>vpls>sap# igmp-snooping
config>service>vpls>sap>igmp-snooping# mrouter-port
config>service>vpls>sap>igmp-snooping# exit
config>service>vpls>sap># exit
config>service>vpls># exit
config>service# ies service-id customer customer-id create
config>service>ies# interface ip-int-name create
config>service>ies>interface# address ip-address/mask
config>service>ies>interface# vpls service-name
```

Example: RVPLS configuration using IGMPv3 snooping

```
#--------------------------------------------------
echo "Port Configuration"
#--------------------------------------------------

    ...snip...

    port 1/1/5
        ethernet
            mode hybrid
            access
            exit
            encap-type dot1q
            multicast-ingress ip-mc
        exit
        no shutdown
    exit

#--------------------------------------------------
```

```
#--------------------------------------------------
echo "Service Configuration"
#--------------------------------------------------
    service
        customer 1 create
            description "Default customer"
        exit
        ies 6 customer 1 create
            interface "IGMP-test" create
            exit
        exit

        ....snip

        vpls 3 customer 1 r-vpls svc-sap-type any create
            allow-ip-int-bind
            exit
            stp
                shutdown
            exit
            igmp-snooping
                no shutdown
            exit
            service-name "GS-IGMP-Snooping"
```

```
            sap 1/1/5:333 create
                igmp-snooping
                    mrouter-port
                exit
                ingress
                exit
                egress
                exit
            exit

        ....snip

        ies 6 customer 1 create
            interface "IGMP-test" create
                address 192.168.x.x/24
                vpls "GS-IGMP-Snooping"
                exit
            exit
            no shutdown
        exit
    exit
#---------------------------------------------------
```

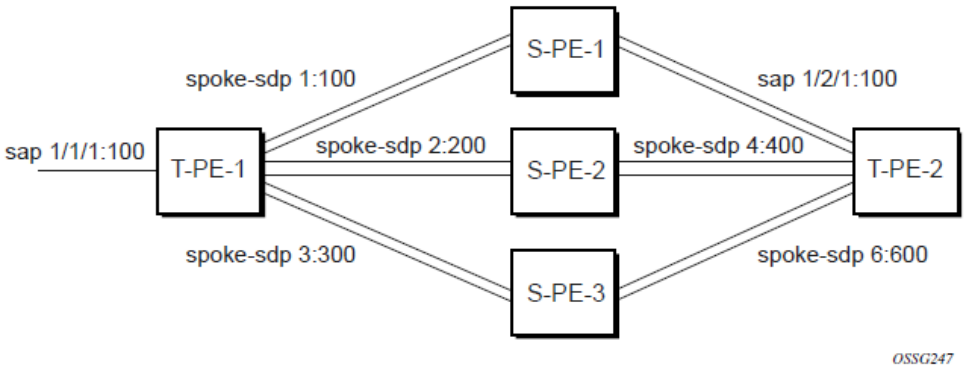
5.5.6 Configuring BGP Auto-Discovery

This section provides important information to describe the different configuration options used to populate the required BGP AD and generate the LDP generalized pseudowire-ID FEC fields. There are a large number of configuration options that are available with the this feature. Not all these configurations option are required to start using BGP AD. A very simple configuration automatically generates the required values used by BGP and LDP. In most cases, deployments provide full mesh connectivity between all nodes across a VPLS instance. However, capabilities are available to influence the topology and build hierarchies or hub and spoke models.

5.5.6.1 Configuration steps

In the following figure, assume PE6 was previously configured with VPLS 100 as indicated by the configurations lines in the upper right. The BGP AD process commences after PE134 is configured with the VPLS 100 instance as shown in the upper left. This shows a very basic and simple BGP AD configuration. The minimum requirement for enabling BGP AD on a VPLS instance is configuring the VPLS-ID and point to a pseudowire template.

Figure 64: BGP AD configuration example



In many cases, VPLS connectivity is based on a pseudowire mesh. To reduce the configuration requirement, the BGP values can be automatically generated using the VPLS-ID and the MPLS router-ID. By default, the lower six bytes of the VPLS-ID are used to generate the RD and the RT values. The VSI-ID value is generated from the MPLS router-ID. All of these parameters are configurable and can be coded to suit requirements and build different topologies

A helpful command displays the service information, the BGP parameters and the SDP bindings in use. When the discovery process is completed successfully, each endpoint has an entry for the service.

```
PE134>#  show service l2-route-table
```

When only one of the endpoints has an entry for the service in the l2-routing-table, it is most likely a problem with the RT values used for import and export. This would most likely happen when different import and export RT values are configured using a router policy or the route-target command.

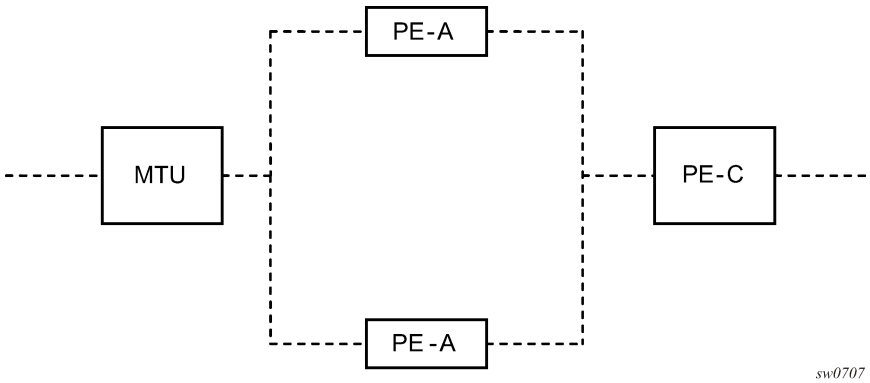
Service-specific commands continue to be available to display service-specific information, including status.

```
PERs6# show service sdp-using
```

BGP AD advertises the VPLS-ID in the extended community attribute, VSI-ID in the NLRI and the local PE ID in the BGP next hop. At the receiving PE, the VPLS-ID is compared against locally provisioned information to determine whether the two PEs share a common VPLS. If it is found that they do, the BGP information is used in the signaling phase.

5.5.7 Configuring AS pseudowire in VPLS

Figure 65: Sample topology-AS pseudowire in VPLS



In the preceding figure, a pseudowire is configured on MTU. The following example shows configuration output on the MTU.

Example: MTU pseudowire configuration

```
*A:MTU>config>service>vpls# info
----------------------------------------------
            send-flush-on-failure
            stp
                shutdown
            exit
            endpoint "vpls1" create
                description "vpls1_endpoint"
                revert-time 60
                ignore-standby-signaling
                no suppress-standby-signaling
                block-on-mesh-failure
            exit
            sap 1/1/3 create
            exit
            spoke-sdp 301:1 endpoint "vpls1" create
                stp
                    shutdown
                exit
                block-on-mesh-failure
            exit
            spoke-sdp 302:1 endpoint "vpls1" create
                stp
                    shutdown
                exit
                block-on-mesh-failure
            exit
            no shutdown
----------------------------------------------
*A:MTU>config>service>vpls#
```

5.6 Service management tasks

5.6.1 Modifying VPLS service parameters

You can change existing service parameters. The changes are applied immediately. To display a list of services, use the **show>service>service-using vpls** command. Enter the parameter such as description SAP and then enter the new information.

Example: Modifying VPLS service parameters

```
*A:ALA-1>config>service>vpls# info
----------------------------------------------
            description "This is a different description."
            disable-learning
            disable-aging
            discard-unknown
            local-age 500
            stp
                shutdown
            exit
            sap 1/1/5:22 create
                description "VPLS SAP"
            exit
            exit
            no shutdown
----------------------------------------------
*A:ALA-1>config>service>vpls#
```

5.6.2 Modifying management VPLS parameters

To modify the range of VLANs on an access port that are to be managed by an existing management VPLS, first the new range should be entered and afterwards the old range removed. If the old range is removed before a new range is defined, all customer VPLS services in the old range become unprotected and may be disabled.

```
config>service# vpls service-id
    - sap sap-id
        - managed-vlan-list
            - [no] range vlan-range
```

5.6.3 Deleting a management VPLS

As with normal VPLS service, a management VPLS cannot be deleted until SAPs and SDPs are unbound (deleted), interfaces are shutdown, and the service is shutdown on the service level.

Use the following syntax to delete a management VPLS service.

```
config>service
    - [no] vpls service-id
    - shutdown
    - [no] sap sap-id
```

```
        - shutdown
```

5.6.4 Disabling a management VPLS

You can shut down a management VPLS without deleting the service parameters.

When a management VPLS is disabled, all associated user VPLS services are also disabled (to prevent loops). If this is not wanted, first unmanage the user VPLS service by removing them from the managed-vlan-list.

```
config>service
    vpls service-id
    shutdown
```

Example: Disabling a management VPLS

```
config>service# vpls 1
config>service>vpls# shutdown
config>service>vpls# exit
```

5.6.5 Deleting a VPLS service

A VPLS service cannot be deleted until SAPs and SDPs are unbound (deleted), interfaces are shutdown, and the service is shutdown on the service level.

Use the following syntax to delete a VPLS service.

```
config>service
    [no] vpls service-id
    shutdown
    [no] spoke-sdp sdp-id
        shutdown
    sap sap-id
    no sap sap-id
        shutdown
```

5.6.6 Disabling a VPLS service

Use the following syntax to shut down a VPLS service without deleting the service parameters.

```
config>service> vpls service-id
    [no] shutdown
```

Example: Disabling a VPLS service

```
config>service# vpls 1
config>service>vpls# shutdown
config>service>vpls# exit
```

5.6.7 Re-enabling a VPLS service

Use the following syntax to re-enable a VPLS service that was shut down.

```
config>service> vpls service-id
    [no] shutdown
```

Example: Re-enabling a VPLS service

```
config>service# vpls 1
config>service>vpls# no shutdown
config>service>vpls# exit
```

5.7 VPLS services command reference

- Command hierarchies
- Command descriptions

5.7.1 Command hierarchies

- VPLS configuration commands
- VPLS xSTP commands
- VPLS SAP DHCP snooping commands
- VPLS SAP commands
- VPLS SAP filter and QoS commands
- VPLS SAP IGMP snooping and MVR commands
- VPLS SAP meter override commands
- VPLS SAP queue override commands
- VPLS SAP xSTP commands
- VPLS SAP statistics commands
- VPLS mesh SDP commands
- VPLS spoke-SDP commands
- Show commands
- Clear commands
- Debug commands

5.7.1.1 VPLS configuration commands

```
config
    - service
```

```
        - vpls service-id [customer customer-id] [create] [vpn vpn-id] [m-vpls] [r-vpls] [svc-
sap-type {null-star | dot1q-preserve | any}] [customer-vid vlan-id] [allow-l2pt-xstp-bpdu
 enable | disable]
        - vpls service-id [customer customer-id] [create] [vpn vpn-id] [m-vpls] [customer-
vid vlan-id] [svc-sap-type {null-star | dot1q-preserve | any}] [r-vpls]
        - no vpls service-id
            - [no] allow-ip-int-bind
            - bgp
                - pw-template-binding policy-id [split-horizon-group group-name] [import-rt
 {ext-community...(up to 5 max)}]
                - no pw-template-binding policy-id
                - route-distinguisher [ip-addr:comm-val | as-number:ext-comm-val]
                - no route-distinguisher
                - route-target {ext-community | {[export ext-community] [import ext-
community]}}
                - no route-target
                - vsi-export policy-name [policy-name...(up to 5 max)]
                - no vsi-export
                - vsi-import policy-name [policy-name...(up to 5 max)]
                - no vsi-import
            - [no] bgp-ad
                - [no] shutdown
                - vpls-id vpls-id
                - vsi-id
                    - prefix low-order-vsi-id
                    - no prefix
            - description description-string
            - no description
            - [no] disable-aging
            - [no] disable-learning
            - [no] discard-unknown
            - endpoint endpoint-name [create]
            - no endpoint
                - block-on-mesh-failure
                - [no] block-on-mesh-failure
                - description description-string
                - no description
                - [no] ignore-standby-signaling
                - [no] mac-pinning
                - max-nbr-mac-addr table-size
                - no max-nbr-mac-addr
                - revert-time revert-time | infinite
                - no revert-time
                - static-mac ieee-address [create]
                - no static-mac
                - [no] suppress-standby-signaling
            - eth-cfm
                - no vpls-sap-bidir
                - vpls-sap-bidir
            - [no] fdb-table-high-wmark high-water-mark
            - [no] fdb-table-low-wmark low-water-mark
            - fdb-table-size table-size
            - no fdb-table-size [table-size]
            - local-age aging-timer
            - no local-age
            - [no] mac-move
                - move-frequency frequency
                - no move-frequency
                - retry-timeout timeout
                - no retry-timeout
                - [no] shutdown
            - [no] propagate-mac-flush
            - remote-age aging-timer
            - no remote-age
```

```
            - [no] send-flush-on-failure
            - service-mtu octets
            - no service-mtu
            - service-mtu-check octets
            - no service-mtu-check
            - no root-guard
            - [no] shutdown
            - split-horizon-group group-name [create]
                - description description-string
                - no description
```

5.7.1.2 VPLS xSTP commands

```
config
    - service
        - vpls service-id [customer customer-id] [create] [vpn vpn-id] [m-vpls] [r-vpls] [svc-
sap-type {null-star | dot1q-preserve | any}] [customer-vid vlan-id] [allow-l2pt-xstp-bpdu
 enable | disable]
        - vpls service-id [customer customer-id] [create] [vpn vpn-id] [m-vpls] [customer-
vid vlan-id] [svc-sap-type {null-star | dot1q-preserve | any}] [r-vpls]
        - no vpls service-id
            - stp
                - forward-delay forward-delay
                - no forward-delay
                - hello-time hello-time
                - no hello-time
                - hold-count  BDPU tx hold count
                - no hold-count
                - max-age max-age
                - no max-age
                - mode {rstp | comp-dot1w | dot1w | mstp | pmstp}
                - no mode
                - [no] mst-instance mst-inst-number
                    - mst-port-priority bridge-priority
                    - no mst-port-priority
                    - [no] vlan-range vlan-range
                - mst-max-hops hops-count
                - no mst-max-hops
                - mst-name region-name
                - no mst-name
                - mst-revision revision-number
                - no mst-revision
                - priority bridge-priority
                - no priority
                - [no] shutdown
```

5.7.1.3 VPLS SAP DHCP snooping commands

```
config
    - service
        - vpls service-id [customer customer-id] [create] [vpn vpn-id] [m-vpls] [r-vpls] [svc-
sap-type {null-star | dot1q-preserve | any}] [customer-vid vlan-id] [allow-l2pt-xstp-bpdu
 enable | disable]
        - vpls service-id [customer customer-id] [create] [vpn vpn-id] [m-vpls] [customer-
vid vlan-id] [svc-sap-type {null-star | dot1q-preserve | any}] [r-vpls]
        - no vpls service-id
            - sap sap-id [split-horizon-group group-name] [g8032-shg-enable] [eth-ring ring-
index]
```

```
            - no sap sap-id
                - dhcp
                    - description description-string
                    - no description
                    - [no] option
                        - action [dhcp-action]
                        - no action
                        - [no] circuit-id [ascii-tuple | vlan-ascii-tuple]
                        - [no] remote-id  [mac | string string]
                        - [no] vendor-specific-option
                            - [no] client-mac-address
                            - [no] sap-id
                            - [no] service-id
                            - string text
                            - no string
                            - [no] system-id
                    - [no] shutdown
                    - [no] snoop
```

5.7.1.4 VPLS SAP commands

```
config
    - service
        - vpls service-id [customer customer-id] [create] [vpn vpn-id] [m-vpls] [r-vpls] [svc-
sap-type {null-star | dot1q-preserve | any}] [customer-vid vlan-id] [allow-l2pt-xstp-bpdu
 enable | disable]
        - vpls service-id [customer customer-id] [create] [vpn vpn-id] [m-vpls] [customer-
vid vlan-id] [svc-sap-type {null-star | dot1q-preserve | any}] [r-vpls]
        - no vpls service-id
            - sap sap-id [split-horizon-group group-name] [create] [capture-sap] [eth-
ring ring-index] [g8032-shg-enable]
            - no sap sap-id
                - accounting-policy acct-policy-id
                - no accounting-policy
                - bpdu-translation {auto | pvst | stp}
                - no bpdu-translation
                - [no] collect-stats
                - description description-string
                - no description
                - [no] disable-aging
                - [no] disable-learning
                - [no] discard-unknown-source
                - dist-cpu-protection policy-name
                - no dist-cpu-protection
                - eth-cfm
                    - mep mep-id domain md-index association ma-index [direction {up | down}]
 primary-vlan-enable
                    - no mep mep-id domain md-index association ma-index
                        - [no] ais-enable
                            - client-meg-level [level [level...]]
                            - no client-meg-level
                            - [no] description
                            - interval
                            - no interval
                            - priority priority-value
                            - no priority
                        - [no] ccm-enable
                        - ccm-ltm-priority priority
                        - no ccm-ltm-priority
                        - description description-string
                        - no description
```

```
                        - [no] eth-test-enable
                            - test-pattern {all-zeros | all-ones} [crc-enable]
                            - no test-pattern
                        - low-priority-defect {allDef | macRemErrXcon | remErrXcon | errXcon |
 xcon | noXcon}
                        - mac-address mac-address
                        - no mac-address
                        - one-way-delay-threshold seconds
                        - [no] shutdown
                    - mip [mac mac address]
                    - mip default-mac
                    - no mip
                    - mip [mac mac address] [primary-vlan-enable vlan-id]
                    - mip default-mac [primary-vlan-enable vlan-id]
                    - no mip [primary-vlan-enable vlan-id]
                - l2pt-termination [cdp] [dtp] [pagp] [stp] [udld] [vtp]
                - no l2pt-termination
                - limit-mac-move [blockable | non-blockable]
                - no limit-mac-move
                - [no] mac-pinning
                - max-nbr-mac-addr table-size
                - no max-nbr-mac-addr
                - managed-vlan-list
                    - default-sap
                    - no default-sap
                    - no range vlan-range
                    - range vlan-range
```

5.7.1.5 VPLS SAP filter and QoS commands

```
config
    - service
        - vpls service-id [customer customer-id] [create] [vpn vpn-id] [m-vpls] [r-vpls] [svc-
sap-type {null-star | dot1q-preserve | any}] [customer-vid vlan-id] [allow-l2pt-xstp-bpdu
 enable | disable]
        - vpls service-id [customer customer-id] [create] [vpn vpn-id] [m-vpls] [customer-
vid vlan-id] [svc-sap-type {null-star | dot1q-preserve | any}] [r-vpls]
        - no vpls service-id
            - sap sap-id [split-horizon-group group-name] [g8032-shg-enable] [eth-ring ring-
index] [create]
            - no sap sap-id
                - egress
                    - agg-rate-limit [cir cir-rate] [pir pir-rate]
                    - no agg-rate-limit
                    - aggregate-meter-rate rate-in-kbps [burst burst-in-kbits] [enable-stats]
                    - no aggregate-meter-rate
                    - filter ip ip-filter-id
                    - filter ipv6 ipv6 -filter-id
                    - filter mac mac-filter-id
                    - no filter [ip ip-filter-id] [ipv6 ipv6 -filter-id] [mac mac-filter-id]
                    - qos policy-id
                    - no qos
                - ingress
                    - aggregate-meter-rate rate-in-kbps [burst burst-in-kbits]
                    - no aggregate-meter-rate
                    - filter ip ip-filter-id
                    - filter [ipv6 ipv6-filter-id]
                    - filter mac mac-filter-id
                    - no filter [ip ip-filter-id] [ ipv6 ipv6-filter-id] [mac mac-filter-id]
                    - qos policy-id [enable-table-classification]
```

```
                - no qos
```

5.7.1.6 VPLS SAP IGMP snooping and MVR commands

```
config
    - service
        - vpls service-id [customer customer-id] [create] [vpn vpn-id] [m-vpls] [r-vpls] [svc-
sap-type {null-star | dot1q-preserve | any}] [customer-vid vlan-id] [allow-l2pt-xstp-bpdu
 enable | disable]
        - vpls service-id [customer customer-id] [create] [vpn vpn-id] [m-vpls] [customer-
vid vlan-id] [svc-sap-type {null-star | dot1q-preserve | any}] [r-vpls]
        - no vpls service-id
            - igmp-snooping
                - mvr
                    - description description-string
                    - no description
                    - group-policy policy-name
                    - no group-policy
                    - no shutdown
                    - shutdown
                - query-interval interval
                - no query-interval
                - no query-src-ip
                - query-src-ip ip-address
                - no report-src-ip
                - report-src-ip ip-address
                - robust-count count
                - no robust-count
                - no shutdown
                - shutdown
            - sap sap-id [split-horizon-group group-name] [g8032-shg-enable] [eth-ring ring-
index]
            - no sap sap-id
                - igmp-snooping
                    - [no] fast-leave
                    - import policy-name
                    - no import
                    - last-member-query-interval interval
                    - no last-member-query-interval
                    - max-num-groups max-num-groups
                    - no max-num-groups
                    - max-num-sources max-num-sources
                    - no max-num-sources
                    - [no] mrouter-port
                    - mvr
                        - from-vpls service-id
                        - no from-vpls
                        - to-sap sap-id
                        - no to-sap
                    - query-interval interval
                    - no query-interval
                    - query-response-interval interval
                    - no query-response-interval
                    - robust-count count
                    - no robust-count
                    - [no] send-queries
                    - static
                        - [no] group group-address
                            - [no] source ip-address
                            - [no] starg
                    - version version
```

```
                - no version
            - mfib-table-high-wmark high-water-mark
            - no mfib-table-high-wmark
            - mfib-table-low-wmark low-water-mark
            - no mfib-table-low-wmark
            - mfib-table-size table-size
            - no mfib-table-size
```

5.7.1.7 VPLS SAP meter override commands

```
config
    - service
        - vpls service-id [customer customer-id] [create] [vpn vpn-id] [m-vpls] [r-vpls] [svc-
sap-type {null-star | dot1q-preserve | any}] [customer-vid vlan-id] [allow-l2pt-xstp-bpdu
 enable | disable]
        - vpls service-id [customer customer-id] [create] [vpn vpn-id] [m-vpls] [customer-
vid vlan-id] [svc-sap-type {null-star | dot1q-preserve | any}] [r-vpls]
        - no vpls service-id
            - sap sap-id [split-horizon-group group-name] [g8032-shg-enable] [eth-ring ring-
index]
            - no sap sap-id
                - ingress
                    - meter-override
                        - meter meter-id [create]
                        - no meter meter-id
                            - adaptation-rule  [pir adaptation-rule] [cir adaptation-rule]
                            - cbs size [kbits | bytes | kbytes]
                            - no cbs
                            - mbs size [kbits | bytes | kbytes]
                            - no mbs
                            - mode mode
                            - no mode
                            - rate cir cir-rate [pir pir-rate]
```

5.7.1.8 VPLS SAP queue override commands

```
config
    - service
        - vpls service-id [customer customer-id] [create] [vpn vpn-id] [m-vpls] [r-vpls] [svc-
sap-type {null-star | dot1q-preserve | any}] [customer-vid vlan-id] [allow-l2pt-xstp-bpdu
 enable | disable]
        - vpls service-id [customer customer-id] [create] [vpn vpn-id] [m-vpls] [customer-
vid vlan-id] [svc-sap-type {null-star | dot1q-preserve | any}] [r-vpls]
        - no vpls service-id
            - sap sap-id [split-horizon-group group-name] [g8032-shg-enable] [eth-ring ring-
index] [create]
            - no sap sap-id
                - ingress
                    - queue-override
                        - queue queue-id [create]
                            - adaptation-rule  [pir adaptation-rule] [cir adaptation-rule]
                            - no port-parent
                            - port-parent [cir-level cir-level] [pir-weight pir-weight]
                            - queue-mgmt name
                            - no queue-mgmt
                            - no rate
                            - rate [cir cir-rate] [pir pir-rate]
```

5.7.1.9 VPLS SAP xSTP commands

```
config
    - service
        - vpls service-id [customer customer-id] [create] [vpn vpn-id] [m-vpls] [r-vpls] [svc-
sap-type {null-star | dot1q-preserve | any}] [customer-vid vlan-id] [allow-l2pt-xstp-bpdu
 enable | disable]
        - vpls service-id [customer customer-id] [create] [vpn vpn-id] [m-vpls] [customer-
vid vlan-id] [svc-sap-type {null-star | dot1q-preserve | any}] [r-vpls]
        - no vpls service-id
            - sap sap-id [split-horizon-group group-name] [g8032-shg-enable] [eth-ring ring-
index]
            - no sap sap-id
                - stp
                    - [no] auto-edge
                    - [no] edge-port
                    - link-type {pt-pt | shared}
                    - no link-type [pt-pt | shared]
                    - mst-instance mst-inst-number
                        - mst-path-cost inst-path-cost
                        - no mst-path-cost
                        - mst-port-priority stp-priority
                        - no mst-port-priority
                    - path-cost sap-path-cost
                    - no path-cost
                    - [no] port-num virtual-port-number
                    - priority stp-priority
                    - no priority
                    - [no] shutdown
                - tod-suite tod-suite-name
                - no tod-suite
```

5.7.1.10 VPLS SAP statistics commands

```
config
    - service
        - vpls service-id [customer customer-id] [create] [vpn vpn-id] [m-vpls] [r-vpls] [svc-
sap-type {null-star | dot1q-preserve | any}] [customer-vid vlan-id] [allow-l2pt-xstp-bpdu
 enable | disable]
        - vpls service-id [customer customer-id] [create] [vpn vpn-id] [m-vpls] [customer-
vid vlan-id] [svc-sap-type {null-star | dot1q-preserve | any}] [r-vpls]
        - no vpls service-id
            - sap sap-id [split-horizon-group group-name] [g8032-shg-enable] [eth-ring ring-
index] [create]
            - no sap sap-id
                - statistics
                    - ingress
                        - counter-mode {in-out-profile-count | forward-drop-count}
                        - [no] drop-count-extra-vlan-tag-pkts
```

5.7.1.11 VPLS mesh SDP commands

```
config
    - service
```

```
        - vpls service-id [customer customer-id] [create] [vpn vpn-id] [m-vpls] [r-vpls] [svc-
sap-type {null-star | dot1q-preserve | any}] [customer-vid vlan-id] [allow-l2pt-xstp-bpdu
 enable | disable]
        - vpls service-id [customer customer-id] [create] [vpn vpn-id] [m-vpls] [customer-
vid vlan-id] [svc-sap-type {null-star | dot1q-preserve | any}] [r-vpls]
        - no vpls service-id
            - mesh-sdp sdp-id[:vc-id] [vc-type {ether | vlan}]
            - no mesh-sdp sdp-id[:vc-id]
                - accounting-policy acct-policy-id
                - no accounting-policys
                - [no] collect-stats
                - [no] control-word
                - description description-string
                - no description
                - egress
                    - no vc-label [egress-vc-label]
                - eth-cfm
                    - mep mep-id domain md-index association ma-index [direction {up}{down}]
                    - no mep mep-id domain md-index association ma-index
                        - [no] ais-enable
                            - client-meg-level [[level [level...]]
                            - no client-meg-level
                            - interval {1 | 60}
                            - no interval
                            - priority priority-value
                            - no priority
                        - [no] ccm-enable
                        - ccm-ltm-priority priority
                        - no ccm-ltm-priority
                        - [no] description description-string
                        - [no] eth-test-enable
                            - test-pattern {all-zeros | all-ones} [crc-enable]
                            - no test-pattern
                        - low-priority-defect {allDef | macRemErrXcon | remErrXcon | errXcon |
 xcon | noXcon}
                        - mac-address mac-address
                        - no mac-address
                        - one-way-delay-threshold seconds
                        - [no] shutdown
                - [no] force-vlan-vc-forwarding
                - hash-label
                - hash-label [signal-capability]
                - no hash-label
                - igmp-snooping
                    - import policy-name
                    - no import
                    - last-member-query-interval interval
                    - no last-member-query-interval
                    - max-num-groups max-num-groups
                    - no max-num-groups
                    - [no] mrouter-port
                    - query-interval interval
                    - no query-interval
                    - query-response-interval interval
                    - no query-response-interval
                    - robust-count count
                    - no robust-count
                    - [no] send-queries
                    - static
                        - [no] group grp-ip-address
                        - [no] starg
                    - version version
                    - no version
                - ingress
```

```
                    - vc-label egress-vc-label
                - [no] mac-pinning
                - [no] static-mac ieee-address
                - [no] shutdown vlan-vc-tag vlan-id
                - no vlan-vc-tag [vlan-id]
```

5.7.1.12 VPLS spoke-SDP commands

```
config
    - service
        - vpls service-id [customer customer-id] [create] [vpn vpn-id] [m-vpls] [r-vpls] [svc-
sap-type {null-star | dot1q-preserve | any}] [customer-vid vlan-id] [allow-l2pt-xstp-bpdu
 enable | disable]
        - vpls service-id [customer customer-id] [create] [vpn vpn-id] [m-vpls] [customer-
vid vlan-id] [svc-sap-type {null-star | dot1q-preserve | any}] [r-vpls]
        - no vpls service-id
            - spoke-sdp sdp-id[:vc-id] [vc-type {ether | vlan}] [split-horizon-group group-
name] [use-evpn-default-shg]
            - no spoke-sdp sdp-id[:vc-id]
                - accounting-policy acct-policy-id
                - no accounting-policy
                - [no] block-on-mesh-failure
                - bpdu-translation {auto | pvst | stp}
                - no bpdu-translation
                - [no] collect-stats
                - [no] control-word
                - description description-string
                - no description
                - [no] disable-aging
                - [no] disable-learning
                - [no] discard-unknown-source
                - eth-cfm
                    - mep mep-id domain md-index association ma-index [direction {up}{down}]
                        - no mep mep-id domain md-index association ma-index[no] ais-enable
                            - client-meg-level [[level [level...]]
                            - no client-meg-level
                            - interval {1 | 60}
                            - no interval
                            - priority priority-value
                            - no priority
                        - [no] ccm-enable
                        - ccm-ltm-priority priority
                        - no ccm-ltm-priority
                        - [no] description description string[
                        - no] eth-test-enable
                            - test-pattern {all-zeros | all-ones} [crc-enable]
                        - no test-patternlow-priority-defect {allDef | macRemErrXcon | remErr
Xcon | errXcon | xcon | noXcon}
                        - mac-address mac-address
                        - no mac-addressone-way-delay-threshold seconds
                        - [no] shutdown
                    - mip [mac mac address]
                    - mip default-mac
                    - no mip
                - egress
                    - vc-label egress-vc-label
                    - no vc-label [egress-vc-label]
                - [no] force-vlan-vc-forwarding
                - hash-label [signal-capability]
                - no hash-label
                - igmp-snooping
```

```
                    - import policy-name
                    - no import
                    - last-member-query-interval interval
                    - no last-member-query-interval
                    - max-num-groups max-num-groups
                    - no max-num-groups
                    - [no] mrouter-port
                    - query-interval interval
                    - no query-interval
                    - query-response-interval interval
                    - no query-response-interval
                    - robust-count count
                    - no robust-count
                    - [no] send-queries
                    - static
                        - [no] group group-address
                            - [no] starg
                    - version version
                    - no version
                - [no] ignore-standby-signaling
                - ingress
                    - vc-label egress-vc-label
                    - no vc-label [egress-vc-label]
                - [no] l2pt-termination [cdp] [dtp] [pagp] [stp] [udld] [vtp]
                - limit-mac-move [blockable | non-blockable]
                - no limit-mac-move
                - [no] mac-pinning
                - max-nbr-mac-addr table-size
                - no max-nbr-mac-addr
                - precedence precedence-value | primary
                - no precedence
                - [no] pw-path-id
                    - agi agi
                    - no agi
                    - saii-type2 global-id:node-id:ac-id
                    - no saii-type2
                    - taii-type2 global-id:node-id:ac-id
                    - no taii-type2
                - [no] pw-status-signaling
                - [no] shutdown
                - [no] static-mac ieee-address
                - stp
                    - [no] auto-edge
                    - [no] edge-port
                    - link-type {pt-pt | shared}
                    - no link-type [pt-pt | shared]
                    - path-cost sap-path-cost
                    - no path-cost
                    - [no] port-num virtual-port-number
                    - priority stp-priority
                    - no priority
                    - no root-guard
                    - root-guard
                    - [no] shutdown
                - vlan-vc-tag vlan-id
                - no vlan-vc-tag [vlan-id]
```

5.7.1.13 Routed VPLS commands

```
config
    - service
```

```
        - vpls service-id [customer customer-id] [create] [vpn vpn-id] [m-vpls] [r-vpls] [svc-
sap-type {null-star | dot1q-preserve | any}] [customer-vid vlan-id] [allow-l2pt-xstp-bpdu
 enable | disable]
        - vpls service-id [customer customer-id] [create] [vpn vpn-id] [m-vpls] [customer-
vid vlan-id] [svc-sap-type {null-star | dot1q-preserve | any}] [r-vpls]
        - no vpls service-id
            - [no] allow-ip-int-bind
```

5.7.1.14 Show commands

```
show
    - service
        - egress-label egress-label1 [egress-label2]
        - fdb-info
        - fdb-mac ieee-address [expiry]
        - id service-id
            - all
            - base [msap] [bfd]
            - dhcp
                - statistics [sap sap-id] [interface interface-name]
                - summary [interface interface-name | saps]
            - endpoint [endpoint-name]
            - fdb [sap sap-id] [expiry]] | [mac ieee-address [expiry]] | [detail] [expiry]
            - igmp-snooping
                - all
                - base
                - mvrmrouters [detail]
                - port-db sap sap-id [detail]
                - port-db sap sap-id group grp-address
                - port-db sdp sdp-id:vc-id [detail]
                - port-db sdp sdp-id:vc-id group grp-address
                - proxy-db [detail]
                - proxy-db [group grp-ip-address]
                - querier
                - static [sap sap-id]
                - statistics[sap sap-id | sdp sdp-ic:vc-id]
            - labels
            - l2pt disabled
            - l2pt [detail]
            - mac-move
            - mfib [brief]
            - mfib [group grp-address | mstp-configuration]
            - sap [sap-id [detail]]
            - sdp [sdp-id | far-end ip-addr] [detail]
            - split-horizon-group [group-name]
            - stp
        - ingress-label start-label [end-label]
        - sap-using [sap sap-id]
        - sap-using [ingress | egress] filter filter-id
        - sap-using [ingress | egress] qos-policy qos-policy-id
        - sap-using [ingress | egress]
        - sdp [sdp-id | far-end ip-address] [detail | keep-alive-history]
        - sdp-using [sdp-id[:vc-id] | far-end ip-address]
        - service-using [vpls]
```

5.7.1.15 Clear commands

```
clear
```

```
    - service
        - id service-id
            - fdb {all | mac ieee-address | sap sap-id | mesh-sdp sdp-id[:vc-id] | spoke-
sdp sdp-id:vc-id}
            - igmp-snooping
                - port-db sap sap-id [group grp-address]
                - port-db sdp sdp-id:vc-id [group grp-ip-address]
                - querier
            - mesh-sdp sdp-id[:vc-id] ingress-vc-label
                - spoke-sdp sdp-id:vc-id ingress-vc-label
            - spoke-sdp sdp-id[:vc-id]
            - stp
                - detected-protocols [all | sap sap-id]
        - statistics
            - id service-id
                - counters
                - mesh-sdp sdp-id[:vc-id] {all | counters | stp}
                - spoke-sdp sdp-id[:vc-id] {all | counters | stp | l2pt}
                - stp
            - sap sap-id {all | counters | stp}
```

5.7.1.16 Debug commands

```
debug
    - service
        - id service-id
            - [no] event-type {config-change | svc-oper-status-change | sap-oper-status-change
 | sdpbind-oper-status-change}
            - [no] sap sap-id
```

5.7.2 Command descriptions

5.7.2.1 VPLS configuration commands

5.7.2.1.1 Generic commands

shutdown

Syntax

[**no**] **shutdown**

Context

config>service>vpls

config>service>vpls>snooping

config>service>vpls>igmp-snooping

config>service>vpls>sap

config>service>vpls>sap>dhcp

config>service>vpls>sap>stp

config>service>vpls>stp

config>service>vpls>spoke-sdp>stp

config>service>vpls>bgp-ad

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

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

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

Services are created in the administratively down (**shutdown**) state. When a **no shutdown** command is entered, the service becomes administratively up and then tries to enter the operationally up state.

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

description

Syntax

description *description-string*

no description

Context

config>service>vpls

config>service>vpls>split-horizon-group

config>service>vpls>igmp-snooping>mvr

config>service>vpls>sap

config>service>vpls>sap>dhcp

config>service>vpls>spoke-sdp config>service>pw-template>split-horizon-group

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

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

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

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

Parameters

description-string

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

dhcp

Syntax

dhcp

Context

config>service>vpls>sap

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

Commands in this context configure DHCP parameters.

action

Syntax

action {**replace** | **drop** | **keep**}

no action

Context

config>service>vpls>sap>dhcp>option

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the Relay Agent Information Option (Option 82) processing.

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

Default

no action

Parameters

replace

Keyword to specify that, in the upstream direction (from the user), the Option 82 field from the router is inserted in the packet (overwriting any existing Option 82 field). In the downstream direction (toward the user) the Option 82 field is stripped (in accordance with RFC 3046).

drop

Keyword to specify that the DHCP packet is dropped if an Option 82 field is present, and a counter is incremented.

keep

Keyword to specify that the existing information is kept in the packet and the router does not add any more information. In the downstream direction, the Option 82 field is not stripped and is forwarded toward the client.

The behavior is slightly different in the case of Vendor Specific Options (VSOs). When the **keep** parameter is specified, the router inserts its own VSO into the Option 82 field. This is done only when the incoming message already has an Option 82 field.

If no Option 82 field is present, the router does not create the Option 82 field. In this case, no VSO is added to the message.

circuit-id

Syntax

circuit-id [**ascii-tuple** | **vlan-ascii-tuple**]

no circuit-id

Context

config>service>vpls>sap>dhcp>option

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

When enabled, the router sends an ASCII-encoded tuple in the **circuit-id** sub-option of the DHCP packet. This ASCII-tuple consists of the access-node-identifier, service-id, and SAPID, separated by "|". If no keyword is configured, the **circuit-id** sub-option is not part of the information option (Option 82).

When this command is configured without parameters, it is the equivalent of **circuit-id** ascii-tuple.

If disabled, the **circuit-id** sub-option of the DHCP packet is left empty.

By default, if any of the other options are configured (for example, remote-id or vso),**circuit-id** is enabled.

Default

no circuit-id

Parameters

ascii-tuple

Specifies that the ASCII-encoded concatenated tuple is used, which consists of the access-node-identifier, service-id, and interface-name.

hex

Specifies the circuit-id hex string.

vlan-ascii-tuple

Specifies that the format includes VLAN ID and dot1p bits, in addition to what is already included in the ascii-tuple. The format is supported on dot1q and qinq encapsulated ports only. Therefore, when the Option 82 bits are stripped, dot1p bits are copied to the Ethernet header of an outgoing packet.

option

Syntax

[**no**] **option**

Context

config>service>vpls>sap>dhcp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables DHCP Option 82 (Relay Agent Information Option) parameters processing and enables the context for configuring Option 82 sub-options.

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

Default

no option

remote-id

Syntax

remote-id [**mac** | **string** *string*]

no remote-id

Context

config>service>vpls>sap>dhcp>option

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

When enabled, the router sends the MAC address of the remote end (typically the DHCP client) in the **remote-id** sub-option of the DHCP packet. This command identifies the host at the other end of the circuit.

If disabled, the **remote-id** sub-option of the DHCP packet is left empty.

The **no** form of this command reverts the system to the default.

Default

remote-id

Parameters

mac

Keyword to specify that the MAC address of the remote end is encoded in the sub-option.

string *string*

Specifies the remote-id.

vendor-specific-option

Syntax

[**no**] **vendor-specific-option**

Context

config>service>vpls>sap>dhcp>option

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the vendor specific sub-option of the DHCP relay packet.

client-mac-address

Syntax

[**no**] **client-mac-address**

Context

config>service>vpls>sap>dhcp>option>vendor

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables the sending of the MAC address in the vendor-specific suboption of the DHCP relay packet.

The **no** form of this command disables the sending of the MAC address in the vendor-specific suboption of the DHCP relay packet.

sap-id

Syntax

[**no**] **sap-id**

Context

config>service>vpls>sap>dhcp>option>vendor config>service>ies>sap>dhcp>option>vendor config>service>vprn>sap>dhcp>option>vendor

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables the sending of the SAP ID in the vendor-specific suboption of the DHCP relay packet.

The **no** form of this command disables the sending of the SAP ID in the vendor-specific suboption of the DHCP relay packet.

service-id

Syntax

[**no**] **service-id**

Context

config>service>vpls>sap>dhcp>option>vendor config>service>ies>sap>dhcp>option>vendor config>service>vprn>sap>dhcp>option>vendor

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables the sending of the service ID in the vendor-specific suboption of the DHCP relay packet.

The **no** form of this command disables the sending of the service ID in the vendor-specific suboption of the DHCP relay packet.

string

Syntax

[**no**] **string** *text*

Context

config>service>vpls>sap>dhcp>option>vendor config>service>ies>sap>dhcp>option>vendor config>service>vprn>sap>dhcp>option>vendor

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command specifies the string in the vendor-specific suboption of the DHCP relay packet.

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

Parameters

text

Specifies a string that can be any combination of ASCII characters up to 32 characters. If spaces are used in the string, enclose the entire string in quotation marks (" ").

system-id

Syntax

[**no**] **system-id**

Context

config>service>vpls>sap>dhcp>option>vendor config>service>ies>sap>dhcp>option>vendor config>service>vprn>sap>dhcp>option>vendor

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command specifies whether the system-id is encoded in the vendor-specific suboption of Option 82.

relay-plain-bootp

Syntax

relay-plain-bootp

no relay-plain-bootp

Context

config>service>ies>if>dhcp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables the relaying of plain BOOTP packets.

The **no** form of this command disables the relaying of plain BOOTP packets.

server

Syntax

server *server1* [*server2*...(**up to 8 max**)]

Context

config>service>ies>if>dhcp

config>service>vprn>if>dhcp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command specifies a list of servers to which requests are forwarded. The list of servers can be entered as either IP addresses or fully qualified domain names. There must be at least one server specified for DHCP relay to work. If there are multiple servers, the request is forwarded to all the servers in the list.

A maximum of 8 DHCP servers can be configured.

Default

no server

Parameters

server

Specifies the DHCP server IP address.

trusted

Syntax

[**no**] **trusted**

Context

config>service>ies>if>dhcp

config>service>vprn>if>dhcp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables relaying of untrusted packets.

The **no** form of this command disables the relay.

Default

not enabled

snoop

Syntax

[**no**] **snoop**

Context

config>service>vpls>sap>dhcp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures DHCP snooping of DHCP messages on the SAP. Enabling DHCP snooping on VPLS interfaces (SAPs) is required where vendor-specific information (as per RFC 4243) is to be inserted into the Option 82 field of the DHCP messages. This includes interfaces that are in the path to receive messages from either DHCP servers or from subscribers.

The **no** form of this command disables DHCP snooping on the specified VPLS SAP.

Note: DHCP snooping for SDP is not supported on the platforms as described in this document.

Default

no snoop

5.7.2.1.2 VPLS commands

vpls

Syntax

vpls *service-id* [**customer** *customer-id*] [**create**] [**vpn** *vpn-id*] [**m-vpls**] [**r-vpls**] [**svc-sap-type** {**null-star** | **dot1q-preserve** | **any**}] [**customer-vid** *vlan-id*] [**allow-l2pt-xstp-bpdu enable** | **disable**]

vpls *service-id* [**customer** *customer-id*] [**create**] [**vpn** *vpn-id*] [**m-vpls**] [**customer-vid** *vlan-id*] [**svc-sap-type** {**null-star** | **dot1q-preserve** | **any**}] [**r-vpls**]

no vpls *service-id*

Context

config>service

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command creates or edits a VPLS 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.

A VPLS service connects multiple customer sites, acting as a zero-hop, Layer 2 switched domain. A VPLS is always a logical full mesh.

When a service is created, the **create** keyword must be specified, if the **create** command is enabled in the **environment** context. When a service is created, the **customer** keyword and *customer-id* parameter must be specified to associate 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 has been created with a customer association, it is not possible to edit the customer association. The service must be deleted and recreated with a new customer association.

When a service is created, the use of the **customer** *customer-id* command is optional for navigating into the service configuration context. Editing a service with the incorrect *customer-id* value specified results in an error.

More than one VPLS service may be created for a single customer ID.

By default, no VPLS instances exist until they are explicitly created.

The **no** form of this command deletes the VPLS service instance with the specified *service-id*. The service cannot be deleted until all SAPs and SDPs defined within the service ID have been shut down and deleted, and the service has been shut down.

Parameters

service-id

Specifies 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 another service of

any type. The *service-id*must be the same number used for every 7210 SAS on which this service is defined.

Values 1 to 2147483647

customer *customer-id*

Specifies the customer ID number to be associated with the service. This parameter is required on service creation and is optional for service editing or deleting.

Values 1 to 2147483647

m-vpls

Specifies a management VPLS.

r-vpls

Specifies to associate this VPLS instance with an IP interface to provide RVPLS functionality.

allow-l2pt-xstp-bpdu enable | disable

Specifies to allow the users to reserve resources for xSTP, L2PT, and BPDU services. Only if the service is created with this parameter, can the user later turn on the xSTP, L2PT, and BPDU features in the service. If not, all attempts to use these features fails.

create

Mandatory keyword while creating a VPLS service. The **create** keyword requirement can be enabled or disabled using the **environment>create** context.

vpn vpn-id

Specifies the VPN ID number, which allows you to identify virtual private networks (VPNs).

Values 1 to 2147483647

Default null (0)

customer-vid vlan-id

Defines the dot1q VLAN ID to be specified while creating the local dot1q SAP for the **svc-sap-type dot1q-preserve** command.

Values 1 to 4094

svc-sap-type

Specifies the type of service and allowed SAPs in the service.

Values **dot1q-preserve —** Keyword to specify that the allowed SAP in the service are dot1q. The dot1q ID is not stripped after packets matches the SAP. This option is supported only when the **r-vpls** keyword is specified.

null-star — Keyword to specify that the allowed SAP in the service, which can be null SAPs, dot1q default, Q.* SAP,0.* SAP or Default QinQ SAP. This option is supported only when the **r-vpls** keyword is specified.

any — Keyword to specify that, for network mode, all supported SAPs are allowed in the service. See section QinQ SAP configuration

restrictions for 7210 SAS in network mode only for information about restrictions related to QinQ SAPs.

Default any

bgp

Syntax

bgp

Context

config>service>vpls

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

Commands in this context configure the BGP-related parameters to BGP AD.

block-on-mesh-failure

Syntax

[**no**] **block-on-mesh-failure**

Context

config>service>vpls>spoke-sdp

config>service>vpls>endpoint

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables blocking (brings the entity to an operationally down state) after all configured mesh-SDPs are in operationally down state. This event is signaled to corresponding T-LDP peers by withdrawing the service label (status-bit-signaling non-capable peer) or by setting the "PW not forwarding" status bit in the T-LDP message (status-bit-signaling capable peer).

Default

disabled

bpdu-translation

Syntax

bpdu-translation {**auto** | **pvst** | **stp**}

no bpdu-translation

Context

config>service>vpls>spoke-sdp

config>service>vpls>sap

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables the translation of BPDUs to a specific format, meaning that all BPDUs transmitted on a specific SAP or spoke-SDP have a specified format.

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

Default

no bpdu-translation

Parameters

auto

Keyword to specify the format is detected automatically, based on the type of BPDUs received on the port.

pvst

Keyword to specify the BPDU format as PVST. The correct VLAN tag is included in the payload, depending on the encapsulation value of the outgoing SAP.

stp

Keyword to specify the BPDU format as STP.

l2pt-termination

Syntax

l2pt-termination [**cdp**] [**dtp**] [**pagp**] [**stp**] [**udld**] [**vtp**]

no l2pt-termination

Context

config>service>vpls>sap config>service>vpls>spoke-sdp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables Layer 2 Protocol Tunneling (L2PT) termination on a specific SAP. L2PT termination is supported for CDP, DTP, PAGP, STP, UDLD and VTP PDUs.

This feature can be enabled only if STP is disabled in the context of the specific VPLS service.

Default

no l2pt-termination

Parameters

cdp

Keyword to specify the Cisco discovery protocol.

dtp

Keyword to specify the dynamic trunking protocol.

pagp

Keyword to specify the port aggregation protocol.

stp

Keyword to specify all spanning tree protocols: stp, rstp, mstp, pvst (default).

udld

Keyword to specify unidirectional link detection.

vtp

Keyword to specify the VLAN trunking protocol.

disable-aging

Syntax

[**no**] **disable-aging**

Context

config>service>vpls

config>service>vpls>sap

config>template>vpls-template config>service>pw-template

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command disables MAC address aging across a VPLS service or on a VPLS service SAP.

Like in a Layer 2 switch, learned MACs can be aged out if no packets are sourced from the MAC address for a period of time (the aging time). In each VPLS service instance, there are independent aging timers for local learned MAC and remote learned MAC entries in the VPLS Forwarding Database (FDB). The **disable-aging** command turns off aging for local and remote learned MAC addresses.

When **no disable-aging** is specified for a VPLS, it is possible to disable aging for specific SAPs by entering the **disable-aging** command at the appropriate level.

When the **disable-aging** command is entered at the VPLS level, the **disable-aging** state of individual SAPs is ignored.

The **no** form of this command enables aging on the VPLS service.

Default

no disable-aging

disable-learning

Syntax

[**no**] **disable-learning**

Context

config>service>vpls config>service>pw-template

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command disables learning of new MAC addresses in the VPLS FDB for the service instance.

When **disable-learning** is enabled, new source MAC addresses are not entered in the VPLS service forwarding database.

When **disable-learning** is disabled, new source MAC addresses are learned or entered into the VPLS forwarding database.

This command is mainly used in conjunction with the **disable-learning** command.

The **no** form of this command enables learning of MAC addresses.

Default

no disable-learning

discard-unknown

Syntax

[**no**] **discard-unknown**

Context

config>service>vpls

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

By default, packets with unknown destination MAC addresses are flooded. If this command is enabled at the VPLS level, packets with unknown destination MAC address are dropped instead (even when the configured FIB size limits for VPLS or SAP are not yet reached).

The **no** form of this command allows flooding of packets with unknown destination MAC addresses in the VPLS.

Default

no discard-unknown

vpls-sap-bidir

Syntax

no vpls-sap-bidir

vpls-sap-bidir

Context

config>service>vpls>eth-cfm

Platforms

7210 SAS-R6 and 7210 SAS-R12 IMMv2

Description

This command links the MEP with the primary VLAN configured under the bridge-identifier for the MA. MEPs cannot be changed from or to primary VLAN functions. This must be configured as part of the creation step and can be changed only by deleting the MEP and recreating it.

This command is used to enable both the ingress and egress MIP functionality for a VPLS SAP.

Before enabling both Ingress and egress MIP functionality, the user must allocate sufficient resources in the egress-internal-tcam resource pool using the **configure system resource-profile egress-internal-tcam eth-cfm bidir-mip-egress** command. See the *7210 SAS-Mxp, R6, R12, S, Sx, T Basic System Configuration Guide* for more information.

The following describes the behavior for this command:

- MIP creation (without PVLAN enabled) is enabled under SAP with **vpls-sap-bidir** enabled and with either default or explicit mode configured for mhf-creation

  In this case, both ingress MIP and egress MIP are created; a MIP (ingress and egress) is created at the level greater than the highest level MEP configured for the VPLS SAP.

- MIP creation (without PVLAN enabled) is enabled under SAP with **vpls-sap-bidir** disabled and with either default or explicit mode configured for mhf-creation

  In this case, only an ingress MIP is created; a MIP (ingress only) is created at the level greater than the highest level MEP configured for the VPLS SAP.
- MIP creation (without PVLAN enabled) is enabled under SDP-Binding (that is, spoke-SDP/mesh-SDP) with **vpls-sap-bidir** enabled or disabled and with either default or explicit mode configured for mhf-creation

  In this case, only ingress MIP is created; a MIP (ingress only) is created at the level greater than the highest level MEP configured for the VPLS SDB binding.
- MIP creation (with PVLAN enabled) is enabled under SAP with **vpls-sap-bidir** enabled or disabled and with either default or explicit mode configured for mhf-creation

  In this case, both ingress MIP and egress MIP are created; a MIP (ingress and egress) is created at the level greater than the highest level MEP configured for the VPLS SAP.
- **vpls-sap-bidir** is enabled in a service and there are previously created and configured ingress MIPs (without PVLAN enabled) for any SAPs configured in the service

  In this case, those MIPS are automatically converted to ingress and egress MIPs, assuming sufficient resources are allocated in the egress-internal-tcam resource pool for this feature. If sufficient resources are not available, attempting to enable the **vpls-sap-bidir** command fails.
- **vpls-sap-bidir** is enabled in a service and there are previously created and configured ingress MIPs (without PVLAN enabled) for any SDP bindings configured in the service

  In this case, those MIPS continue to function as ingress MIPs. That is, the **vpls-sap-bidir** has no effect on MIPs configured on SDP bindings.
- **vpls-sap-bidir** is enabled in a service and there are previously created and configured ingress MIPs with PVLAN enabled for any SAP configured in the service

  In this case, those MIPS continue to function as both ingress MIP and egress MIP. That is, the **vpls-sap-bidir** setting has no effect on MIPs with primary VLAN enabled and configured on SAPs.

Default

no vpls-sap-bidir

endpoint

Syntax

endpoint *endpoint-name* [**create**]

no endpoint

Context

config>service>vpls

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures a service endpoint.

Parameters

endpoint-name

Specifies an endpoint name up to 32 characters.

create

Mandatory keyword for creating a service endpoint.

description

Syntax

description *description-string*

no description

Context

config>service>vpls>endpoint

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

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

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

Parameters

description-string

Specifies the description character string. Allowed values are any string up to 80 characters composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

ignore-standby-signaling

Syntax

[**no**] **ignore-standby-signaling**

Context

config>service>vpls>endpoint

config>service>vpls>spoke-sdp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

When this command is enabled, the node ignores the standby-bit received from TLDP peers for the specific spoke-SDP and performs internal tasks without taking it into account.

This command is present at the endpoint level and at the spoke-SDP level. If the spoke-SDP is part of the explicit-endpoint, it is not possible to change this setting at the spoke-SDP level. The existing spoke-SDP becomes part of the explicit-endpoint only if the setting is not conflicting. The newly created spoke-SDP, which is part of the specific explicit-endpoint, inherits this setting from the endpoint configuration.

Default

disabled

revert-time

Syntax

revert-time *revert-time* | **infinite**

no revert-time

Context

config>service>vpls>endpoint

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the time to wait before reverting to primary spoke-SDP.

In a regular endpoint, the revert-time setting affects only the pseudowire defined as primary (precedence 0). For a failure of the primary pseudowire followed by restoration, the revert-timer is started. After it expires, the primary pseudowire takes the active role in the endpoint. This behavior does not apply for case where both pseudowires are defined as secondary; for example, if the active secondary pseudowire fails and is restored, it stays in standby until a configuration change or a force command occurs.

Parameters

revert-time

Specifies the time to wait, in seconds, before reverting back to the primary spoke-SDP defined on this service endpoint, after having failed over to a backup spoke-SDP.

Values 0 to 600

infinite

Keyword that makes the endpoint non-revertive.

split-horizon-group

Syntax

split-horizon-group *group-name* [**create**]

Context

config>service>vpls config>service>pw-template

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command creates a new split horizon group (SHG) for the VPLS instance. Traffic arriving on a SAP or spoke-SDP within this SHG are not copied to other SAPs or spoke SDPs in the same SHG.

An SHG must be created before SAPs and spoke SDPs can be assigned to the group.

The SHG is defined within the context of a single VPLS instance. The same group name can be reused in different VPLS instances.

Note:

- On the 7210 SAS-R6 with IMM (v1 cards) and IMM-c cards, service-based SHGs and mesh-SDPs are mutually exclusive in a VPLS service.
- On the 7210 SAS-R6 and 7210 SAS-R12 with IMM-b cards, an SHG can be used with spoke-SDPs or mesh-SDPs configured in the service.
- Service-based SHGs are not supported in an R-VPLS service.

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

Parameters

group-name

Specifies the name of the split horizon group to which the SAP or spoke-SDP belongs.

create

Mandatory keyword to create a split-horizon group.

static-mac

Syntax

static-mac ieee-address [**create**]

no static-mac

Context

config>service>vpls>endpoint

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command assigns a static MAC address to the endpoint. In the FDB, the static MAC is then associated with the active spoke-SDP.

Parameters

ieee-address

Specifies the static MAC address to the endpoint. This value cannot be all zeros.

Values 6-byte mac-address (xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx)

create

Mandatory keyword for creating a static MAC.

suppress-standby-signaling

Syntax

[**no**] **suppress-standby-signaling**

Context

config>service>vpls>endpoint

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

When this command is enabled, the pseudowire standby bit (with value 0x00000020) is not sent to T-LDP peer when the specific spoke is selected as a standby. This allows faster switchover as the traffic is sent over this SDP and discarded at the blocking side of the connection. This is particularly applicable to multicast traffic.

Default

enabled

fdb-table-high-wmark

Syntax

[**no**] **fdb-table-high-wmark** *high-water-mark*

Context

config>service>vpls

config>template>vpls-template

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command specifies the upper threshold value for FDB entries. The high-water-mark is configured as a percentage of the FDB. When the number of FDB entries exceeds the high-water-mark, the system raises a log event.

Parameters

high-water-mark

Specifies the upper threshold for FDB entries, which when exceeded, causes the system to raise a log event.

Values 0 to 100

Default 95%

fdb-table-low-wmark

Syntax

[**no**] **fdb-table-low-wmark** *low-water-mark*

Context

config>service>vpls

config>template>vpls-template

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command specifies the lower threshold value for FDB entries. The low-water-mark is configured as a percentage of the FDB. When the number of FDB entries drops below the low-water-mark, the system raises a log event.

Parameters

low-water-mark

Specifies the lower threshold for FDB entries, which when dropped below, causes the system to raise a log event.

Values 0 to 100

Default 90%

fdb-table-size

Syntax

fdb-table-size *table-size*

no fdb-table-size [*table-size*]

Context

config>service>vpls

config>template>vpls-template

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command specifies the maximum number of MAC entries in the FDB for the VPLS instance on this node.

The **fdb-table-size** specifies the maximum number of FDB entries for both learned and static MAC addresses for the VPLS instance.

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

Default

fdb-table-size 250

Parameters

table-size

Specifies the maximum number of MAC entries in the FDB.

vsi-export

Syntax

vsi-export policy-name [*policy-name*...(up to 5 max)]

no vsi-export

Context

config>service>vpls>bgp-ad config>service>vpls>bgp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command specifies the name of the VSI export policies to be used for BGP auto-discovery, if this feature is configured in the VPLS service. If multiple policy names are configured, the policies are evaluated in the order they are specified. The first policy that matches is applied.

The policy name list is handled by the SNMP agent as a single entity.

vsi-import

Syntax

vsi-import policy-name [*policy-name*...(up to 5 max)]

no vsi-import

Context

config>service>vpls>bgp-ad>vsi-id config>service>vpls>bgp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command specifies the name of the VSI import policies to be used for BGP auto-discovery, if this feature is configured in the VPLS service. If multiple policy names are configured, the policies are evaluated in the order they are specified. The first policy that matches is applied. The policy name list is handled by the SNMP agent as a single entity.

route-target

Syntax

route-target {**ext-community** | {[**export** *ext-community*][**import** *ext-community*]}}

no route-target

Context

config>service>vpls>bgp-ad config>service>vpls>bgp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the route target (RT) component that is signaled in the related MPBGP attribute to be used for BGP auto-discovery, if this feature is configured in the VPLS service.

If this command is not used, the RT is built automatically using the VPLS ID. The extended community can have the same formats as the VPLS ID: a two-octet AS-specific extended community, or an IPv4-specific extended community.

The following rules apply.

- If BGP AD VPLS-id is configured and no RT is configured under the BGP node: RT = VPLS-ID.
- If BGP AD VPLS-id is not configured, an RT value must be configured under the BGP node. (This is the case when only BGP VPLS is configured.)
- If BGP AD VPLS-id is configured and an RT value is also configured under the BGP node, the configured RT value prevails.

Parameters

export ext-community

Specifies communities allowed to be sent to remote PE neighbors.

import ext-community

Specifies communities allowed to be accepted from remote PE neighbors.

pw-template-binding

Syntax

pw-template-binding *policy-id* [**split-horizon-group** *group-name*] [**import-rt** {*ext-community*,**...**(up to 5 max)}]

no pw-template-bind *policy-id*

Context

config>service>vpls>bgp-ad

config>service>vpls>bgp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command binds the advertisements received with the RT that match the configured list (either the generic or the specified import) to a specific pw-template. If the RT list is not present, the pw-template is used for all of them.

The pw-template-binding applies to BGP-AD, if this feature is configured in the VPLS service.

The tools perform commands can be used to control the application of changes in pw-template for BGP-AD.

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

Parameters

policy-id

Specifies an existing policy ID.

Values 1 to 2147483647

split-horizon-group ***group-name***

Specifies the group name that overrides the split horizon group template settings.

import-rt ***ext-comm***

Specifies communities allowed to be accepted from remote PE neighbors. An extended BGP community in the type:x:y format. The value x can be an integer or IP address.

The type can be the target or origin; x and y are 16-bit integers.

Values *ip-addr:comm-val* | *2byte-asnumber:ext-comm-val* | *4byte-asnumber:comm-val*

where:

ip-addr — IP address in the form a.b.c.d.

comm-val — 0 to 65535

2byte-asnumber — 0 to 65535

ext-comm-val — 0 to 4294967295

4byte-asnumber — 0 to 4294967295

target:{ip-addr:comm-val| 2byte-asnumber:ext-comm-val|4byte-asnumber:comm-val} ip-addr a.b.c.d

route-distinguisher

Syntax

route-distinguisher [*rd*]

no route-distinguisher

Context

config>service>vpls>bgp-ad>vsi-id

config>service>vpls>bgp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the Route Distinguisher (RD) component that is signaled in the MPBGP NLRI for L2VPN AFI. This value is used for BGP-AD, if this feature is configured in the VPLS service.

If this command is not configured, the RD is automatically built using the BGP-AD VPLS ID. The following rules apply:

- If BGP AD VPLS-id is configured and no RD is configured under BGP node: RD = VPLS-ID.
- If BGP AD VPLS-id is not configured, an RD value must be configured under BGP node. (This is the case when only BGP VPLS is configured.)
- If BGP AD VPLS-id is configured and an RD value is also configured under BGP node, the configured RD value prevails

The values and format consist of 6 bytes, where the other 2 bytes of type is automatically generated.

Parameters

rd

Specifies the RD component in one of the following forms:

- *ip-addr:comm-val*
- *2byte-asnumber:ext-comm-val*
- *4byte-asnumber:comm-val*

Values *ip-addr* — IP address in the form a.b.c.d.
comm-val — 0 to 65535
2byte-asnumber — 1 to 65535
ext-comm-val — 0 to 4294967295
4byte-asnumber — 0 to 4294967295

local-age

Syntax

local-age *aging-timer*

no local-age

Context

config>service>vpls

config>template>vpls-template

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command specifies the aging time for locally learned MAC addresses in the FDB for the VPLS instance. In a VPLS service, MAC addresses are associated with a Service Access Point (SAP). MACs associated with a SAP are classified as local MACs, and MACs associated with are remote MACs.

Like in a Layer 2 switch, learned MACs can be aged out if no packets are sourced from the MAC address for a period of time (the aging time). The **local-age** timer specifies the aging time for local learned MAC addresses.

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

Default

local-age 300

Parameters

aging-timer

Specifies the aging time for local MACs, in seconds.

Values 60 to 86400

mac-move

Syntax

[**no**] **mac-move**

Context

config>service>vpls

config>template>vpls-template

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures MAC move attributes. A sustained high relearn rate can be a sign of a loop somewhere in the VPLS topology. Typically, STP detects loops in the topology, but for those networks that do not run STP, the **mac-move** command is an alternative way to protect your network against loops.

When enabled in a VPLS, the **mac-move** command monitors the relearn rate of each MAC. If the rate exceeds the configured maximum allowed limit, it disables the SAP where the source MAC was last seen. The SAP can be disabled permanently (until a **shutdown**/**no shutdown** command is executed) or for a length of time that grows linearly with the number of times the specific SAP was disabled. A SAP can be marked as non-blockable using the **config>service>vpls>sap>limit-mac-move** context. This means that when the relearn rate has exceeded the limit, another (blockable) SAP is disabled instead.

The **mac-move** command enables the feature at the service level for SAPs; only those objects can be blocked by this feature.

The operation of this feature is the same on the SAP; for example, if a MAC address moves from SAP to SAP, one is blocked to prevent thrashing.

The **mac-move** command disables a VPLS port when the number of relearns detected has reached the number of relearns needed to reach the move-frequency in the 5-second interval. For example, when the move-frequency is configured to 1 (relearn per second) the **mac-move** command disables one of the VPLS ports when 5 relearns were detected during the 5-second interval, because the average move-frequency of 1 relearn per second has been reached. This can occur in the first second if the real relearn rate is 5 relearns per second or higher.

The **no** form of this command disables the **mac-move** command.

move-frequency

Syntax

move-frequency *frequency*

no move-frequency

Context

config>service>vpls>mac-move

config>template>vpls-template>mac-move

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command indicates the maximum rate at which MACs can be relearned in the VPLS service, before the SAP where the moving MAC was last seen is automatically disabled to protect the system against undetected loops or duplicate MACs.

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

Default

move-frequency 2

Parameters

frequency

Specifies the rate, in 5-second intervals, for the maximum number of relearns.

Values 1 to 100

retry-timeout

Syntax

retry-timeout *timeout*

no retry-timeout

Context

config>service>vpls>mac-move

config>template>vpls-template>mac-move

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the time in seconds to wait before a SAP that has been disabled after exceeding the maximum relearn rate is re-enabled.

Nokia recommends that the retry-timeout value be larger or equal to 5s * cumulative factor of the highest priority port, so that the sequential order of port blocking is not disturbed by reinitializing lower priority ports.

A zero value indicates that the SAP is not automatically re-enabled after being disabled. If, after the SAP is re-enabled it is disabled again, the effective retry timeout is doubled to avoid thrashing.

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

Default

retry-timeout 10

Parameters

timeout

Specifies the time, in seconds, to wait before a SAP that has been disabled after exceeding the maximum relearn rate is re-enabled.

Values 0 to 120

mfib-table-high-wmark

Syntax

[**no**] **mfib-table-high-wmark** *high-water-mark*

Context

config>service>vpls

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command specifies the multicast FIB (MFIB) high watermark. When the percentage filling level of the MFIB exceeds the configured value, a trap is generated and a log entry is added.

Parameters

high-water-mark

Specifies the MFIB high watermark as a percentage.

Values 1 to 100

Default 95%

mfib-table-low-wmark

Syntax

[**no**] **mfib-table-low-wmark** *low-water-mark*

Context

config>service>vpls

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command specifies the MFIB low watermark. When the percentage filling level of the MFIB drops below the configured value, the corresponding trap is cleared and a log entry is added.

Parameters

low-water-mark

Specifies the multicast FIB low watermark as a percentage.

Values 1 to 100

Default 90%

mfib-table-size

Syntax

mfib-table-size *table-size*

no mfib-table-size

Context

config>service>vpls

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command specifies the maximum number of (s,g) entries in the MFIB database for this VPLS instance.

The *size* parameter specifies the maximum number of multicast database entries for both learned and static multicast addresses for the VPLS instance. When a table-size limit is set on the MFIB of a service that is lower than the current number of dynamic entries present in the MFIB, the number of entries remains above the limit.

The **no** form of this command removes the configured maximum MFIB table size.

Parameters

table-size

Specifies the maximum number of (s,g) entries allowed in the MFIB.

Values 1 to 1024

remote-age

Syntax

remote-age *seconds*

no remote-age

Context

config>service>vpls

config>template>vpls-template

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command specifies the aging time for remotely learned MAC addresses in the FDB for the VPLS instance. In a VPLS service, MAC addresses are associated with a SAP or an SDP. MACs associated with a SAP are called local MACs, and MACs associated with an SDP are called remote MACs.

Like in a Layer 2 switch, learned MACs can be aged out if no packets are sourced from the MAC address for a period of time (the aging time). In each VPLS service instance, there are independent aging timers for local learned MAC and remote learned MAC entries in the FDB. The **remote-age** timer specifies the aging time for remote learned MAC addresses. To reduce the amount of signaling required between switches, configure this timer with a value larger than the **local-age** timer.

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

Default

remote-age 900

Parameters

seconds

Specifies the aging time for remote MACs, in seconds.

Values 60 to 86400

send-flush-on-failure

Syntax

[**no**] **send-flush-on-failure**

Context

config>service>vpls

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables sending out "flush-all-from-ME" messages to all LDP peers included in the affected VPLS, in the event of physical port failures or "oper-down" events of individual SAPs.

This command provides an LDP-based mechanism for recovering a physical link failure in a dual-homed connection to a VPLS service. This method provides an alternative to RSTP solutions where dual homing redundancy and recovery, in the case of link failure, is resolved by RSTP running between a PE router and CE devices. If the endpoint is configured within the VPLS and the **send-flush-on-failure** command is enabled, flush-all-from-me messages are sent out only when all spoke SDPs associated with the endpoint go down.

This feature cannot be enabled on management VPLS.

Default

no send-flush-on-failure

service-mtu

Syntax

service-mtu *octets*

no service-mtu

Context

config>service>vpls

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the service payload Maximum Transmission Unit (MTU), in bytes, for the service. This MTU value overrides the service-type default MTU. The **service-mtu** command defines the payload capabilities of the service and is used by the system to validate the SAP and SDP binding operational state within the service.

The service MTU and a SAP service delineation encapsulation overhead (that is, 4 bytes for a dot1q tag) is used to derive the required MTU of the physical port or channel on which the SAP was created. If the required payload is larger than the port or channel MTU, the SAP is placed in an inoperative state. If the required MTU is equal to or less than the port or channel MTU, the SAP is able to transition to the operative state.

When a service MTU, port or channel MTU, or path MTU is dynamically or administratively modified, all associated SAP and SDP binding operational states are automatically reevaluated.

The **no** form of this command reverts the **service-mtu** value for the indicated service type to the default.

Note:
To disable service MTU check, run the **no service-mtu-check** command. Disabling service MTU check allows the packets to pass to the egress if the packet length is less than or equal to the MTU configured on the port.

Default

service-mtu 1514

Parameters

octets

Specifies the size of the MTU in octets, expressed as a decimal integer. The following table displays MTU values for specific VC types.

Table 52: MTU values for VC types

VC-type	Example service MTU	Advertised MTU
Ethernet	1514	1500
Ethernet (with preserved dot1q)	1518	1504
VPLS	1514	1500
VPLS (with preserved dot1q)	1518	1504
VLAN (dot1p transparent to MTU value)	1514	1500
VLAN (QinQ with preserved bottom Qtag)	1518	1504

Values 1 to 9194

service-mtu-check

Syntax

[**no**] **service-mtu-check**

Context

config>service>vpls

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command, when disabled, allows the packets to pass to the egress if the packet length is less than or equal to the MTU configured on the port. The length of the packet sent from a SAP is limited only by the access port MTU. In case of a pseudowire, the length of a packet is limited by the network port MTU (including the MPLS encapsulation).

The **no** form of this command disables the service MTU check.

Note: If TLDP is used for signaling, the configured value for service-mtu is used during a pseudowire setup.

Default

enabled

root-guard

Syntax

[**no**] **root-guard**

Context

config>service>vpls>sap>stp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command specifies whether this port is allowed to become an STP root port. It corresponds to the restrictedRole parameter in 802.1Q. If set, it can cause lack of spanning tree connectivity.

Default

no root-guard

tod-suite

Syntax

tod-suite *tod-suite-name*

no tod-suite

Context

config>service>vpls>sap

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

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

Default

no tod-suite

Parameters

tod-suite-name

Specifies the collection of policies (ACLs, QoS), including time-ranges, that define the full or partial behavior of a SAP. The suite can be applied to more than one SAP.

vsi-id

Syntax

vsi-id

Context

config>service>vpls>bgp-ad

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

Commands in this context configure the Virtual Switch Instance Identifier (VSI-ID).

prefix

Syntax

prefix *low-order-vsi-id*

no prefix

Context

config>service>vpls>bgp-ad>vsi-id

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command specifies the low-order 4 bytes used to compose the VSI-ID to use for NLRI in BGP auto-discovery in the specified VPLS service.

If no value is set, the system IP address is used.

Default

no prefix

Parameters

low-order-vsi-id

Specifies a unique VSI-ID.

Values *ip-addr* — a.b.c.d

raw-prefix — 0 to 4294967295

5.7.2.1.3 VPLS STP commands

stp

Syntax

stp

Context

config>service>vpls

config>service>vpls>sap

config>template>vpls-template

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

Commands in this context configure the Spanning Tree Protocol (STP) parameters.

The Nokia STP is the Spanning Tree Protocol (STP) with a few modifications to better suit the operational characteristics of VPLS services. The most evident change is to the root bridge election. Because the core network operating between the service routers should not be blocked, the root path is calculated from the core perspective.

auto-edge

Syntax

auto-edge

no auto-edge

Context

config>service>vpls>sap>stp

config>service>vpls>spoke-sdp>stp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures automatic detection of the edge port characteristics of the SAP.

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

Default

auto-edge

edge-port

Syntax

[**no**] **edge-port**

Context

config>service>vpls>sap>stp

config>service>vpls>spoke-sdp>stp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the SAP as an edge or non-edge port. If the **auto-edge** command is enabled for the SAP, this value is used only as the initial value.

However, RSTP can detect that the actual situation is different from what the **edge-port** command may indicate.

Initially, the value of the SAP parameter is set to edge-port. This value changes in the following circumstances:

- a BPDU is received on that port. This means that there is another bridge connected to this port; in this case, the edge-port becomes disabled.
- auto-edge is configured and no BPDU is received within a specified period of time; RSTP concludes that it is on an edge and enables the edge-port

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

Default

no edge-port

forward-delay

Syntax

forward-delay *seconds*

no forward-delay

Context

config>service>vpls>stp

config>template>vpls-template>stp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

RSTP, as defined in the IEEE 802.1D-2004 standards, transitions to the forwarding state via a handshaking mechanism (rapid transition), without wait times. If handshaking fails (for example, on shared links (see the following)), the system falls back to the timer-based mechanism defined in the original STP (802.1D-1998) standard.

A shared link is a link with more than two nodes (for example, a shared 10/100BaseT segment). The **port-type** command is used to configure a link as point-to-point or shared.

For timer-based transitions, the 802.1D-2004 standard defines an internal variable forward-delay, which is used in calculating the default number of seconds that a SAP spends in the discarding and learning states when transitioning to the forwarding state.

The value of the **forward-delay** parameter depends on the STP operating mode of the VPLS instance, as described in the following:

- in rstp or mstp mode, but only when the SAP has not fallen back to legacy STP operation, the value configured by the **hello-time** command is used
- in all other situations, the value configured by the **forward-delay** command is used

Default

forward-delay 15

Parameters

seconds

Specifies the forward delay timer for the STP instance, in seconds.

Values 4 to 30

hello-time

Syntax

hello-time *hello-time*

no hello-time

Context

config>service>vpls>stp

config>template>vpls-template>stp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the STP hello time for the VPLS STP instance.

The *hello-time* parameter defines the default timer value that controls the sending interval between BPDU configuration messages by this bridge, on ports where this bridge assumes the designated role.

The active hello time for the spanning tree is determined by the root bridge (except when the STP is running in RSTP mode; in this case, the hello time is always taken from the locally configured parameter).

The configured hello time can also be used to calculate the forward delay. See the auto-edge command for more information.

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

Default

hello-time 2

Parameters

hello-time

Specifies the hello time for the STP instance, in seconds.

Values 1 to 10

hold-count

Syntax

hold-count *BDPU tx hold count*

no hold-count

Context

config>service>vpls>stp

config>template>vpls-template>stp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the peak number of BPDUs that can be transmitted in a period of one second.

The **no** form of this command reverts to the default value

Default

hold-count 6

Parameters

BDPU tx hold count

Specifies the hold count for the STP instance, in seconds.

Values 1 to 10

link-type

Syntax

link-type {**pt-pt** | **shared**}

no link-type

Context

config>service>vpls>sap>stp

config>service>vpls>spoke-sdp>stp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the maximum number of bridges for STP behind this SAP.

If there is only a single bridge, transitioning to forwarding state is based on handshaking (fast transitions). If more than two bridges are connected via a shared media, their SAPs should all be configured as shared, and timer-based transitions are used.

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

Default

link-type pt-pt

mst-instance

Syntax

mst-instance *mst-inst-number*

Context

config>service>vpls>sap>stp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures Multiple Spanning Tree Instance (MSTI) related parameters at the SAP level. This context can be open only for existing MSTIs defined at the service level.

Parameters

mst-inst-number

Specifies an existing MSTI number.

Values 1 to 4094

mst-path-cost

Syntax

mst-path-cost *inst-path-cost*

no mst-path-cost

Context

config>service>vpls>sap>stp>mst-instance

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This commands specifies path-cost within a specific instance. If a loop occurs, this parameter indicates the probability of a specific port being assigned a forwarding state. The highest value expresses the lowest priority.

By default, the path-cost is proportional to the link speed.

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

Parameters

inst-path-cost

Specifies the contribution of this port to the MSTI path cost.

Values 1 to 200000000

mst-port-priority

Syntax

mst-port-priority *stp-priority*

no mst-port-priority

Context

config>service>vpls>sap>stp>mst-instance

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command specifies the port priority within a specific instance. If a loop occurs, this parameter indicates the probability of a specific port being assigned a forwarding state.

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

Default

mst-port-priority 128

Parameters

stp-priority

Specifies the value of the port priority field.

max-age

Syntax

max-age *seconds*

no max-age

Context

config>service>vpls>stp

config>template>vpls-template>stp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures how many hops a BPDU can traverse the network starting from the root bridge. The message age field in a BPDU transmitted by the root bridge is initialized to 0. Each other bridge takes the message_age value from BPDUs received on their root port and increments this value by 1. The message_age therefore reflects the distance from the root bridge. BPDUs with a message age exceeding the **max-age** value are ignored.

STP uses the **max-age** value configured in the root bridge. This value is propagated to the other bridges via the BPDUs.

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

Default

max-age 20

Parameters

seconds

Specifies the max info age for the STP instance in seconds.

Values 6 to 40

mode

Syntax

mode {**rstp** | **comp-dot1w** | **dot1w** | **mstp** | **pmstp**}

no mode

Context

config>service>vpls>stp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command specifies the version of STP that the bridge is currently running.

See Spanning tree operating modes for information about these modes.

The **no** form of this command reverts to the default.

Default

mode rstp

Parameters

rstp

Keyword that corresponds to the Rapid STP specified in IEEE 802.1D/D4-2003.

dot1w

Keyword that corresponds to the mode where the Rapid STP is backward compatible with IEEE 802.1w.

compdot1w

Keyword that corresponds to the Rapid STP fully conformant to IEEE 802.1w.

mstp

Keyword that sets MSTP as the STP mode of operation. Corresponds to the Multiple STP specified in 802.1Q REV/D5.0-09/2005

pmstp

This mode is supported only in VPLS services where the mVPLS flag is configured.

mst-instance

Syntax

[**no**] **mst-instance** *mst-inst-number*

Context

config>service>vpls>stp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures Multiple Spanning Tree Instance (MSTI) related parameters. MSTP supports "16" instances. The instance "0" is mandatory (by protocol) and cannot be created by the CLI. The software automatically maintains this instance.

Parameters

mst-inst-number

Specifies the MST instance.

Values 1 to 4094

mst-priority

Syntax

mst-priority *bridge-priority*

no mst-priority

Context

config>service>vpls>stp>mst-instance

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command specifies the bridge priority for this specific Multiple Spanning Tree Instance for this service. The *bridge-priority* value reflects likelihood that the switch is chosen as the regional root switch (65535 represents the least likely). It is used as the highest 4 bits of the bridge ID included in the MSTP BPDUs generated by this bridge.

The values of the priority are only multiples of 4096 (4k). If a value is specified that is not a multiple of 4K, the value is replaced by the closest multiple of 4K (lower than the value entered).

All instances that are created by the vlan-range command do not have an explicit definition of bridge-priority and inherit the default value.

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

Default

mst-priority 32768

Parameters

bridge-priority

Specifies the priority of this specific MSTI for this service.

Values 0 to 65535

vlan-range

Syntax

[**no**] **vlan-range** [*vlan-range*]

Context

config>service>vpls>stp>mst-instance

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command specifies a range of VLANs associated with a particular MSTI. This range applies to all SAPs of the mVPLS.

Every VLAN range that is not assigned within any of the created mst-instance is automatically assigned to mst-instance 0. This instance is automatically maintained by the software and cannot be modified. Changing the VLAN range value can be performed only when the specific mst-instance is shut down.

The **no** form of this command removes the **vlan-range** from the specific mst-instance.

Parameters

vlan-range

The first VLAN range specifies the left-bound (minimum value) of a range of VLANs that are associated with the mVPLS SAP. This value must be smaller than (or equal to) the second VLAN range value. The second VLAN range specifies the right-bound (maximum value) of a range of VLANs that are associated with the mVPLS SAP.

Values 1 to 4094

mst-max-hops

Syntax

mst-max-hops *hops-count*

no mst-max-hops

Context

config>service>vpls>stp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command specifies the number of hops in the region before BPDU is discarded and the information held for the port is aged out. The root bridge of the instance sends a BPDU (or M-record) with remaining-hop-count set to configured *max-hops*. When a bridge receives the BPDU (or M-record), it decrements the received remaining-hop-count by 1 and propagates it in the BPDU (or M-record) it generates.

The **no** form of this command reverts the *hops-count* to the default value.

Default

mst-max-hops 20

Parameters

hops-count

Specifies the maximum number of hops.

Values 1 to 40

mst-name

Syntax

mst-name *region-name*

no mst-name

Context

config>service>vpls>stp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command defines an MST region name. Two bridges are considered as a part of the same MST region as soon as their configuration of the MST region name, the MST-revision and VLAN-to-instance assignment is identical.

The **no** form of this command removes *region-name* from the configuration.

Default

no mst-name

Parameters

region-name

Specifies an MST-region name, up to 32 characters.

mst-revision

Syntax

mst-revision *revision-number*

Context

config>service>vpls>stp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command defines the MST configuration revision number. Two bridges are considered as a part of the same MST region if their configured MST-region name, MST-revision, and VLAN-to-instance are identical.

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

Default

mst-revision 0

Parameters

revision-number

Specifies the MSTP revision number to define the MSTP region.

Values 0 to 65535

path-cost

Syntax

path-cost *sap-path-cost*

no path-cost

Context

config>service>vpls>sap>stp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the STP path cost for the SAP.

The path cost is used by STP to calculate the path cost to the root bridge. The path cost in BPDUs received on the root port is incremented with the configured path cost for that SAP. When BPDUs are sent out other egress SAPs, the newly calculated root path cost is used.

STP suggests that the path cost is defined as a function of the link bandwidth. Because SAPs are controlled by complex queuing dynamics in the STP, path cost is a static configuration.

The **no** form of this command reverts the path cost to the default value.

Parameters

path-cost

Specifies the path cost for the SAP.

Values 1 to 200000000 (1 is the lowest cost)

Default 10

port-num

Syntax

[**no**] **port-num** *virtual-port-number*

Context

config>service>vpls>sap>stp

config>service>vpls>spoke-sdp>stp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the virtual port number, which uniquely identifies a SAP within configuration BPDUs.

The internal representation of a SAP is unique to a system and has a reference space much bigger than the 12 bits definable in a configuration BPDU. STP takes the internal representation value of a SAP and identifies it using a virtual port number that is unique from every other SAP defined on the TLS. The virtual port number is assigned at the time that the SAP is added to the TLS. Because the order that the SAP was added to the TLS is not preserved between reboots of the system, the virtual port number may change between restarts of the STP instance.

The virtual port number cannot be administratively modified.

priority

Syntax

priority *bridge-priority*

no priority

Context

config>service>vpls>stp

config>template>vpls-template>stp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command is used to populate the priority portion of the bridge ID field within outbound BPDUs (the most significant 4 bits of the bridge ID). It is also used as part of the decision process when determining the best BPDU between messages received and sent. All values are truncated to multiples of 4096, conforming with IEEE 802.1t and 802.1D-2004.

The **no** form of this command reverts the bridge priority to the default value.

Default

priority 4096

Parameters

bridge-priority

Specifies the bridge priority for the STP instance.

Values Allowed values are integers in the range of 4096 to 65535 (4096 is the highest priority).

The actual *bridge-priority* value stored and used is the number entered with the lowest 12 bits masked off, which means the actual range of values is 4096 to 61440 in increments of 4096.

priority

Syntax

priority *stp-priority*

no priority

Context

config>service>vpls>spoke-sdp

config>service>vpls>sap>stp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the STP priority for the SAP or spoke SDP.

When configuration BPDUs are received, the priority is used in some circumstances as a tie breaking mechanism to determine whether the SAP is designated or blocked.

In traditional STP implementations (802.1D-1998), this field is called the port priority and has a value of 0 to 255. This field is coupled with the port number (0 to 255 also) to create a 16-bit value. In the latest STP standard (802.1D-2004), only the upper 4 bits of the port priority field are used to encode the SAP priority. The remaining 4 bits are used to extend the port ID field into a 12-bit virtual port number field. The virtual port number uniquely references a SAP within the STP instance.

STP computes the actual priority by taking the input value and masking out the lower four bits. The result is the value that is stored in the priority parameter. For example, if a value of 0 is entered, masking out the lower 4 bits results in a parameter value of 0. If a value of 255 is entered, the result is 240.

The **no** form of this command reverts the STP priority to the default value.

Default

priority 128

Parameters

stp-priority

Specifies the STP priority value for the SAP or spoke SDP.

Values 0 to 255 (with masking, actual values are 0 to 240, in increments of 16)

Default 128

5.7.2.1.4 VPLS SAP commands

sap

Syntax

sap *sap-id* [**split-horizon-group** *group-name*] [**create**] [**capture-sap**] [**eth-ring** *ring-index*] [**g8032-shg-enable**]

no sap *sap-id*

Context

config>service>vpls

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command creates a SAP within a service. A SAP is a combination of port and encapsulation parameters that identifies the SAP on the interface and within the 7210 SAS. Each SAP must be unique.

A physical port can have only one SAP to be part of one service. Multiple SAPs can be defined over a physical port, but each of these SAPs should belong to a different service.

All SAPs must be explicitly created. If no SAPs are created within a service or on an IP interface, a SAP does 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.

If a port is shut down, all SAPs on that port become operationally down. When a service is shut down, SAPs for the service are not displayed as operationally down, although all traffic traversing the service is 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 are also deleted.

Special Cases

A default SAP has the following format: port-id:*. This type of SAP is supported only on Ethernet MDAs, and its creation is allowed only in the scope of Layer 2 services (Epipe and VPLS).

Parameters

sap-id

Specifies the physical port identifier portion of the SAP definition. See Common CLI command descriptions for command syntax.

create

Keyword used to create a SAP instance. The **create** keyword requirement can be enabled or disabled using the **environment>create** context.

g8032-shg-enable

Keyword that must be used only with the SAPs created in the service for the virtual channel on the interconnection nodes in a topology that uses multiple rings. This command creates a split-horizon group to ensure that Sub-Ring control messages from the major ring are only passed to the Sub-Ring control service.

eth-ring

Keyword to create an instance of a Ring APS Control SAP or a Data SAP whose traffic is protected by a Ring APS Instance.

ring-index

Specifies the ring index of the Ethernet ring.

split-horizon-group *group-name*

Specifies the name of the split horizon group to which the SAP belongs.

accounting-policy

Syntax

accounting-policy *acct-policy-id*

no accounting-policy

Context

config>service>vpls>sap

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the accounting policy context that can be applied to a SAP.

An accounting policy must be defined before it can be associated with a SAP. If the *policy-id* does not exist, an error message is generated.

A maximum of one accounting policy can be associated with a SAP at one time. Accounting policies are configured in the **config>log** context.

The **no** form of this command removes the accounting policy association from the SAP, and the accounting policy reverts to the default value.

Parameters

acct-policy-id

Specifies the accounting *policy-id* as configured in the **config>log>accounting-policy** context.

Values 1 to 99

discard-unknown-source

Syntax

[**no**] **discard-unknown-source**

Context

config>service>vpls>sap

config>service>vpls>spoke-sdp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

When this command is enabled, packets received on a SAP or with an unknown source MAC address are dropped only if the maximum number of MAC addresses for that SAP (see the command) has been reached. If the **max-nbr-mac-addr** command has not been configured for the SAP, enabling the **discard-unknown-source** command has no effect.

When disabled, the packets are forwarded based on the destination MAC addresses.

The **no** form of this command causes packets with an unknown source MAC addresses to be forwarded by destination MAC addresses in VPLS.

Default

no discard-unknown-source

dist-cpu-protection

Syntax

dist-cpu-protection *policy-name*

no dist-cpu-protection

Context

config>service>vpls>sap

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command assigns a valid existing Distributed CPU Protection (DCP) policy to a SAP. By default, no DCP policy is associated with the SAP.

The **no** form of this command disables the use of DCP policies for the SAP.

Default

no dist-cpu-protection

Parameters

policy-name

Specifies the name of the DCP policy, up to 32 characters.

5.7.2.1.5 VPLS SAP statistics commands

statistics

Syntax

statistics

Context

config>service>vpls>sap

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

Commands in this context configure the counters associated with SAP ingress and egress.

ingress

Syntax

ingress

Context

config>service>vpls>sap>statistics

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

Commands in this context configure the ingress SAP statistics counters.

counter-mode

Syntax

counter-mode {**in-out-profile-count** | **forward-drop-count**}

Context

config>service>vpls>sap>statistics>ingress

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the counter mode for the counters associated with SAP ingress meters (also known as policers). A pair of counters is available with each meter. These counters count different events based on the **counter-mode** value.

Note: The **counter-mode** command can be changed if an accounting policy is associated with a SAP. If the **counter-mode** is changed, the counters associated with the meter are reset and the counts are cleared. If an accounting policy is in use when the **counter-mode** is changed, a new record is written into the current accounting file.

Execute the following sequence of commands on the specified SAP to ensure the correct statistics are collected when the counter-mode is changed:

1. Execute the **config service vpls sap no collect-stats** command to disable writing of accounting records for the SAP.
2. Change the **counter-mode** to the desired option by executing the **config service vpls sap counter-mode** {**in-out-profile-count** | **forward-drop-count**} command
3. Execute the **config service vpls sap collect-stats** command to enable writing of accounting records for the SAP.

Default

in-out-profile-count

Parameters

forward-drop-count

Keyword to specify that one counter counts the forwarded packets and octets received on ingress of a SAP and another counts the dropped packets. The forwarded count is the sum of in-profile and out-of-profile packets and octets received on SAP ingress. The dropped count is the count of packets and octets dropped by the policer. A packet is determined to be in-profile or out-of-profile based on the meter rate parameters configured. A packet is dropped by the policer if it exceeds the configured PIR rate. The in-profile count and out-of-profile count is not individually available when operating in this mode.

in-out-profile-count

Keyword to specify that one counter counts the total in-profile packets and octets received on ingress of a SAP and another counts the total out-of-profile packets and octets received on ingress of a SAP. A packet is determined to be in-profile or out-of-profile based on the meter rate parameters configured. A packet is dropped by the policer if it exceeds the configured PIR rate. Dropped counts are not maintained in hardware when this mode is used. It is obtained by subtracting the sum of in-profile count and out-of-profile count from the total SAP ingress received count and displayed.

drop-count-extra-vlan-tag-pkts

Syntax

[**no**] **drop-count-extra-vlan-tag-pkts**

Context

config>service>vpls>sap>statistics>ingress

config>service>vpls>mesh-sdp>statistics>ingress

config>service>vpls>spoke-sdp>statistics>ingress

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command associates a counter that enables the counting of extra VLAN-tag dropped packets for the SAP, spoke-SDP, or mesh SDP. A limited number of such counters are available for use.

The **no** form of this command removes the associated counter.

5.7.2.1.6 ETH-CFM service commands

eth-cfm

Syntax

eth-cfm

Context

config>service>vpls

config>service>vpls>mesh-sdp

config>service>vpls>spoke-sdp

config>service>vpls>sap

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

Commands in this context configure ETH-CFM parameters.

mep

Syntax

mep *mep-id* **domain** *md-index* **association** *ma-index* [**direction** {**up** | **down**}] **primary-vlan-enable**

no mep *mep-id* **domain** *md-index* **association** *ma-index*

Context

config>service>vpls>mesh-sdp>eth-cfm

config>service>vpls>sap>eth-cfm

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the ETH-CFM maintenance endpoint (MEP).

The **primary-vlan-enable** parameter provides a method for linking the MEP with the primary VLAN configured under the bridge-identifier for the MA. MEPs cannot be changed from or to primary vlan functions. This must be configured as part of the creation step and can only be changed by deleting the MEP and recreating it. Primary VLANs are only supported under Ethernet SAPs.

Parameters

mep-id

Specifies the maintenance association endpoint identifier.

Values 1 to 8191

md-index

Specifies the maintenance domain (MD) index value.

Values 1 to 4294967295

ma-index

Specifies the MA index value.

Values 1 to 4294967295

direction {up | down}

Indicates the direction in which the maintenance association (MEP) faces on the bridge port. Direction is not supported when a MEP is created directly in the **vpls>eth-cfm** context (vMEP).

Values **down** — Sends ETH-CFM messages away from the MAC relay entity.

up — Sends ETH-CFM messages toward the MAC relay entity.

primary-vlan-enable

Provides a method for linking the MEP with the primary VLAN configured under the bridge-identifier for the MA.

ais-enable

Syntax

[**no**] **ais-enable**

Context

config>service>vpls>mesh-sdp>eth-cfm>mep

config>service>epipe>spoke-sdp>eth-cfm>mep

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables the generation and reception of AIS messages.

client-meg-level

Syntax

client-meg-level [[*level* [*level* **...**]]

no client-meg-level

Context

config>service>vpls>mesh-sdp>eth-cfm>mep>ais-enable

config>service>epipe>spoke-sdp>eth-cfm>mep>ais-enable

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the client Maintenance Entity Group (MEG) levels to use for AIS message generation. Up to 7 levels can be provisioned, with the restriction that the client MEG level must be higher than the local MEG level.

Parameters

level

Specifies the client MEG level.

Values 1 to 7

Default 1

interval

Syntax

interval {**1** | **60**}

no interval

Context

config>service>vpls>mesh-sdp>eth-cfm>mep>ais-enable

config>service>epipe>spoke-sdp>eth-cfm>mep>ais-enable

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command specifies the transmission interval of AIS messages in seconds.

Parameters

1 | 60

Specifies the transmission interval of AIS messages, in seconds.

Default 1

priority

Syntax

priority *priority-value*

no priority

Context

config>service>vpls>mesh-sdp>eth-cfm>mep>ais-enable

config>service>epipe>spoke-sdp>eth-cfm>mep>ais-enable

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command specifies the priority of AIS messages originated by the node.

Parameters

priority-value

Specifies the priority value of the AIS messages originated by the node.

Values 0 to 7

Default 7

ccm-enable

Syntax

[**no**] **ccm-enable**

Context

config>service>vpls>mep

config>service>vpls>sap>eth-cfm>mep

config>service>vpls>mesh-sdp>mep

config>service>epipe>spoke-sdp>eth-cfm>mep

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables the generation of CCM messages.

The **no** form of this command disables the generation of CCM messages.

ccm-ltm-priority

Syntax

ccm-ltm-priority *priority*

no ccm-ltm-priority

Context

config>service>vpls>sap>eth-cfm>mep

config>service>vpls>mesh-sdp>mep config>service>epipe>spoke-sdp>eth-cfm>mep

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command specifies the priority value for CCMs and LTMs transmitted by the MEP.

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

Parameters

priority

Specifies the priority of CCM and LTM messages.

Values 0 to 7

Default highest priority on the bridge-port

eth-test-enable

Syntax

[**no**] **eth-test-enable**

Context

config>service>vpls>spoke-sdp>eth-cfm>mep

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

For ETH-test to work, configure ETH-test parameters on both sender and receiver nodes. The ETH-test can be performed using the following OAM command:

oam eth-cfm eth-test *mac-address* **mep** *mep-id* **domain** *md-index* **association** *ma-index* [**priority** *priority*] [**data-length** *data-length*]

A check is performed for both the provisioning and test to ensure the MEP is a Y.1731 MEP (MEP provisioned with domain format none, association format icc-based). If not, the operation fails. An error message in the CLI and SNMP indicates the problem.

test-pattern

Syntax

test-pattern {**all-zeros** | **all-ones**} [**crc-enable**]

no test-pattern

Context

config>service>vpls>sap>eth-cfm>mep>eth-test-enable

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the test pattern for eth-test frames.

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

Parameters

all-zeros

Specifies to use all zeros in the test pattern.

all-ones

Specifies to use all ones in the test pattern.

crc-enable

Generates a CRC checksum.

Default all-zeros

fault-propagation-enable

Syntax

fault-propagation-enable {**use-if-tlv** | **suspend-ccm**}

no fault-propagation-enable

Context

config>service>epipe>sap>eth-cfm>mep

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the fault propagation for the MEP.

Parameters

use-if-tlv

Keyword to specify the use of the interface TLV.

suspend-ccm

Keyword to suspend the continuity check messages.

low-priority-defect

Syntax

low-priority-defect {**allDef** | **macRemErrXcon** | **remErrXcon** | **errXcon** | **xcon** | **noXcon**}

Context

config>service>epipe>spoke-sdp>eth-cfm>mep

config>service>vpls>mesh-sdp>eth-cfm>mep

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command specifies the lowest priority defect that is allowed to generate a fault alarm.

Default

macRemErrXcon

Parameters

allDef | macRemErrXcon | remErrXcon | errXcon | xcon | noXcon

Specifies the lowest priority defect.

Values

allDef	DefRDICCM, DefMACstatus, DefRemoteCCM, DefErrorCCM, and DefXconCCM
macRemErrXcon	Only DefMACstatus, DefRemoteCCM, Def ErrorCCM, and DefXconCCM
remErrXcon	Only DefRemoteCCM, DefErrorCCM, and Def XconCCM
errXcon	Only DefErrorCCM and DefXconCCM
xcon	Only DefXconCCM; or

noXcon	No defects DefXcon or lower are to be reported

mac-address

Syntax

mac-address *mac-address*

no mac-address

Context

config>service>vpls>mesh-sdp>eth-cfm>mep

config>service>epipe>spoke-sdp>eth-cfm>mep

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command specifies the MAC address of the MEP.

The **no** form of this command reverts the MAC address of the MEP back to that of the port (if the MEP is on a SAP) or the bridge (if the MEP is on a spoke).

Parameters

mac-address

Specifies the MAC address of the MEP.

Values 6-byte mac-address in the form of xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx of the MEP. Must be unicast. Using the all zeros address is equivalent to the **no** form of this command.

one-way-delay-threshold

Syntax

one-way-delay-threshold *seconds*

Context

config>service>vpls>sap>eth-cfm>mep

config>service>epipe>spoke-sdp>eth-cfm>mep

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables or disables eth-test functionality on MEP.

Parameters

seconds

Specifies the one-way delay threshold, in seconds.

Values 0 to 600

Default 3

mip

Syntax

mip [**mac** *mac-address*] [**primary-vlan-enable** *vlan-id*]

mip default-mac [**primary-vlan-enable** *vlan-id*]

no mip [**primary-vlan-enable** *vlan-id*]

Context

config>service>vpls>sap>eth-cfm

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command allows Maintenance Intermediate Points (MIPs) to be created if mhf-creation for the MA is configured using the default option.

The **primary-vlan-enable** parameter provides a method for linking the MEP with the primary VLAN configured under the bridge-identifier for the MA. MEPs cannot be changed from or to primary vlan functions. This must be configured as part of the creation step and can only be changed by deleting the MEP and recreating it. Primary VLANs are only supported under Ethernet SAPs.

Parameters

mac-address

Specifies the MAC address of the MIP.

Values 6-byte mac-address in the form of xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx of the MIP. The MAC must be unicast. Using the all zeros address is equivalent to the no form of this command.

default-mac

Using the no command deletes the MIP. This keyword is useful if the operator needs to change the MAC back to the default MAC without having to delete the MIP and reconfiguring.

Default no mip

primary-vlan-enable ***vlan-id***

Provides a method for linking the MEP with the primary VLAN configured under the bridge-identifier for the MA.

Values 0 to 4094

limit-mac-move

Syntax

limit-mac-move [**blockable** | **non-blockable**]

no limit-mac-move

Context

config>service>vpls>spoke-sdp

config>service>vpls>sap

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command specifies whether the mac-move agent, when enabled using the **config service vpls mac-move** or **config service epipe mac-move** command, limits the MAC relearn (move) rate on this SAP.

Default

blockable

Parameters

blockable

Keyword to specify that the agent monitors the MAC relearn rate on the SAP and blocks it when the relearn rate is exceeded.

non-blockable

Keyword to specify this SAP is not blocked, and another blockable SAP is blocked instead.

mac-pinning

Syntax

[**no**] **mac-pinning**

Context

config>service>vpls>sap

config>service>vpls>spoke-sdp

config>service>vpls>mesh-sdp

config>service>vpls>endpoint config>service>pw-template

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command disables relearning of MAC addresses on other mesh SDPs within the VPLS.

The MAC address remains attached to a specific mesh for duration of its age-timer.

The age of the MAC address entry in the FIB is set by the age timer. If MAC aging is disabled on a specific VPLS service, a MAC address learned on a mesh with **mac-pinning** enabled remains in the FIB on this mesh forever. Every event that otherwise results in relearning is logged (MAC address; original - mesh SDP; new - mesh SDP).

Default

no mac-pinning

max-nbr-mac-addr

Syntax

max-nbr-mac-addr *table-size*

no max-nbr-mac-addr

Context

config>service>vpls>sap

config>service>vpls>spoke-sdp config>service>vpls>endpoint

config>service>pw-template

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command specifies the maximum number of FDB entries for both learned and static MAC addresses for this SAP.

When the configured limit is reached, and discard-unknown-source has been enabled for this SAP or spoke-SDP (see the command), packets with unknown source MAC addresses are discarded.

The **no** form of this command restores the global MAC learning limitations for the SAP.

Default

no max-nbr-mac-addr

Parameters

table-size

Specifies the maximum number of learned and static entries allowed in the FDB of this service.

Values 1 to 65535 (X)

Values 1to 61439 (7210 SAS-R6 and 7210 SAS-R12)

statistics

Syntax

statistics

Context

config>service>vpls>sap

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

Commands in this context configure the counters associated with SAP ingress and egress.

ingress

Syntax

ingress

Context

config>service>epipe>sap>statistics

config>service>vpls>sap>statistics

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

Commands in this context configure the ingress SAP statistics counter.

counter-mode

Syntax

counter-mode {**in-out-profile-count** | **forward-drop-count**}

Context

config>service>epipe>sap>statistics>ingress

config>service>vpls>sap>statistics>ingress

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the counter mode for the counters associated with SAP ingress meters (also known as policers). A pair of counters is available with each meter. These counters count different events based on the **counter-mode** value.

The **counter-mode** can be changed if an accounting policy is associated with a SAP. If the **counter-mode** is changed, the counters associated with the meter are reset and the counts are cleared. If an accounting policy is in use when the **counter-mode** is changed a new record is written into the current accounting file.

Execute the following sequence of commands to ensure a new accounting file is generated when the **counter-mode** is changed:

1. Execute the **config service epipe** or **vpls sap no collect-stats** command to disable the writing of accounting records.
2. Change the **counter-mode** to the required value by executing the **config service epipe** or **vpls sap counter-mode** {**in-out-profile-count** | **forward-drop-count**} command.
3. Execute the **config service epipe** or **vpls sap collect-stats** command to enable writing of accounting records.

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

Default

in-out-profile-count

Parameters

forward-drop-count

Keyword to specify that one counter counts the forwarded packets and octets received on ingress of a SAP and another counts the dropped packets. The forwarded count is the sum of in-profile and out-of-profile packets and octets received on SAP ingress. The dropped count is count of packets and octets dropped by the policer. A packet is determined to be in-profile or out-of-profile based on the meter rate parameters configured. A packet is dropped by the policer if it exceeds the configured PIR rate. The in-profile count and out-of-profile count is not individually available when operating in this mode.

in-out-profile-count

Keyword to specify that one counter counts the total in-profile packets and octets received on ingress of a SAP and another counts the total out-of-profile packets and octets received on ingress of a SAP. A packet is determined to be in-profile or out-of-profile based on the meter rate parameters configured. A packet is dropped by the policer if it exceeds the configured PIR rate. Dropped counts are not maintained in hardware when this mode is used. It is obtained by subtracting the sum of in-profile count and out-of-profile count from the total SAP ingress received count and displayed.

static-mac

Syntax

[**no**] **static-mac** *ieee-mac-address* [**create**]

Context

config>service>vpls>sap

config>service>vpls>mesh-sdp

config>service>vpls>spoke-sdp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures a local static MAC entry in the VPLS FDB associated with the SAP.

In a VPLS service, MAC addresses are associated with a SAP or with an SDP. MACs associated with a SAP are classified as local MACs, and MACs associated with an SDP are remote MACs.

Local static MAC entries create a permanent MAC address to SAP association in the forwarding database for the VPLS instance, so that the MAC address is not learned on the edge device.

Static MAC definitions on one edge device are not propagated to other edge devices participating in the VPLS instance; that is, each edge device has an independent forwarding database for the VPLS.

Only one static MAC entry (local or remote) can be defined per MAC address per VPLS instance.

By default, no static MAC address entries are defined for the SAP.

The **no** form of this command deletes the static MAC entry with the specified MAC address associated with the SAP from the VPLS FDB.

Parameters

ieee-mac-address

Specifies the 48-bit MAC address for the static ARP in the form *aa*:*bb*:*cc*:*dd*:*ee*:*ff* or *aa*-*bb*-*cc*-*dd*-*ee*-*ff* where *aa*, *bb*, *cc*, *dd*, *ee* and *ff* are hexadecimal numbers. Allowed values are any non-broadcast, non-multicast MAC and non-IEEE reserved MAC addresses.

create

Mandatory keyword for specifying a static MAC address.

managed-vlan-list

Syntax

managed-vlan-list

Context

config>service>vpls>sap

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

Commands in this context configure VLAN ranges managed by a management VPLS. The list indicates, for each SAP, the ranges of associated VLANs that is affected when the SAP changes state.

This command is valid only when the VPLS in which it is entered was created as a management VPLS.

default-sap

Syntax

[**no**] **default-sap**

Context

config>service>vpls>sap>managed-vlan-list

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command adds a default SAP to the managed VLAN list.

The **no** form of this command removes the default SAP from the managed VLAN list.

range

Syntax

[**no**] **range** *vlan-range*

Context

config>service>vpls>sap>managed-vlan-list

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures a range of VLANs on an access port that are to be managed by an existing management VPLS.

This command is valid only when the VPLS in which it is entered was created as a management VPLS, and when the SAP in which it was entered was created on an Ethernet port with encapsulation type of dot1q.

To modify the range of VLANs, first the new range should be entered and then the old range removed. See Modifying VPLS service parameters for more information.

Parameters

vlan-range

Specify the VLAN start value and VLAN end value. The *end-vlan* value must be greater than the *start-vlan* value. The format is *start-vlan-end-vlan*

Values *start-vlan*: 0 to 4094 *end-vlan*: 0 to 4094

5.7.2.1.7 VPLS filter and QoS policy commands

egress

Syntax

egress

Context

config>service>vpls>sap

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

Commands in this context configure egress filter policies.

If **no** egress filter is defined, no filtering is performed.

agg-rate-limit

Syntax

agg-rate-limit [**cir** *cir-rate*] [**pir** *pir-rate*]

no agg-rate-limit

Context

config>service>vpls>sap>egress

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures a maximum total rate for all egress queues on a service SAP.

The port scheduler mode should be set to "sap-based" scheduling mode before using this command. The egress port scheduler enforces the aggregate queue rate for the SAP as it distributes its bandwidth to all the SAPs configured on the port. The port scheduler stops distributing bandwidth to member queues when it has detected that the aggregate rate limit has been reached.

A SAP aggregate scheduler is created for each instance of the SAP queues created on each of the member ports of the LAG. For a LAG, the port scheduler-mode configured for the primary port is used for all the member ports of the LAG.

The scheduler mode is specified using the **scheduler-mode** command. To implement the aggregate-rate-limit, the scheduler mode must be specified as "sap-based". See the *7210 SAS-Mxp, R6, R12, S, Sx, T Interface Configuration Guide* for more information about the **scheduler-mode** command.

The **no** form of this command removes the aggregate rate limit from the SAP or multi-service site.

Parameters

cir-rate

Specifies the CIR in kilobits per second. This parameter is supported only on the 7210 SAS-R6 and 7210 SAS-R12.

Values 0 to 10000000

pir-rate

Specifies the PIR in kilobits per second.

Values 1 to 10000000, max

aggregate-meter-rate

Syntax

aggregate-meter-rate *rate-in-kbps* [**burst** *burst-in-kbits*] [**enable-stats**]

no aggregate-meter-rate

Context

config>service>vpls>sap>egress

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command associates a set of two counters to count total forwarded packets and octets and total dropped packets and octets. When the counter is enabled, the amount of resources required increases by twice the amount of resources taken up when counter is not used. If the **enable-stats** keyword is specified during the creation of the meter, the counter is allocated by the software, if available. To free up the counter and relinquish its use, use the **no aggregate-meter-rate** command, and then recreate the meter using the **aggregate-meter rate** command.

If egress frame-based accounting is used, the SAP egress aggregate meter rate accounts for the Ethernet frame overhead. The system accounts for 12 bytes of IFG and 8 bytes of start delimiter. Frame-based counting does not affect the count of octets maintained by the counter, if in use.

Note:

- Before enabling this command for a SAP, resources must be allocated to this feature from the egress internal TCAM resource pool using the **configure system resource-profile egress-internal-tcam egress-sap-aggregate-meter** command. For more information, see the *7210 SAS-Mxp, R6, R12, S, Sx, T Basic System Configuration Guide*.
- The egress aggregate meter is not FC aware. The forward and drop decisions are made based on the order the packets are sent out of the SAP by the egress port scheduler.

The **no** form of this command removes the egress aggregate policer from use.

Default

no aggregate-meter-rate

Parameters

rate-in-kbps

Specifies the rate in kilobits/s.

Values 1 to 100000000 | max

Default max

burst-in-kbits

Specifies the burst size for the policer in kilobits. The burst size cannot be configured without configuring the rate.

Values 4 to 2146959 | default

Default 512

enable-stats

Keyword to specify whether the counter is to count forwarded and dropped packets must be allocated.

filter

Syntax

filter ip *ip-filter-id*

filter ipv6 *ipv6-filter-id*

filter mac *mac-filter-id*

no filter [**ip ip-filter-id**] [**ipv6 ipv6-filter-id**] [**mac mac-filter-id**]

Context

config>service>vpls>sap>egress

config>service>vpls>sap>ingress

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command associates an IP filter policy or MAC filter policy with an ingress or egress SAP or IP interface.

Filter policies control the forwarding and dropping of packets based on IP or MAC matching criteria. There types of filter policies are IP and MAC. Only one type may be applied to a SAP at a time.

The **filter** command is used to associate a filter policy with a specified filter ID with an ingress or egress SAP. The filter ID must already be defined before the **filter** command is executed. If the filter policy does not exist, the operation fails and an error message is returned.

In general, filters applied to SAPs (ingress or egress) apply to all packets on the SAP. One exception is that 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 is not removed from the system.

Special Cases

VPLS

Both MAC and IP filters are supported on a VPLS service SAP.

Parameters

ip *ip-filter-id*

Specifies the IP filter policy. The filter ID must already exist within the created IP filters.

Values 1 to 65535

ipv6 *ipv6-filter-id*

Specifies the IPv6 filter policy. The filter ID must already exist within the created IPv6 filters.

Values 1 to 65535

mac ***mac-filter-id***

Specifies the MAC filter policy. The specified filter ID must already exist within the created MAC filters. The filter policy must already exist within the created MAC filters.

Values 1 to 65535

qos

Syntax

qos *policy-id*

qos *policy-id* [**enable-table-classification**]

no qos

Context

config>service>vpls>sap>egress config>service>vpls>sap>ingress

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command associates a QoS policy with an ingress SAP or IP interface.

QoS ingress policies are important for the enforcement of SLA agreements. The policy ID must be defined before associating the policy with a SAP. If the *policy-id* does not exist, an error is 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 only allows 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 at one time. Attempts to associate a second policy of same or different type replaces the earlier one with the new policy.

On the 7210 SAS-R6 and 7210 SAS-R12 (ingress), using the **enable-table-classification** keyword enables the use of IP DSCP tables to assign FC and profile on a per-SAP ingress basis. The match-criteria configured in the service ingress policy, which require CAM resources, are ignored. Only meters from the service ingress policy are used (and the meters still require CAM resources). The IP DSCP classification policy configured in the SAP ingress policy is used to assign FC and profile. The default FC is assigned from the SAP ingress policy.

By default, if no specific QoS policy is associated with the SAP for ingress or egress, the default QoS policy is used.

The **no** form of this command removes the QoS policy association from the SAP, and the QoS policy reverts to the default.

Parameters

policy-id

Specifies the ingress or egress policy ID to associate with SAP on ingress or egress. The policy ID must already exist.

Values 1 to 65535

enable-table-classification

Keyword to enable the use of table-based classification instead of CAM-based classification at SAP ingress. The FC and profile are taken from the IP DSCP classification policy configured in the ingress policy, along with the meters from the SAP ingress policy. Match-criteria entries in the SAP ingress policy are ignored.

ingress

Syntax

ingress

Context

config>service>vpls>sap

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

Commands in this context configure ingress SAP 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.

aggregate-meter-rate

Syntax

aggregate-meter-rate *rate-in-kbps* [**burst** *burst-in-kbits*]

no aggregate-meter-rate

Context

config>service>vpls>sap>ingress

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

Note: The sum of CIR of the individual FCs configured under the SAP cannot exceed the PIR rate configured for the SAP. The 7210 SAS software does not block this configuration, however it is not recommended.

The meter modes "srtcm" and "trtcm1" are used in the absence of an aggregate meter.

The SAP ingress meter counters increment the packet or octet counts based on the final disposition of the packet.

If ingress frame-based accounting is used, the SAP aggregate meter rate accounts for the Ethernet frame overhead. The system accounts for 12 bytes of IFG and 8 bytes of start delimiter.

The **no** form of this command removes the aggregate policer from use.

Default

no aggregate-meter-rate

Parameters

rate-in-kbps

Specifies the rate in kilobits per second.

Values 0 to 20000000 | max

Default max

burst burst-in-kilobits

Specifies the burst size for the policer in kilobits. The burst size cannot be configured without configuring the rate.

Values 4 to 2146959

Default 512

The following table provides information about the final disposition of the packet, based on the operating rate of the per-FC policer and the per-SAP aggregate policer:

Table 53: Final disposition of the packet based on per-FC and per-SAP policer or meter

Per-FC meter operating rate	Per-FC assigned color	SAP aggregate meter operating rate	SAP aggregate meter color	Final packet color
Within CIR	Green	Within PIR	Green	Green or In-profile
Within CIR[15]	Green	Above PIR	Red	Green or

[15] This row is not recommended for use. For more information, see the Note in the command description.

Per-FC meter operating rate	Per-FC assigned color	SAP aggregate meter operating rate	SAP aggregate meter color	Final packet color
				In-profile
Above CIR, Within PIR	Yellow	Within PIR	Green	Yellow or Out-of-Profile
Above CIR, Within PIR	Yellow	Above PIR	Red	Red or Dropped
Above PIR	Red	Within PIR	Green	Red or Dropped
Above PIR	Red	Above PIR	Red	Red or Dropped

When the SAP aggregate policer is configured, per-FC policer can be configured only in "trtcm2" mode (RFC 4115).

meter-override

Syntax

[**no**] **meter-override**

Context

config>service>vpls>sap>ingress

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables the context for specific overrides to one or more meters created on the SAP through the SAP ingress QoS policies.

The **no** form of this command removes existing meter overrides.

Default

no meter-override

meter

Syntax

meter *meter-id* [**create**]

no meter *meter-id*

Context

config>service>vpls>sap>ingress>meter-override

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables the context for specific overrides to a specific meter created on the SAP through a sap-ingress QoS policies.

The **no** form of this command is used to remove any existing overrides for the specified meter-id.

Parameters

meter-id

Required when executing the **meter** command within the **meter-overrides** context. The specified *meter-id* must exist within the SAP ingress QoS policy applied to the SAP. If the meter is not currently used by any forwarding class or forwarding type mappings, the meter will not exist on the SAP. This does not preclude creating an override context for the *meter-id*.

create

Mandatory keyword for when a **meter** *meter-id* override node is being created and the system is configured to expect explicit confirmation that a new object is being created. When the system is not configured to expect explicit confirmation, the **create** keyword is not required.

adaptation-rule

Syntax

adaptation-rule [**pir** *adaptation-rule*] [**cir** *adaptation-rule*]

no adaptation-rule

Context

config>service>vpls>sap>ingress>meter-override>meter

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command overrides specific attributes of the specified meter adaptation rule parameters. The adaptation rule controls the method used by the system to derive the operational CIR and PIR settings when the meter is provisioned in hardware. For the CIR and PIR parameters individually, the system attempts to find the best operational rate depending on the defined constraint.

The **no** form of this command removes explicitly defined constraints used to derive the operational CIR and PIR created by the application of the policy. When a specific **adaptation-rule** is removed, the default constraints for **rate** and **cir** apply.

Default

no adaptation-rule

Parameters

pir

Defines the constraints enforced when adapting the PIR rate defined using the **meter-override meter** *meter-id* command. The **pir** parameter requires a qualifier that defines the constraint used when deriving the operational PIR for the queue. When the **meter-override** command is not specified, the default applies.

When the meter mode in use is "trtcm2", this parameter is interpreted as EIR value. See the description and relevant notes for meter modes in the *7210 SAS-Mxp, R6, R12, S, Sx, T Quality of Service Guide* for more information.

cir

Defines the constraints enforced when adapting the CIR rate defined using the **meter-override meter** *meter-id* command. The **cir** parameter requires a qualifier that defines the constraint used when deriving the operational CIR for the queue. When the **cir** parameter is not specified, the default constraint applies.

adaptation-rule

Specifies the criteria to use to compute the operational CIR and PIR values for this meter, while maintaining a minimum offset.

Values **max** — The **max**, **min** and **closest** options are mutually exclusive. When **max** (maximum) is defined, the operational PIR for the meter is equal to or less than the administrative rate specified using the **meter-override** command.

min — The **min**, **max** and **closest** options are mutually exclusive. When **min** (minimum) is defined, the operational PIR for the queue is equal to or greater than the administrative rate specified using the **meter-override** command.

closest — The **closest**, **min** and **max** options are mutually exclusive. When **closest** is defined, the operational PIR for the meter is the rate closest to the rate specified using the **meter-override** command.

cbs

Syntax

cbs *size* [**kbits** | **bytes** | **kbytes**]

no cbs

Context

config>service>vpls>sap>ingress>meter-override>meter

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command overrides the default CBS for the meter. The committed burst size parameter specifies the maximum burst size that can be transmitted by the source while still complying with the CIR. If the transmitted burst is lower than the CBS value then the packets are marked as in-profile by the meter to indicate that the traffic is complying meter configured parameters.

The **no** form of this command reverts the CBS size to the default value.

Default

32 kbits

Parameters

size

Specifies the value in kbits, bytes, or kilobytes.

Values **kbits**: 4 to 2146959 | default **bytes**: 512 to 274810752 | **kbytes**: 1 to 268369

mbs

Syntax

mbs *size* [**kbits** | **bytes** | **kbytes**]

no mbs

Context

config>service>vpls>sap>ingress>meter-override>meter

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command overrides the default MBS for the meter. The maximum burst size parameter specifies the maximum burst size that can be transmitted by the source while still complying with the CIR. If the transmitted burst is lower than the MBS value, the packets are marked as in-profile by the meter to indicate that the traffic is complying with meter configured parameters.

The **no** form of this command reverts the MBS size to the default value.

Default

512 kbits

Parameters

size

Specifies the value in kbits, bytes, or kilobytes.

Values **kbits**: 4 to 2146959 | default **bytes**: 512 to 274810752 | **kbytes**: 1 to 268369

mode

Syntax

mode *mode*

no mode

Context

config>service>vpls>sap>ingress>meter-override>meter

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command overrides the SAP ingress QoS policy configured mode parameters for the specified *meter-id*.

The **no** form of this command restores the policy defined metering and profiling mode to a meter.

Parameters

mode

Specifies the rate mode of the meter-override.

Values trtcm1, trtcm2, srtcm

rate

Syntax

rate cir *cir-rate* [**pir** *pir-rate*]

no rate

Context

config>service>vpls>sap>ingress>meter-override>meter

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command overrides the SAP ingress QoS policy configured rate parameters for the specified *meter-id*.

The **max** default specifies the amount of bandwidth in kilobits per second (thousand bits per second). The **max** value is mutually exclusive to the *pir-rate* value.

The **no** form of this command restores the policy defined metering and profiling rate to a meter.

Default

max

Parameters

pir-rate

Defines the administrative PIR rate, in kilobits, for the queue. When the **rate** command is executed, a valid PIR setting must be explicitly defined. When the **rate** command has not been executed, the default PIR of **max** is assumed. Fractional values are not allowed and must be specified as a positive integer.

When the meter mode is set to "trtcm2", the PIR value is interpreted as the EIR value. For more information, see the *7210 SAS-Mxp, R6, R12, S, Sx, T Quality of Service Guide*.

The actual PIR rate is dependent on the queue **adaptation-rule** parameters and the hardware where the queue is provisioned.

Values 0 to 20000000 | max

Default max

cir-rate

Overrides the default administrative CIR used by the queue. When the **rate** command is executed, a CIR setting is optional. When the **rate** command has not been executed or the **cir** parameter is not explicitly specified, the default CIR (0) is assumed. Fractional values are not allowed and must be specified as a positive integer.

Values 0 to 20000000 | max

Default 0

collect-stats

Syntax

[**no**] **collect-stats**

Context

config>service>vpls>spoke-sdp

config>service>vpls>mesh-sdp

config>service>vpls>sap

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables accounting and statistical data collection for either the SAP, network port, or IP interface. When applying accounting policies, by default the data is collected in the appropriate records and written to the designated billing file.

When the **no collect-stats** command is issued, the statistics are still accumulated by the cards. However, the CPU does not obtain the results and write them to the billing file. If a subsequent **collect-stats** command is issued, the counters written to the billing file include all the traffic while the **no collect-stats** command was in effect.

Default

no collect-stats

5.7.2.1.8 VPLS SDP commands

mesh-sdp

Syntax

mesh-sdp *sdp-id*[**:***vc-id*] [**vc-type** {**ether** | **vlan**}]

no mesh-sdp *sdp-id*[**:***vc-id*]

Context

config>service>vpls

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command binds a VPLS service to an existing SDP. Mesh SDPs bound to a service are logically treated like a single bridge "port" for flooded traffic, where flooded traffic received on any mesh SDP on the service is replicated to other "ports" (spoke SDPs and SAPs) and not transmitted on any mesh SDPs.

This command creates a binding between a service and an SDP. The SDP has an operational state that determines the operational state of the SDP within the service; for example, if the SDP is administratively or operationally down, the SDP for the service is down.

The SDP must already be defined in the **config>service>sdp** context to associate the SDP with a valid service. If the **sdp** *sdp-id* is not already configured, an error message is generated. If the *sdp-id* does exist, a binding between that *sdp-id* and the service is created.

SDPs must be explicitly associated and bound to a service. If an SDP is not bound to a service, no far-end devices can participate in the service.

The **no** form of this command removes the SDP binding from the service. The SDP configuration is not affected, only the binding of the SDP to a service. When removed, no packets are forwarded to the far-end router.

Special Cases

VPLS

Several SDPs can be bound to a VPLS. Each SDP must be destined for a different router. If two *sdp-id* bindings terminate on the same router, an error occurs and the second SDP is binding is rejected.

Parameters

sdp-id

Specifies the SDP identifier.

Values 1 to 17407

vc-id

Specifies the virtual circuit identifier. This value is used to validate the VC ID portion of each mesh SDP binding defined in the service. The default value of this object is equal to the service ID.

Values 1 to 4294967295

vc-type

Keyword that overrides the default VC type signaled for the spoke or mesh binding to the far end of the SDP. The VC type is a 15 bit-quantity containing a value which represents the type of VC. The actual signaling of the VC type depends on the signaling parameter defined for the SDP. If signaling is disabled, the **vc-type** command can still be used to define the dot1q value expected by the far-end provider equipment. A change of the bindings VC type causes the binding to signal the new VC type to the far end when signaling is enabled. VC types are derived according to IETF *draft-martini-l2circuit-trans-mpls*.

- The VC type value for Ethernet is 0x0005.
- The VC type value for an Ethernet VLAN is 0x0004.

ether

Keyword that defines the VC type as Ethernet. The **ethernet** and **vlan** keywords are mutually exclusive. When the VC type is not defined, the default is Ethernet for spoke-SDP bindings. Defining Ethernet is the same as executing **no vc-type**, and restores the default VC type for the spoke-SDP binding. (hex 5)

vlan

Defines the VC type as VLAN. The **ethernet** and **vlan** keywords are mutually exclusive. When the VC type is not defined, the default is Ethernet for mesh SDP bindings.

spoke-sdp

Syntax

spoke-sdp *sdp-id*[**:***vc-id*] [**vc-type** {**ether** | **vlan**}] [**create**] [**split-horizon-group** *group-name*] [**use-evpn-default-shg**]

no spoke-sdp *sdp-id*[**:***vc-id*]

Context

config>service>vpls

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command binds a service to an existing Service Distribution Point (SDP). A spoke-SDP is treated like the equivalent of a traditional bridge "port" where flooded traffic received on the spoke-SDP is replicated on all other "ports" (other spoke and mesh SDPs or SAPs) and not transmitted on the port on which it was received.

The operational state of the SDP determines the SDP state within the service. For example, if the SDP is administratively or operationally down, the SDP for the service is down.

The SDP must already exist in the **config>service>sdp** context before it can be associated with a VPLS service. If the **sdp** *sdp-id* is not already configured, an error message is generated. If the *sdp-id* exists, a binding between the specific *sdp-id* and service is created.

SDPs must be explicitly associated and bound to a service to allow far-end devices to participate in the service.

The **no** form of this command removes the SDP binding from the service; the SDP configuration is not affected. When the SDP binding is removed, no packets are forwarded to the far-end router.

Special Cases

VPLS

Several SDPs can be bound to a VPLS service. Each SDP must use unique *vc-ids*. An error message is generated if two SDP bindings with identical *vc-ids* terminate on the same router. Split horizon groups can be created only in the scope of a VPLS service.

Parameters

sdp-id

Specifies the SDP identifier.

Values 1 to 17407

vc-id

Specifies the virtual circuit identifier.

Values 1 to 4294967295

create

Mandatory keyword while creating a spoke-SDP.

endpoint

Specifies the service endpoint to which this SDP bind is attached. The service ID of the SDP binding must match the service ID of the service endpoint.

no-endpoint

Keyword to remove the association of a spoke-SDP with an explicit endpoint name.

ether

Keyword to define the VC type as Ethernet. The **ether** and **vlan** keywords are mutually exclusive. When the VC type is not defined, the default is Ethernet for spoke-SDP bindings. Defining Ethernet is the same as executing **no vc-type** and restores the default VC type for the spoke-SDP binding. (hex 5)

split-horizon-group *group-name*

Specifies the name of the split horizon group to which the SDP belongs.

vc-type

Keyword that overrides the default VC type signaled for the spoke or mesh binding to the far end of the SDP. The VC type is a 15-bit quantity containing a value that represents the VC type. The actual signaling of the VC type depends on the signaling parameter defined for the SDP. If signaling is disabled, the **vc-type** command can still be used to define the dot1q value expected by the far-end provider equipment. If signaling is enabled, a change of the bindings VC type causes the binding to signal the new VC type to the far end.

VC types are derived in accordance with IETF *draft-martini-l2circuit-trans-mpls*.

- The VC type value for Ethernet is 0x0005.
- The VC type value for an Ethernet VLAN is 0x0004.

Values ether, vlan

vlan

Keyword that defines the VC type as VLAN. The **ether** and **vlan** keywords are mutually exclusive. When the VC type is not defined then the default is Ethernet for spoke-SDP bindings. The VLAN VC-type requires at least one dot1q tag within each encapsulated Ethernet packet transmitted to the far end.

use-evpn-default-shg

Keyword to add the spoke-SDP to the default SHG, which causes the spoke-SDP to behave as a mesh SDP. See Note: for more information.

Note: The following restrictions apply for the **use-evpn-default-shg** keyword:

- This option is not blocked in a VPLS service, but it can be configured only for an EVPN-VPLS service. The default SHG is created when EVPN is enabled in the service, and all EVPN bindings are added to it by default.
- Use this option only when the 7210 SAS-R6 or 7210 SAS-R12 is equipped with an IMM-c card. It is not required when the node is equipped with only an IMM-b card.

control-word

Syntax

[**no**] **control word**

Context

config>service>vpls>mesh-sdp

config>service>vpls>spoke-sdp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables the use of the control word on pseudowire packets in VPLS, and enables the use of the control word individually on each mesh SDP or spoke-SDP. By default, the control word is disabled. When the control word is enabled, all VPLS packets, including the BPDU frames, are encapsulated with the control word when sent over the pseudowire. The T-LDP control plane behavior is the same as in the implementation of control word for VLL services. The configuration for the two directions of the Ethernet pseudowire should match.

The **no** form of this command reverts the mesh SDP or spoke-SDP to the default value.

Default

no control word

egress

Syntax

egress

Context

config>service>vpls>mesh-sdp

config>service>vpls>spoke-sdp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables the egress SDP context.

ingress

Syntax

ingress

Context

config>service>vpls>mesh-sdp

config>service>vpls>spoke-sdp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables the ingress SDP context.

vc-label

Syntax

[**no**] **vc-label** *vc-label*

Context

config>service>vpls>mesh-sdp>egress

config>service>vpls>spoke-sdp>egress

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the egress VC label.

Parameters

vc-label

Specifies a VC egress value that indicates a specific connection.

Values 16 to 1048575

vc-label

Syntax

[**no**] **vc-label** *vc-label*

Context

config>service>vpls>mesh-sdp>ingress

config>service>vpls>spoke-sdp>ingress

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the ingress VC label.

Parameters

vc-label

Specifies a VC ingress value that indicates a specific connection.

Values 2048 to 18431

vlan-vc-tag

Syntax

vlan-vc-tag *vlan-id*

no vlan-vc-tag [*vlan-id*]

Context

config>service>vpls>spoke-sdp

config>service>vpls>mesh-sdp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command specifies an explicit dot1q value used when encapsulating to the SDP far end. When signaling is enabled between the near and far end, the configured dot1q tag can be overridden by a received TLV specifying the dot1q value expected by the far end. This signaled value must be stored as the remote signaled dot1q value for the binding. The provisioned local dot1q tag must be stored as the administrative dot1q value for the binding.

When the dot1q tag is not defined, the default value of zero is stored as the administrative dot1q value. Setting the value to zero is equivalent to not specifying the value.

The **no** form of this command disables the command.

Default

no vlan-vc-tag

Parameters

vlan-id

Specifies a valid VLAN identifier to bind an 802.1Q VLAN tag ID.

Values 0 to 4094

description

Syntax

description *description-string*

no description

Context

config>service>vpls>igmp-snooping>mvr

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

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

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

Parameters

description-string

Specifies the description character string. Allowed values are any string up to 80 characters composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

fast-leave

Syntax

[**no**] **fast-leave**

Context

config>service>vpls>sap>igmp-snooping

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables fast leave. When IGMP fast leave processing is enabled, the system immediately removes a SAP from the multicast group if it detects an IGMP "leave" on that SAP. Fast leave processing allows the switch to remove a SAP that sends a "leave" message from the forwarding table without first sending out group-specific queries to the SAP, and therefore speeds up the process of changing channels (known as "zapping").

Fast leave should be enabled only when there is a single receiver present on the SAP. When fast leave is enabled, the configured **last-member-query-interval** value is ignored.

Default

no fast-leave

from-vpls

Syntax

from-vpls *service-id*

no from-vpls

Context

config>service>vpls>sap>igmp-snooping>mvr

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the VPLS and RVPLS service from which multicast traffic is copied upon receipt of an IGMP join request. IGMP snooping must be enabled on the MVR VPLS and MVR RVPLS service.

Default

no from-vpls

Parameters

service-id

Specifies the MVR VPLS from which multicast channels should be copied into this SAP.

Values *service-id*: 1 to 2147483648

group

Syntax

[**no**] **group** *grp-address*

Context

config>service>vpls>sap>igmp-snooping>static

config>service>vpls>spoke-sdp>snooping>static

config>service>vpls>mesh-sdp>snooping>static

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command adds a static multicast group as a (*, g). When a static IGMP group is added, multicast data for that (*,g) is forwarded to the specific SAP or SDP without receiving a membership report from a host.

Note: Only SAPs are supported in an RVPLS service. SDPs are not supported in an RVPLS service.

Parameters

grp-address

Specifies an IGMP multicast group address that receives data on an interface. The IP address must be unique for each static group.

group-policy

Syntax

group-policy *policy-name*

no group-policy

Context

config>service>vpls>igmp-snooping>mvr

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command identifies a filter policy for multicast groups applied to this VPLS entity. The sources of the multicast traffic must be members of the VPLS.

The **no** form of this command removes the policy association from the VPLS configuration.

Parameters

policy-name

Specifies the group policy name. Allowed values are any string up to 32 characters composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes. Routing policies are configured in the **config>router>policy-options** context. The router policy must be defined before it can be imported.

hash-label

Syntax

hash-label [**signal-capability**]

no hash-label

Context

config>service>vpls>spoke-sdp

config>service>vpls>mesh-sdp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables the use of the hash label on a VLL or VPLS service bound to LDP or RSVP SDP using the autobind mode with the ldp, rsvp-te, or mpls options. When this feature is enabled, the ingress datapath is modified so that the result of the hash on the packet header is communicated to the egress datapath for use as the value of the label field of the hash label. The egress datapath appends the hash label at the bottom of the stack (BoS) and sets the S-bit to one (1).

Note: On 7210 SAS, the hash label is not used on the local node for purpose of ECMP hashing and LAG hashing. It is available for use by LSR nodes through which the traffic flows and that are capable of using the labels for hashing.

Packets generated in CPM and that are forwarded labeled within the context of a service (for example, OAM packets) must also include a hash label at the BoS and set the S-bit accordingly.

The TTL of the hash label is set to a value of 0.

Enable the signaling of the **hash-label** capability under a VLL spoke-sdp, a VPLS spoke-sdp or mesh-sdp interface by adding the **signal-capability** option. In this case, the decision whether to insert the hash label on the user and control plane packets by the local PE is solely determined by the outcome of the signaling process and can override the local PE configuration. The following apply when the **hash-label** option and the **signal-capability** option are enabled on the local PE.

- The 7210 local PE inserts the Flow Label Interface Parameters sub-TLV with T=1 and R=1 in the PW ID FEC element in the label mapping message for that spoke-sdp or mesh-sdp.
- If the remote PE does not send the Flow Label sub-TLV in the PW ID FEC element, or sends a Flow Label sub-TLV in the PW ID FEC element with T=FALSE and R=FALSE, the local node disables the hash label capability. Therefore, the local PE node does not insert a hash label in user and control plane

packets that it forwards on the spoke-sdp or mesh-sdp. It also drops user and control plane packets received from a remote PE if they include a hash label. The latter case may be caused by a remote 7210 PE that does not support the hash-label option, or that has the **hash-label** option enabled but does not support the **signal-capability** option, or does support both options but the user did not enable them.

- If the remote PE sends Flow Label sub-TLV in the PW ID FEC element with T=TRUE and R=TRUE, the local PE enables the hash label capability. Therefore, the local PE inserts a hash label in user and control plane packets that it forwards on the spoke-sdp or mesh-sdp. It also accepts user and control plane packets remote PE with or without a hash label.

If the **hash-label**option was enabled on the local configuration of the spoke-sdp or mesh-sdp at the remote PE, the pseudowire packets received by the local PE will have the hash label included. These packets must be dropped. Solve this by disabling the signaling capability option on the local node, which will result in the insertion of the hash label by both PE nodes.

If the **hash-label** option is not supported or was not enabled on the local configuration of the spoke-sdp or mesh-sdp at the remote PE, the pseudowire received by the local PE will not have the hash label included.

The user can enable or disable the signal-capability option in CLI as needed. When doing so, the router must withdraw the label it sent to its peer and send a new label mapping message with the new value of the F bit in the flow label interface parameters sub-TLV of the PW ID FEC element.

Note:

- This feature is supported only for VLL and VPLS services. It not supported for VPRN services. It is also not supported on multicast packets forwarded using RSVP P2MP LPS or mLDP LSP in both the base router instance and in the multicast VPN (mVPN) instance.
- In 7x50 and possibly other vendor implementations, to allow applications where the egress LER infers the presence of the hash label implicitly from the value of the label, the Most Significant Bit (MSB) of the result of the hash is set before copying into the Hash Label. This means that the value of the hash label always in the range [524,288 to 1,048,575] and does not overlap with the signaled/static LSP and signaled/static service label ranges. This also guarantees that the hash label does not match a value in the reserved label range. This is not supported on 7210 SAS for service traffic (for MPLS OAM traffic the MSB bit is set). That is, 7210 SAS devices do not set the MSB bit in the hash label value for service traffic. Therefore, users must ensure that both ends are correctly configured to process hash labels or disable the feature.

The **no** form of this command disables the use of the hash label.

Default

no hash-label

Parameters

signal-capability

Keyword to enable the signaling and negotiation of the use of the hash label between the local and remote PE nodes.

igmp-snooping

Syntax

igmp-snooping

Context

config>service>vpls

config>service>vpls>sap

config>service>vpls>spoke-sdp

config>service>vpls>mesh-sdp

config>service>pw-template

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables the Internet Group Management Protocol (IGMP) snooping context.

import

Syntax

import *policy-name*

no import

Context

config>service>vpls>sap>igmp-snooping

config>service>vpls>spoke-sdp>igmp-snooping

config> service>vpls> mesh-sdp>igmp-snooping

config>service>pw-template>igmp-snooping

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command specifies the import routing policy for IGMP packets to be used on this SAP or SDP. Only a single policy can be imported on a single SAP or SDP at any time.

The **no** form of this command removes the policy association from the SAP or SDP.

Default

no import

Parameters

policy-name

Specifies the import policy name. Values can be string up to 32 characters composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes. These policies are configured in the **config>router>policy-options** context. The router policy must be defined before it can be imported.

last-member-query-interval

Syntax

last-member-query-interval *tenths-of-seconds*

no last-member-query-interval

Context

config>service>vpls>sap>igmp-snooping

config>service>vpls>spoke-sdp>igmp-snooping

config>service>vpls>mesh-sdp>igmp-snooping

config>service>pw-template>igmp-snooping

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the maximum response time used in group-specific queries sent in response to "leave" messages, and is also the amount of time between 2 consecutive group-specific queries. This value may be tuned to modify the leave latency of the network. A reduced value results in reduced time to detect the loss of the last member of a group. The configured **last-member-query-interval** is ignored when the **fast-leave** command is enabled on the SAP or SDP.

Default

last-member-query-interval 10

Parameters

tenths-of-seconds

Specifies the frequency, in tenths of seconds, at which query messages are sent.

Values 1 to 50

max-num-groups

Syntax

max-num-groups *count*

no max-num-groups

Context

config>service>vpls>sap>igmp-snooping

config>service>vpls>spoke-sdp>igmp-snooping

config>service>vpls>mesh-sdp>igmp-snooping

config>service>pw-template>igmp-snooping

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command defines the maximum number of multicast groups that can be joined on this SAP or SDP. If the node receives an IGMP join message that would exceed the configured number of groups, the request is ignored.

Default

no max-num-groups

Parameters

count

Specifies the maximum number of groups that can be joined on this SAP.

Values **For VPLS** (SAP, mesh SDP, and spoke-SDP):

1 to 1024

For RVPLS:

1 to 1000

max-num-sources

Syntax

max-num-sources *max-num-sources*

no max-num-sources

Context

config>service>vpls>sap>igmp-snooping

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command defines the maximum number of multicast sources allowed per group that can be joined on this SAP. If the node receives an IGMP join message that would exceed the configured number of sources, the request is ignored.

Note: The **max-num-sources** command is applicable only in the context of RVPLS service. It cannot be used in the context of VPLS service.

The **no** form of this command disables checking the number of sources.

Default

no max-num-sources

Parameters

max-num-sources

Specifies the maximum number of multicast sources per group that can be joined on this SAP.

Values 1 to 2043

mrouter-port

Syntax

[**no**] **mrouter-port**

Context

config>service>vpls>sap>igmp-snooping

config>service>vpls>spoke-sdp>igmp-snooping

config>service>vpls>mesh-sdp>igmp-snooping

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command specifies whether a multicast router is attached behind this SAP.

Configuring a SAP or SDP as an mrouter-port has a dual effect. Firstly, all multicast traffic received on another SAP or SDP is copied to this SAP or SDP. Secondly, IGMP reports generated by the system as a result of someone joining or leaving a multicast group are sent to this SAP or SDP.

If two multicast routers exist in the network, one of them becomes the active querier. While the other multicast router (non-querier) stops sending IGMP queries, it should still receive reports to keep its

multicast trees up to date. To support this, the mrouter-port should be enabled on all SAPs or SDPs connecting to a multicast router.

The IGMP version to be used for the reports (v1 or v2) is only determined after an initial query is received. Until the IGMP version is determined, no reports are sent on the SAP or SDP, even if **mrouter-port** is enabled.

If the **send-queries** command is enabled on this SAP or SDP, the **mrouter-port** command cannot be enabled.

Default

no mrouter-port

mvr

Syntax

mvr

Context

config>service>vpls>igmp-snooping

config>service>vpls>sap>igmp-snooping

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

Commands in this context configure Multicast VPLS Registration (MVR) parameters.

query-interval

Syntax

query-interval *seconds*

no query-interval

Context

config>service>vpls>igmp-snooping

config>service>vpls>sap>igmp-snooping

config>service>vpls>spoke-sdp>igmp-snooping

config>service>vpls>mesh-sdp>igmp-snooping config>service>pw-template>igmp-snooping

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the IGMP query interval. If the **send-queries** command is enabled, this parameter specifies the interval between two consecutive general queries sent by the system on this SAP or SDP. The configured **query-interval** must be greater than the configured **query-response-interval**. If **send-queries** is not enabled on this SAP or SDP, the configured **query-interval** value is ignored.

Default

125

Parameters

seconds

Specifies the time interval, in seconds, that the router transmits general host-query messages.

query-src-ip

Syntax

query-src-ip *ip-address*

no query-src-ip

Context

config>service>vpls>igmp-snooping

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the IP source address used in IGMP queries.

query-response-interval

Syntax

query-response-interval *seconds*

Context

config>service>vpls>sap>igmp-snooping

config>service>vpls>spoke-sdp>igmp-snooping

config>service>vpls>mesh-sdp>igmp-snooping config>service>pw-template>igmp-snooping

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the IGMP query response interval. If the **send-queries** command is enabled, this parameter specifies the maximum response time advertised in IGMP queries.

The configured **query-response-interval** must be smaller than the configured **query-interval**.

If **send-queries** is not enabled on this SAP or SDP, the configured **query-response-interval** value is ignored.

Default

query-response-interval 10

Parameters

seconds

Specifies the length of time to wait to receive a response to the host-query message from the host.

Values 1 to 1023

report-src-ip

Syntax

report-src-ip *ip-address*

no report-src-ip

Context

config>service>vpls>igmp-snooping

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command specifies the source IP address used when generating IGMP reports. According the IGMPv3 standard, a zero source address is allowed in sending IGMP reports. However, for interoperability with some multicast routers, the source IP address of IGMP group reports can be configured using this command.

Default

report-src-ip 0.0.0.0

Parameters

ip-address

Specifies the source IP source address in transmitted IGMP reports.

robust-count

Syntax

robust-count *robust-count*

no robust-count

Context

config>service>vpls>igmp-snooping

config>service>vpls>sap>igmp-snooping

config>service>vpls>spoke-sdp>igmp-snooping

config>service>vpls>mesh-sdp>igmp-snooping config>service>pw-template>igmp-snooping

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures tuning for the expected packet loss on a SAP or SDP, and is comparable to a retry count. This command is functional for a SAP or SDP if the **send-queries** command is enabled. If the **send-queries** command is not enabled, the **robust-count** command is ignored. If this SAP or SDP is expected to experience packet loss (called "lossy"), the value of the *robust-count* parameter may be increased. IGMP snooping on this SAP or SDP is robust up to *robust-count* minus 1 packet losses.

Default

robust-count 2

Parameters

robust-count

Specifies the robust count for the SAP or SDP.

Values **config>service>vpls>sap>igmp-snooping**: 2 to 7

config>service>vpls>igmp-snooping: 1 to 255

config>service>vpls>spoke-sdp>igmp-snooping: 2 to 7

config>service>vpls>mesh-sdp>igmp-snooping: 2 to 7

precedence

Syntax

precedence *precedence-value* | **primary**

no precedence

Context

config>service>vpls>spoke-sdp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the spoke-SDP precedence.

Default

precedence 4

Parameters

precedence-value

Specifies the spoke-SDP precedence.

Values 0 to 4

primary

Specifies that the precedence is primary.

propagate-mac-flush

Syntax

[**no**] **propagate-mac-flush**

Context

config>service>vpls

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command specifies whether MAC flush messages received from the specific LDP are propagated to all spoke and mesh SDPs within the context of this VPLS service. The propagation follows the split-horizon principle and any datapath blocking to avoid the looping of these messages.

Default

no propagate-mac-flush

send-queries

Syntax

[**no**] **send-queries**

Context

config>service>vpls>sap>igmp-snooping

config>service>vpls>spoke-sdp>igmp-snooping

config>service>vpls>mesh-sdp>igmp-snooping config>service>pw-template>igmp-snooping

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command specifies whether to send IGMP general query messages on the SAP or SDP.

When the **send-queries** command is configured, all query reports generated locally are of the type belonging to the configured version. If a report of a version higher than the configured version is received, the report is dropped and a new counter to track the wrong version is incremented. If **send-queries** is not configured, the **version** command has no effect. The version used is the version of the querier.

Default

no send-queries

static

Syntax

static

Context

config>service>vpls>sap>igmp-snooping

config>service>vpls>spoke-sdp>igmp-snooping

config>service>vpls>mesh-sdp>igmp-snooping

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

Commands in this context configure static group addresses. Static group addresses can be configured on a SAP or SDP. When present either as a (*, g) entry, multicast packets matching the configuration are forwarded even if no join message was registered for the specific group.

group

Syntax

[**no**] **group grp-address**

Context

config>service>vpls>sap>igmp-snooping>static

config>service>vpls>spoke-sdp>snooping>static

config>service>vpls>mesh-sdp>snooping>static

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command adds a static multicast group either as a (*, g) or as one or more (s,g) records. When a static IGMP group is added, multicast data for that (*,g) or (s,g) is forwarded to the specific SAP or SDP without receiving a membership report from a host.

Parameters

grp-address

Specifies an IGMP multicast group address that receives data on an interface. The IP address must be unique for each static group.

source

Syntax

source *ip-address*

no source *ip-address*

Context

config>service>vpls>sap>igmp-snooping>static>group

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command adds a static (s,g) entry to allow multicast traffic for the corresponding multicast group from the specified source.

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

Note: The **source** command is applicable only in the context of RVPLS service. It cannot be used in the context of VPLS service.

Default

no source

starg

Syntax

[**no**] **starg**

Context

config>service>vpls>sap>igmp-snooping>static>group

config>service>vpls>spoke-sdp>igmp-snooping>static>group

config>service>vpls>mesh-sdp>igmp-snooping>static>group

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command adds a static (*,g) entry to allow multicast traffic for the corresponding multicast group from any source. This command can be enabled only if no existing source addresses for this group are specified.

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

Default

no starg

version

Syntax

version *version*

no version

Context

config>service>vpls>sap>igmp-snooping

config>service>vpls>mesh-sdp>igmp-snooping

config>service>vpls>spoke-sdp>igmp-snooping

config>service>pw-template>igmp-snooping

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command specifies the version of IGMP that is running on this SAP or SDP. This object can be used to configure a router capable of running either value. For IGMP to function correctly, all routers on a LAN must be configured to run the same version of IGMP.

When the **send-query** command is configured, all query types generated locally are of the configured **version**. If a report of a version higher than the configured version is received, the report gets dropped and a new counter is incremented to track the wrong version.

If the **send-query** command is not configured, the **version** command has no effect. The version used on that SAP is the version of the querier.

Parameters

version

Specifies the IGMP version.

Values 1 or 2 (in network mode for VPLS services)

1, 2, 3 (for RVPLS, only in network mode)

to-sap

Syntax

to-sap *sap-id*

no to-sap

Context

config>service>vpls>sap>igmp-snooping>mvr

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the SAP to which the multicast data needs to be copied.

In some scenarios, the multicast traffic should not be copied from the MVR VPLS or MVR RVPLS to the SAP on which the IGMP message was received (standard MVR behavior) but to another SAP.

Default

no to-sap

Parameters

sap-id

Specifies the SAP to which multicast channels should be copied.

5.7.2.2 Routed VPLS commands

allow-ip-int-bind

Syntax

[**no**] **allow-ip-int-bind**

Context

config>service>vpls

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command sets a flag on the VPLS service that allows an IES or VPRN IP interface to attach to the VPLS service to make the VPLS service routable. When the **allow-ip-int-bind** command is not enabled, the VPLS service cannot be attached to an IP interface.

VPLS Configuration Constraints for Enabling the allow-ip-int-bind Command

When attempting to set the **allow-ip-int-bind** VPLS flag, the system first checks whether 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 to set the **allow-ip-int-bind** flag.

- SAP ingress QoS policies applied to the VPLS SAPs cannot have MAC match criteria defined.
- The VPLS service type cannot be I-VPLS, B-VPLS, or M-VPLS, and it cannot be an I-VPLS service bound to a B-VPLS context.

When the VPLS **allow-ip-int-bind** flag is set on a VPLS service, the preceding features cannot be enabled on the VPLS service.

VPLS Service Name Bound to IP Interface without the allow-ip-int-bind Flag Set

In the event 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-bind** 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 fails. After the **allow-ip-int-bind** flag is successfully set on the VPLS service, either the service name on the VPLS service must be removed and reapplied, or the IP interface must be reinitialized using the **shutdown /no shutdown** commands. This causes the system to reattempt the name resolution process between the IP interface and the VPLS service.

The **no** form of this command resets the **allow-ip-int-bind** 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-bind** command fails. When the **allow-ip-int-bind** 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.

5.7.2.3 Show commands

5.7.2.3.1 VPLS show commands

egress-label

Syntax

egress-label *egress-label1* [*egress-label2*]

Context

show>service

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays service information using a range of egress labels.

If only the mandatory *egress-label1* parameter is specified, only services using the specified label are displayed.

If both *egress-label1* and *egress-label2* parameters are specified, the services using the range of labels X where *egress-label1* <= X <= *egress-label2* are displayed.

Use the **show router ldp bindings** command to display dynamic labels.

Parameters

egress-label1

Specifies the starting egress label value for which to display services using the label range. If only *egress-label1* is specified, services only using *egress-label1* are displayed.

Values 0, 2049 to 131071

egress-label2

Specifies the ending egress label value for which to display services using the label range.

Default *egress-label1* value

Values 2049 to 131071

fdb-info

Syntax

fdb-info

Context

show>service

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays global FDB usage information.

Output

The following output is an example of FDB information, and Table 54: Output fields: FDB info describes the output fields.

Sample output

```
A:7210-SAS# show service fdb-info
===============================================================================
Forwarding Database(FDB) Information
===============================================================================
Service Id        : 1                   Mac Move          : Disabled
Mac Move Rate     : 2                   Mac Move Timeout  : 10
Table Size        : 8191                Total Count       : 675
Learned Count     : 675                 Static Count      : 0
Local Age         : 60
High WaterMark    : 5%                  Low Watermark     : 1%
Mac Learning      : Enabl               Discard Unknown   : Dsabl
Mac Aging         : Enabl               Relearn Only      : False

Service Id        : 2                   Mac Move          : Disabled
Mac Move Rate     : 2                   Mac Move Timeout  : 10
Table Size        : 8191                Total Count       : 0
Learned Count     : 0                   Static Count      : 0
Local Age         : 80
High WaterMark    : 10%                 Low Watermark     : 2%
Mac Learning      : Enabl               Discard Unknown   : Dsabl
Mac Aging         : Enabl               Relearn Only      : False

Service Id        : 3                   Mac Move          : Disabled
Mac Move Rate     : 2                   Mac Move Timeout  : 10
Table Size        : 8191                Total Count       : 675
Learned Count     : 675                 Static Count      : 0
Local Age         : 100
High WaterMark    : 15%                 Low Watermark     : 3%
Mac Learning      : Enabl               Discard Unknown   : Dsabl
Mac Aging         : Enabl               Relearn Only      : False

Service Id        : 4                   Mac Move          : Disabled
Mac Move Rate     : 2                   Mac Move Timeout  : 10
Table Size        : 8191                Total Count       : 0
Learned Count     : 0                   Static Count      : 0
Local Age         : 120
High WaterMark    : 20%                 Low Watermark     : 4%
Mac Learning      : Enabl               Discard Unknown   : Dsabl
Mac Aging         : Enabl               Relearn Only      : False

Service Id        : 5                   Mac Move          : Disabled
Mac Move Rate     : 2                   Mac Move Timeout  : 10
Table Size        : 8191                Total Count       : 0
Learned Count     : 0                   Static Count      : 0
```

```
Local Age          : 600
High WaterMark     : 25%                Low Watermark     : 5%
Mac Learning       : Enabl              Discard Unknown   : Dsabl
Mac Aging          : Enabl              Relearn Only      : False

Service Id         : 6                  Mac Move          : Disabled
Mac Move Rate      : 2                  Mac Move Timeout  : 10
Table Size         : 8191               Total Count       : 675
Learned Count      : 675                Static Count      : 0
Local Age          : 86400
High WaterMark     : 30%                Low Watermark     : 10%
Mac Learning       : Enabl              Discard Unknown   : Dsabl
Mac Aging          : Enabl              Relearn Only      : False
-------------------------------------------------------------------------------
Total Service FDBs : 6
Total FDB Configured Size : 49146
Total FDB Entries In Use  : 2025
-------------------------------------------------------------------------------
===============================================================================
A:7210-SAS#
```

Table 54: Output fields: FDB info

Label	Description
Service ID	The value that identifies a service.
Mac Move	Indicates the administrative state of the MAC movement feature associated with the service.
Mac Move Rate	The maximum rate at which MACs can be relearned in this TLS service, before the SAP where the moving MAC was last seen is automatically disabled to protect the system against undetected loops or duplicate MACs. The rate is computed as the maximum number of relearns allowed in a 5 second interval. The default rate of 10 relearns per second corresponds to 50 relearns in a 5 second period.
Mac Move Timeout	Indicates the time in seconds to wait before a SAP that has been disabled after exceeding the maximum relearn rate is re-enabled. A value of zero indicates that the SAP is not automatically re-enabled after being disabled. If after the SAP is re-enabled it is disabled again, the effective retry timeout is doubled to avoid thrashing.
Table Size	The maximum number of learned and static entries allowed in the FDB.
Total Count	The current number of entries (both learned and static) in the FDB of this service.
Learned Count	The current number of learned entries in the FDB of this service.
Static Count	The current number of static entries in the FDB of this service.

Label	Description
Remote Age	The number of seconds used to age out FDB entries learned on an SDP. These entries correspond to MAC addresses learned on remote SAPs.
Local Age	The seconds used to age out FDB entries learned on local SAPs.
High WaterMark	The utilization of the FDB table of this service at which a "table full" alarm is raised by the agent.
Low WaterMark	The utilization of the FDB table of this service at which a "table full" alarm is cleared by the agent.
Mac Learning	Specifies whether the MAC learning process is enabled in this service.
Discard Unknown	Specifies whether frames received with an unknown destination MAC are discarded in this service.
MAC Aging	Specifies whether the MAC aging process is enabled in this service.
MAC Pinning	Specifies whether MAC pinning is enabled in this service.
Relearn Only	When enabled, indicates that either the FDB table of this service is full or that the maximum system-wide number of MACs supported by the agent has been reached; therefore MAC learning is temporary disabled, and only MAC relearns can take place.
Total Service FDB	The current number of service FDBs configured on this node.
Total FDB Configured Size	The sum of configured FDBs.
Total FDB Entries In Use	The total number of entries (both learned and static) in use.

fdb-mac

Syntax

fdb-mac *ieee-address* [**expiry**]

Context

show>service

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays the FDB entry for a specific MAC address.

Parameters

ieee-address

Specifies the 48-bit MAC address for which to display the FDB entry in the form *aa*:*bb*:*cc*:*dd*:*ee*:*ff* or *aa-bb-cc-dd-ee-ff* where *aa*, *bb*, *cc*, *dd*, *ee* and *ff* are hexadecimal numbers.

expiry

Keyword that displays the time until the MAC is aged out.

Output

The following output is an example of MAC address FDB entry information, and Table 55: Output fields: FDB MAC describes the output fields.

Sample output

```
*A:ALA-12# show service fdb-mac 00:99:00:00:00:00
===============================================================================
Services Using Forwarding Database Mac 00:99:00:00:00:00
===============================================================================
ServId  MAC                       Source-Identifier         Type/
Age Last Change
-------------------------------------------------------------------------------
1       00:99:00:00:00:00         sap:1/2/7:0               Static
===============================================================================
*A:ALA-12#
```

Table 55: Output fields: FDB MAC

Label	Description
Service ID	The service ID number.
MAC	The specified MAC address.
Source-Identifier	The location where the MAC is defined.
Type/Age	Static — FDB entries created by management.
	Learned — Dynamic entries created by the learning process
	OAM — Entries created by the OAM process.
	H — Host, the entry added by the system for a static configured subscriber host.
	D or DHCP — DHCP-installed MAC. Learned addresses can be temporarily frozen by the DHCP snooping application for the duration of a DHCP lease
	P — Indicates the MAC is protected by the MAC protection feature.

ingress-label

Syntax

ingress-label *start-label* [*end-label*]

Context

show>service

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays services using a range of ingress labels.

If only the mandatory *start-label* parameter is specified, only services using the specified label are displayed.

If both *start-label* and *end-label* parameters are specified, the services using the range of labels X where *start-label* <= X <= *end-label* are displayed.

Use the **show router ldp bindings** command to display dynamic labels.

Parameters

start-label

Specifies the starting ingress label value for which to display services using the label range. If only *start-label* is specified, services only using *start-label* are displayed.

Values 0, 2048 to 131071

end-label

Specifies the ending ingress label value for which to display services using the label range.

Default *start-label* value

Values 2049 to 131071

Output

The following table describes the show service ingress-label output fields.

Sample output

Table 56: Output fields: service ingress label

Label	Description
Svc ID	The service identifier.
SDP Id	The SDP identifier.

Label	Description
Type	Indicates whether the SDP is spoke.
I.Lbl	The ingress label used by the far-end device to send packets to this device in this service by the SDP.
E.Lbl	The egress label used by this device to send packets to the far-end device in this service by the SDP.
Number of Bindings Found	The number of SDP bindings within the label range specified.

sap-using

Syntax

sap-using interface [*ip-address* | *ip-int-name*]

sap-using [**ingress** | **egress**] **filter** *filter-id*

sap-using [**sap** *sap-id*]

sap-using [**ingress**] **qos-policy** *qos-policy-id*

Context

show>service

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays SAP information.

If no optional parameters are specified, the command displays a summary of all defined SAPs.

The optional parameters restrict output to only SAPs matching the specified properties.

Parameters

ingress

Specifies matching an ingress policy.

egress

Specifies matching an egress policy.

filter *filter-id*

Specifies the ingress or egress filter policy ID for which to display matching SAPs.

Values 1 to 65535

sap-id

Specifies the physical port identifier portion of the SAP definition. See Common CLI command descriptions for command syntax.

Output

The following output is an example of SAP service information, and Table 57: Output fields: service SAP-using describes the output fields.

Sample output

```
*A:ALU_SIM2>config>service>vpls# show service sap-using
===============================================================================
Service Access Points
===============================================================================
PortId                          SvcId      Ing.  Ing.    Egr.   Adm  Opr
                                           QoS   Fltr    Fltr
-------------------------------------------------------------------------------
1/1/1:10                        1          1     none    1none   Up   Up
1/1/3:500.*                     1          1     none    1none   Up   Up
1/1/1:200                       200        1     none    1none   Up   Up
1/1/3:100.200                   200        1     none    1none   Up   Up
1/1/1:300                       300        1     none    1none   Up   Up
-------------------------------------------------------------------------------
Number of SAPs : 5
-------------------------------------------------------------------------------
*A:ALU_SIM2>config>service>vpls#

*A:DUT-B_sasx>show>service# sap-using

===============================================================================
Service Access Points
===============================================================================
PortId                          SvcId      Ing.  Ing.    Egr.  Egr.   Adm  Opr
                                           QoS   Fltr    QoS   Fltr
-------------------------------------------------------------------------------
1/1/3:1                         1          10    none    1     none   Up   Up
1/1/3:2                         2          1     none    1     none   Up   Up
1/1/3:3                         3          1     none    1     none   Up   Up
1/1/3:4                         4          1     none    1     none   Up   Up
1/1/3:5                         5          1     none    1     none   Up   Up
1/1/3:6                         6          1     none    1     none   Up   Up
1/1/3:7                         7          1     none    1     none   Up   Up
1/1/3:8                         8          1     none    1     none   Up   Up
1/1/3:9                         9          1     none    1     none   Up   Up
1/1/3:10                        10         1     none    1     none   Up   Up
1/1/3:11                        11         1     none    1     none   Up   Up
1/1/3:12                        12         1     none    1     none   Up   Up
1/1/3:13                        13         1     none    1     none   Up   Up
1/1/3:14                        14         1     none    1     none   Up   Up
1/1/3:15                        15         1     none    1     none   Up   Up
1/1/3:16                        16         1     none    1     none   Up   Up
1/1/3:17                        17         1     none    1     none   Up   Up
1/1/3:18                        18         1     none    1     none   Up   Up
1/1/3:19                        19         1     none    1     none   Up   Up
1/1/3:20                        20         1     none    1     none   Up   Up
1/1/3:21                        21         1     none    1     none   Up   Up
1/1/3:22                        22         1     none    1     none   Up   Up
1/1/3:23                        23         1     none    1     none   Up   Up
1/1/3:24                        24         1     none    1     none   Up   Up
1/1/3:25                        25         1     none    1     none   Up   Up
1/1/3:26                        26         1     none    1     none   Up   Up
1/1/3:27                        27         1     none    1     none   Up   Up
```

```
1/1/3:28                        28          1     none    1     none    Up   Up
1/1/3:29                        29          1     none    1     none    Up   Up
1/1/3:30                        30          1     none    1     none    Up   Up
1/1/3:31                        31          1     none    1     none    Up   Up
1/1/3:32                        32          1     none    1     none    Up   Up
1/1/3:33                        33          1     none    1     none    Up   Up
1/1/3:34                        34          1     none    1     none    Up   Up
1/1/3:35                        35          1     none    1     none    Up   Up
1/1/3:36                        36          1     none    1     none    Up   Up
1/1/3:37                        37          1     none    1     none    Up   Up
1/1/3:38                        38          1     none    1     none    Up   Up
1/1/3:39                        39          1     none    1     none    Up   Up
1/1/3:40                        40          1     none    1     none    Up   Up
1/1/3:41                        41          1     none    1     none    Up   Up
1/1/3:42                        42          1     none    1     none    Up   Up
1/1/3:43                        43          1     none    1     none    Up   Up
1/1/3:44                        44          1     none    1     none    Up   Up
1/1/3:45                        45          1     none    1     none    Up   Up
1/1/3:46                        46          1     none    1     none    Up   Up
1/1/3:47                        47          1     none    1     none    Up   Up
1/1/3:48                        48          1     none    1     none    Up   Up
1/1/3:49                        49          1     none    1     none    Up   Up
1/1/3:50                        50          1     none    1     none    Up   Up
1/1/3:51                        51          1     none    1     none    Up   Up
1/1/3:52                        52          1     none    1     none    Up   Up
1/1/3:53                        53          1     none    1     none    Up   Up
1/1/3:54                        54          1     none    1     none    Up   Up
1/1/3:55                        55          1     none    1     none    Up   Up
1/1/3:56                        56          1     none    1     none    Up   Up
1/1/3:57                        57          1     none    1     none    Up   Up
1/1/3:58                        58          1     none    1     none    Up   Up
1/1/3:59                        59          1     none    1     none    Up   Up
1/1/3:60                        60          1     none    1     none    Up   Up
1/1/3:61                        61          1     none    1     none    Up   Up
1/1/3:62                        62          1     none    1     none    Up   Up
1/1/3:63                        63          1     none    1     none    Up   Up
1/1/3:64                        257         1     none    1     none    Up   Up
-------------------------------------------------------------------------------
Number of SAPs : 64
-------------------------------------------------------------------------------
===============================================================================
```

Table 57: Output fields: service SAP-using

Label	Description
Port ID	The ID of the access port where the SAP is defined.
Svc ID	The service identifier.
I.QoS	The SAP ingress QoS policy number specified on the ingress SAP.
I.MAC/IP	The MAC or IP filter policy ID applied to the ingress SAP.
Egr. Fltr	The filter policy ID applied to the egress SAP.
A.Pol	The accounting policy ID assigned to the SAP.
Adm	The administrative state of the SAP.

Label	Description
Opr	The actual state of the SAP.

sdp

Syntax

sdp [*sdp-id* | **far-end** *ip-addr*] [**detail** | **keep-alive-history**]

Context

show>service>id

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays information for the SDPs associated with the service.

If no optional parameters are specified, a summary of all associated SDPs is displayed.

Parameters

sdp-id

Displays only information for the specified SDP ID. An SDP is a logical mechanism that ties a far-end 7210 SAS to a particular service without having to specifically define far end SAPs. Each SDP represents a method to reach a 7210 SAS router.

Default All SDPs.

Values 1 to 17407

far-end *ip-addr*

Displays only SDPs matching with the specified system IP address of the far-end destination 7210 SAS router for the Service Distribution Point (SDP) that is the termination point for a service.

Default SDPs with any far-end IP address.

detail

Displays detailed SDP information.

Output

The following table describes the show service SDP output fields.

Sample output

Table 58: Output fields: service SDP

Label	Description
Sdp Id	The SDP identifier.
Type	Indicates whether the SDP is a spoke.
VC Type	Displays the VC type: ether or vlan.
VC Tag	Displays the explicit dot1Q value used when encapsulating to the SDP far end.
I. Lbl	The VC label used by the far-end device to send packets to this device in this service by the SDP.
Admin Path MTU	The operating path MTU of the SDP is equal to the admin path MTU (when one is set) or the dynamically computed tunnel MTU, when no admin path MTU is set (the default case.)
Oper Path MTU	The actual largest service frame size (in octets) that can be transmitted through this SDP to the far-end router, without requiring the packet to be fragmented.
Far End	Specifies the IP address of the remote end of the MPLS tunnel defined by this SDP.
Delivery	Specifies the type of delivery used by the SDP: MPLS.
Admin State	The administrative state of this SDP.
Oper State	The operational state of this SDP.
Ingress Label	The label used by the far-end device to send packets to this device in this service by this SDP.
Egress Label	The label used by this device to send packets to the far-end device in this service by the SDP.
Last Changed	The date and time of the most recent change to the SDP.
Signaling	Specifies the signaling protocol used to obtain the ingress and egress labels used in frames transmitted and received on this SDP.
Admin State	The administrative state of the keepalive process.
Oper State	The operational state of the keepalive process.
Hello Time	Specifies how often the SDP echo request messages are transmitted on this SDP.

Label	Description
Max Drop Count	Specifies the maximum number of consecutive SDP echo request messages that can be unacknowledged before the keepalive protocol reports a fault.
Hello Msg Len	Specifies the length of the SDP echo request messages transmitted on this SDP.
Hold Down Time	Specifies the amount of time to wait before the keepalive operating status is eligible to enter the alive state.
I. Fwd. Pkts.	Specifies the number of forwarded ingress packets.
I. Dro. Pkts	Specifies the number of dropped ingress packets.
E. Fwd. Pkts.	Specifies the number of forwarded egress packets.
E. Fwd. Octets	Specifies the number of forwarded egress octets.
Associated LSP List	When the SDP type is MPLS, a list of LSPs used to reach the far-end router displays. All the LSPs in the list must terminate at the IP address specified in the Far End field.

sdp-using

Syntax

sdp-using [*sdp-id*[**:***vc-id*] | **far-end** *ip-address*]

Context

show>service

Platforms

Supported on all 7210 SAS platforms as described in this document

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 to 17407

vc-id

Specifies the virtual circuit identifier.

Values 1 to 4294967295

far-end *ip-address*

Displays only services matching with the specified far-end IP address.

Default Services with any far-end IP address.

Output

The following output is an example of SDP service information, and Table 59: Output fields: SDP-using describes the output fields.

Sample output

```
*A:ALA-1# show service sdp-using 300
===============================================================================
Service Destination Point (Sdp Id : 300)
===============================================================================
SvcId       SdpId               Type Far End        Opr State I.Label  E.Label
-------------------------------------------------------------------------------
2           300:2               Spok 10.0.0.13      Up        131070   131070
-------------------------------------------------------------------------------
Number of SDPs : 51
-------------------------------------------------------------------------------
*A:ALA-1#
```

Table 59: Output fields: SDP-using

Label	Description
Svc ID	The service identifier.
Sdp ID	The SDP identifier.
Type	Specifies the type of SDP: Spoke.
Far End	The far-end address of the SDP.
Oper State	The operational state of the service.
Ingress Label	The label used by the far-end device to send packets to this device in this service by this SDP.
Egress Label	The label used by this device to send packets to the far-end device in this service by this SDP.

service-using

Syntax

service-using [**epipe**] [**vpls**] [**mirror**] [**customer** *customer-id*]

Context

show>service

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays services matching the specified usage properties. If no optional parameters are specified, all services defined on the system are displayed.

Parameters

epipe

Keyword to display matching Epipe services.

vpls

Keyword to display matching VPLS instances.

mirror

Keyword to display matching mirror services.

customer *customer-id*

Specifies to display services only associated with the specified customer ID.

Default Services associated with a customer.

Values 1 to 2147483647

Output

The following output is an example of service information, and Table 60: Output fields: service-using describes the output fields.

Sample output

```
*A:ALA-12# show service service-using customer 10
===============================================================================
Services
===============================================================================
ServiceId    Type      Adm    Opr        CustomerId        Last Mgmt Change
-------------------------------------------------------------------------------
1            VPLS      Up     Up         10                09/05/2006 13:24:15
100          IES       Up     Up         10                09/05/2006 13:24:15
300          Epipe     Up     Up         10                09/05/2006 13:24:15
-------------------------------------------------------------------------------
Matching Services : 3
===============================================================================
*A:ALA-12#


*A:ALA-12# show service service-using epipe
===============================================================================
Services [epipe]
===============================================================================
ServiceId    Type      Adm    Opr        CustomerId        Last Mgmt Change
-------------------------------------------------------------------------------
6            Epipe     Up     Up         6                 09/22/2006 23:05:58
7            Epipe     Up     Up         6                 09/22/2006 23:05:58
8            Epipe     Up     Up         3                 09/22/2006 23:05:58
103          Epipe     Up     Up         6                 09/22/2006 23:05:58
-------------------------------------------------------------------------------
```

```
Matching Services : 4
===============================================================================
*A:ALA-12#


*A:ALA-14# show service service-using
===============================================================================
Services
===============================================================================
ServiceId    Type      Adm    Opr        CustomerId        Last Mgmt Change
-------------------------------------------------------------------------------
10           mVPLS     Down   Down       1                 10/26/2006 15:44:57
11           mVPLS     Down   Down       1                 10/26/2006 15:44:57
100          mVPLS     Up     Up         1                 10/26/2006 15:44:57
101          mVPLS     Up     Up         1                 10/26/2006 15:44:57
102          mVPLS     Up     Up         1                 10/26/2006 15:44:57
-------------------------------------------------------------------------------
Matching Services : 5
-------------------------------------------------------------------------------
*A:ALA-14#



A:Dut-A>config>service# show service service-using
===============================================================================
Services
===============================================================================
ServiceId    Type      Adm    Opr        CustomerId        Last Mgmt Change
-------------------------------------------------------------------------------
100          mVPLS     Up     Up         1                 07/07/2009 14:39:13
101          uVPLS     Up     Up         1                 07/07/2009 14:39:13
102          uVPLS     Up     Up         1                 07/07/2009 14:39:13
103          uVPLS     Up     Up         1                 07/07/2009 14:39:13
104          uVPLS     Up     Up         1                 07/07/2009 14:39:13
105          uVPLS     Up     Up         1                 07/07/2009 14:39:13
201          VPLS      Up     Up         1                 07/07/2009 14:39:13
202          VPLS      Up     Up         1                 07/07/2009 14:39:13
203          VPLS      Up     Up         1                 07/07/2009 14:39:13
204          VPLS      Up     Up         1                 07/07/2009 14:39:13
205          VPLS      Up     Up         1                 07/07/2009 14:39:13
300          mVPLS     Up     Up         1                 07/07/2009 14:39:13
301          uVPLS     Up     Up         1                 07/07/2009 14:39:13
302          uVPLS     Up     Up         1                 07/07/2009 14:39:13
303          uVPLS     Up     Up         1                 07/07/2009 14:39:13
304          uVPLS     Up     Up         1                 07/07/2009 14:39:1
305          uVPLS     Up     Up         1                 07/07/2009 14:39:1
401          VPLS      Up     Up         1                 07/07/2009 14:39:1
402          VPLS      Up     Up         1                 07/07/2009 14:39:1
403          VPLS      Up     Up         1                 07/07/2009 14:39:1
404          VPLS      Up     Up         1                 07/07/2009 14:39:1
405          VPLS      Up     Up         1                 07/07/2009 14:39:1
500          mVPLS     Up     Up         1                 07/07/2009 14:39:1
511          uVPLS     Up     Up         1                 07/07/2009 14:39:1
513          uVPLS     Up     Up         1                 07/07/2009 14:39:1
515          uVPLS     Up     Up         1                 07/07/2009 14:39:1
517          uVPLS     Up     Up         1                 07/07/2009 14:39:1
519          uVPLS     Up     Up         1                 07/07/2009 14:39:1
601          VPLS      Up     Up         1                 07/07/2009 14:39:1
602          VPLS      Up     Up         1                 07/07/2009 14:39:1
603          VPLS      Up     Up         1                 07/07/2009 14:39:1
604          VPLS      Up     Up         1                 07/07/2009 14:39:1
605          VPLS      Up     Up         1                 07/07/2009 14:39:1
701          VPLS      Up     Up         1                 07/07/2009 14:39:1
702          VPLS      Up     Up         1                 07/07/2009 14:39:1
```

```
703          VPLS      Up     Up         1                  07/07/2009 14:39:1
704          VPLS      Up     Up         1                  07/07/2009 14:39:1
801          VPLS      Up     Up         1                  07/07/2009 14:39:1
802          VPLS      Up     Up         1                  07/07/2009 14:39:1
803          VPLS      Up     Up         1                  07/07/2009 14:39:1
804          VPLS      Up     Up         1                  07/07/2009 14:39:1
805          VPLS      Up     Up         1                  07/07/2009 14:39:1
901          VPLS      Up     Up         1                  07/07/2009 14:39:1
902          VPLS      Up     Up         1                  07/07/2009 14:39:1
903          VPLS      Up     Up         1                  07/07/2009 14:39:1
904          VPLS      Up     Up         1                  07/07/2009 14:39:1
905          VPLS      Up     Up         1                  07/07/2009 14:39:1
906          VPLS      Up     Up         1                  07/07/2009 14:39:1
907          VPLS      Up     Up         1                  07/07/2009 14:39:1
908          VPLS      Up     Up         1                  07/07/2009 14:39:1
909          VPLS      Up     Up         1                  07/07/2009 14:39:1
910          VPLS      Up     Up         1                  07/07/2009 14:39:1
1101         Epipe     Up     Up         1                  07/07/2009 14:39:1
1102         Epipe     Up     Up         1                  07/07/2009 14:39:1
1103         Epipe     Up     Up         1                  07/07/2009 14:39:1
1104         Epipe     Up     Up         1                  07/07/2009 14:39:1
1105         Epipe     Up     Up         1                  07/07/2009 14:39:1
1501         Epipe     Up     Up         1                  07/07/2009 14:39:1
1502         Epipe     Up     Up         1                  07/07/2009 14:39:1
1503         Epipe     Up     Up         1                  07/07/2009 14:39:1
1504         Epipe     Up     Up         1                  07/07/2009 14:39:1
1505         Epipe     Up     Up         1                  07/07/2009 14:39:1
2001         Mirror    Up     Up         1                  07/07/2009 14:39:1
2002         Mirror    Up     Up         1                  07/07/2009 14:39:1
2011         Epipe     Up     Up         1                  07/07/2009 14:39:1
2012         VPLS      Up     Up         1                  07/07/2009 14:39:1
3000         mVPLS     Up     Up         1                  07/07/2009 14:39:1
4001         VPLS      Up     Up         1                  07/07/2009 14:39:1
4002         VPLS      Up     Up         1                  07/07/2009 14:39:1
-------------------------------------------------------------------------------
Matching Services : 69
===============================================================================
A:Dut-A>config>service#
```

Table 60: Output fields: service-using

Label	Description
Service Id	The service identifier.
Type	Specifies the service type configured for the service ID.
Adm	The administrative state of the service.
Opr	The operating state of the service.
CustomerID	The ID of the customer who owns this service.
Last Mgmt Change	The date and time of the most recent management-initiated change to this service.

id

Syntax

id *service-id* {**all** | **arp** | **base** | **endpoint** | **fdb** | **interface** | **label** | **labels** | **sap** | **splithorizon-group** | **stp** |**mstp-configuration**}

Context

show>service

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays information for a particular service ID.

Parameters

service-id

Specifies the unique service identification number that identifies the service in the service domain.

Values service-id: 1 to 214748364

svc-name: A string up to 64 characters.

all

Keyword to display detailed information about the service.

base

Keyword to display basic service information.

endpoint

Keyword to display service endpoint information.

fdb

Keyword to display FDB entries.

labels

Keyword to display labels being used by this service.

mstp-configuration

Keyword to display MSTP information.

sap

Keyword to display SAPs associated with the service.

sdp

Keyword to display SDPs associated with the service.

stp

Keyword to display STP information.

all

Syntax

all

Context

show>service>id

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays detailed information for all aspects of the service.

Output

The following output is an example of detailed service information, and Table 61: Output fields: service ID All describes the output fields.

Sample output

```
show service id 100 all
===============================================================================
Service Detailed Information
===============================================================================
Service Id        : 100                Vpn Id            : 0
Service Type      : Epipe
Name              : (Not Specified)
Description       : (Not Specified)
Customer Id       : 1                  Creation Origin   : manual
Last Status Change: 12/14/2019 11:35:20
Last Mgmt Change  : 12/14/2019 13:09:09
Test Service      : No
Admin State       : Down               Oper State        : Down
MTU               : 1514
MTU Check         : Enabled
Vc Switching      : False
SAP Count         : 1                  SDP Bind Count    : 1
SAP Type:         : Qinq Inner Tag Pre*
Propagate MacFlush: Disabled           Per Svc Hashing   : Disabled
Allow IP Intf Bind: Disabled           Fwd-IPv4-Mcast-To*: Disabled
VSD Domain        : <none>
Per Svc Hashing   : Disabled
Force QTag Fwd    : Disabled

-------------------------------------------------------------------------------
BGP Information
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
ETH-CFM service specifics
-------------------------------------------------------------------------------
Tunnel Faults     : ignore
-------------------------------------------------------------------------------
Service Destination Points(SDPs)
-------------------------------------------------------------------------------
```

```
-------------------------------------------------------------------------------
Sdp Id 102:100  -(10.10.10.2)
-------------------------------------------------------------------------------
Description     : (Not Specified)
SDP Id            : 102:100                 Type              : Spoke
Spoke Descr     : (Not Specified)
VC Type           : VLAN                    VC Tag            : 2
Admin Path MTU    : 0                       Oper Path MTU     : 1578
Delivery          : MPLS
Far End           : 10.10.10.2
Tunnel Far End    : n/a                     LSP Types         : RSVP
Hash Label        : Disabled                Hash Lbl Sig Cap  : Disabled
Oper Hash Label   : Disabled

Admin State       : Up                      Oper State        : Down
Acct. Pol         : None                    Collect Stats     : Disabled
Ingress Label     : 131065                  Egress Label      : None
Ingr Mac Fltr-Id  : n/a                     Egr Mac Fltr-Id   : n/a
Ingr IP Fltr-Id   : n/a                     Egr IP Fltr-Id    : n/a
Ingr IPv6 Fltr-Id : n/a                     Egr IPv6 Fltr-Id  : n/a
Admin ControlWord : Not Preferred           Oper ControlWord  : False
Admin BW(Kbps)    : 0                       Oper BW(Kbps)     : 0
BFD Template      : None
BFD-Enabled       : no                      BFD-Encap         : ipv4
Last Status Change : 12/14/2019 11:35:20    Signaling         : TLDP
Last Mgmt Change  : 12/14/2019 13:09:09
Endpoint          : N/A                     Precedence        : 4
PW Status Sig     : Enabled
Force Vlan-Vc     : Disabled                Force Qinq-Vc     : Disabled
Class Fwding State : Down
Flags             : SvcAdminDown
                    NoEgrVCLabel
Local Pw Bits     : lacIngressFault lacEgressFault psnEgressFault
Peer Pw Bits      : None
Peer Fault Ip     : None
Peer Vccv CV Bits : None
Peer Vccv CC Bits : None
Application Profile: None
Standby Sig Slave : False
Block On Peer Fault: False
Use SDP B-MAC     : False

KeepAlive Information :
Admin State       : Disabled                Oper State        : Disabled
Hello Time        : 10                      Hello Msg Len     : 0
Max Drop Count    : 3                       Hold Down Time    : 10
Statistics          :
I. Fwd. Pkts.     : 0                       I. Fwd. Octs.     : 0
E. Fwd. Pkts.     : 0                       E. Fwd. Octets    : 0
Extra-Tag-Drop-Pkts: n/a                    Extra-Tag-Drop-Oc*: n/a
-------------------------------------------------------------------------------
Control Channel Status
-------------------------------------------------------------------------------
PW Status         : disabled                Refresh Timer     : <none>
Peer Status Expire : false
Request Timer     : <none>
Acknowledgement   : false
-------------------------------------------------------------------------------
ETH-CFM SDP-Bind specifics
-------------------------------------------------------------------------------
Squelch Levels    : None

-------------------------------------------------------------------------------
RSVP/Static LSPs
```

```
-------------------------------------------------------------------------------
Associated LSP List :
Lsp Name           : a_b
Admin State        : Up                       Oper State        : Up
Time Since Last Tr*: 00h00m13s

-------------------------------------------------------------------------------
Number of SDPs : 1
-------------------------------------------------------------------------------
* indicates that the corresponding row element may have been truncated.
-------------------------------------------------------------------------------
Service Access Points
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
SAP 1/1/9:1.2
-------------------------------------------------------------------------------
Service Id         : 100
SAP                : 1/1/9:1.2                Encap             : qinq
QinQ Dot1p         : Default
Description        : (Not Specified)
Admin State        : Down                     Oper State        : Down
Flags              : ServiceAdminDown SapAdminDown
Last Status Change : 12/14/2019 11:35:20
Last Mgmt Change   : 12/14/2019 13:09:09
Dot1Q Ethertype    : 0x8100                   QinQ Ethertype    : 0x8100
Split Horizon Group: (Not Specified)
Admin MTU          : 1522                     Oper MTU          : 1522
Ingr IP Fltr-Id    : n/a                      Egr IP Fltr-Id    : n/a
Ingr Mac Fltr-Id   : n/a                      Egr Mac Fltr-Id   : n/a
Ingr IPv6 Fltr-Id  : n/a                      Egr IPv6 Fltr-Id  : n/a
tod-suite          : None
Egr Agg Rate CIR   : 0                        Egr Agg Rate PIR  : max
Endpoint           : N/A
                                              Limit Unused BW   : Disabled
Acct. Pol          : None                     Collect Stats     : Disabled
Oper Group         : (none)                   Monitor Oper Grp  : (none)
Host Lockout Plcy  : n/a
Lag Link Map Prof  : (none)
Cflowd             : Disabled
-------------------------------------------------------------------------------
QOS
-------------------------------------------------------------------------------
Ingress qos-policy : 1                        Egress qos-policy : 1
Table-based        : disabled
-------------------------------------------------------------------------------
Aggregate Policer
-------------------------------------------------------------------------------
Rate               : n/a                      Burst             : n/a
-------------------------------------------------------------------------------
Egress Aggregate Meter
-------------------------------------------------------------------------------
Rate               : n/a                      Burst             : n/a
-------------------------------------------------------------------------------
Ingress QoS Classifier Usage
-------------------------------------------------------------------------------
Classifiers Allocated: 2                    Meters Allocated   : 1
Classifiers Used     : 1                    Meters Used        : 1
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
Sap Statistics
-------------------------------------------------------------------------------
                     Packets                 Octets
Ingress Stats:       0                       0
Egress Stats:        0                       0
```

```
Ingress Drop Stats:     0                       0

Extra-Tag Drop Stats:   n/a                     n/a
-------------------------------------------------------------------------------
Sap per Meter stats (in/out counter mode)
-------------------------------------------------------------------------------
                        Packets                 Octets
Ingress Meter 1
For. InProf           : 0                       0
For. OutProf          : 0                       0
-------------------------------------------------------------------------------
Sap per Egress Queue stats
-------------------------------------------------------------------------------
                        Packets                 Octets
Egress Queue 1 (be)
Fwd Stats             :  0                      0
Drop Stats            :  0                      0

Egress Queue 2 (l2)
Fwd Stats             :  0                      0
Drop Stats            :  0                      0

Egress Queue 3 (af)
Fwd Stats             :  0                      0
Drop Stats            :  0                      0

Egress Queue 4 (l1)
Fwd Stats             :  0                      0
Drop Stats            :  0                      0

Egress Queue 5 (h2)
Fwd Stats             :  0                      0
Drop Stats            :  0                      0

Egress Queue 6 (ef)
Fwd Stats             :  0                      0
Drop Stats            :  0                      0

Egress Queue 7 (h1)
Fwd Stats             :  0                      0
Drop Stats            :  0                      0

Egress Queue 8 (nc)
Fwd Stats             :  0                      0
Drop Stats            :  0                      0
-------------------------------------------------------------------------------
Service Endpoints
-------------------------------------------------------------------------------
No Endpoints found.
-------------------------------------------------------------------------------
===============================================================================
VLL Sites
===============================================================================
Site                Site-Id   Dest                Admin       Oper  Fwdr
-------------------------------------------------------------------------------
No Matching Entries
===============================================================================
===============================================================================
* indicates that the corresponding row element may have been truncated.
A:Dut-A#
```

Table 61: Output fields: service ID All

Label	Description
Service Id	Displays the service identifier
VPN Id	Displays the number that identifies the VPN
Service Type	Specifies the type of service
Name	Displays the name of the service
Description	Displays generic information about the service
Customer Id	Displays the customer identifier
Creation Origin	Displays how the service was created
Last Status Change	Displays the date and time of the most recent status change to this customer
Last Mgmt Change	Displays the date and time of the most recent management-initiated change to this customer
Admin State	Displays the administrative state of the service
Oper State	Displays the operational state of the service
MTU	Displays the largest frame size (in octets) that the service can handle
MTU Check	Displays whether the service performs an MTU check of the ingress packet before forwarding it
VC Switching	Specifies whether the service is configured as a PW switching point
SAP Count	Displays the number of SAPs specified for this service
SDP Bind Count	Displays the number of SDPs bound to this service
SAP Type	Displays the SAP type
Propagate MacFlush	Specifies whether propagating a MAC flush is enabled or disabled
Allow IP Intf Bind	Displays whether the service is enabled for route packets if used with an IES or VPRN service
ETH-CFM Service Specifics	
Tunnel Faults	Displays whether tunnel faults are ignored or accepted
Service Destination Points (SDPs)	

Label	Description
Description	Displays the description of the split horizon group
SDP Id	Displays the SDP identifier
Type	Indicates whether this service SDP binding is a spoke or a mesh
Spoke Descr	Displays the description of the spoke SDP
VC Type	Displays the service SDP type (for example, spoke)
VC Tag	Displays the explicit dot1q value used when encapsulating to the SDP far end
Admin Path MTU	The configured largest service frame size (in octets) that can be transmitted through this SDP to the far-end router, without requiring the packet to be fragmented.
Oper Path MTU	The actual largest service frame size (in octets) that can be transmitted through this SDP to the far-end router, without requiring the packet to be fragmented.
Delivery	Specifies the type of delivery used by the SDP: MPLS.
Tunnel Far End	Displays the far end IP address where the transport tunnel used by the SDP terminates
LSP Types	Displays the supported LSP types: • R = RSVP • L = LDP • B = BGP • I = SR-ISIS • O = SR-OSPF • T = SR-TE • n/a = not applicable
Hash Lbl Sig Cap	Displays whether the hash label signal capability is enabled
Oper Hash Label	Displays the operational state of the hash label
Admin State	Displays the administrative state of this SDP
Oper State	Displays the operational state of this SDP
Acct. Pol	Displays the accounting policy applied to the SDP
Collect Stats	Displays whether accounting statistics are collected on the SDP
Ingress Label	Displays the label used by the far-end device to send packets to this device in this service by this SDP

Label	Description
Egress Label	Displays the label used by this device to send packets to the far-end device in this service by this SDP
Ingress IP Filter-Id	The ID of the ingress IP filter policy
Egress IP Filter-Id	The ID of the egress IP filter policy
Ingress IPv6 Filter-Id	The ID of the ingress IPv6 filter policy
Egress IPv6 Filter-Id	The ID of the egress IPv6 filter policy
Admin ControlWord	Not Preferred — **control-word** is not configured on the spoke-SDP Preferred — **control-word** is configured on the spoke-SDP
Oper ControlWord	True — the spoke-SDP transmits the control word when signaling the peer False — the spoke-SDP does not transmit the control word when signaling the peer
Last Status Change	Displays the date and time of the most recent status change to this SDP
Signaling	Displays the signaling protocol used to obtain the ingress and egress labels used in frames transmitted and received on this SDP
Last Mgmt Change	Displays the date and time of the most recent management initiated change to this SDP
Endpoint	Displays the endpoint configured in the service
Precedence	Displays the precedence level of the SDP binding
PW Status Sig	Displays whether pseudowire status signaling for spoke SDPs is enabled or disabled
Force Vlan-Vc	Displays whether the spoke-SDP has been configured to transmit the VLAN of the customer packet ingressing the SAP in the service
Class Fwding State	Displays the admin state of class-based forwarding on this SDP
Flags	Specifies the conditions that affect the operating status of this SAP
Local Pw Bits	Displays the setting of the local pseudowire bits
Peer Pw Bits	Displays the setting of the peer pseudowire bits
Peer Vccv CV Bits	Displays the setting of the pseudowire peer VCCV control verification bits (lspPing)

Label	Description
Peer Vccv CC Bits	Displays the setting of the pseudowire peer VCCV control channel bits (pwe3ControlWord, mplsRouterAlertLabel, or both)
Keepalive Information	
Admin State	Displays the configured keepalive state
Oper State	Displays the operating keepalive state
Hello Time	Displays how often the SDP Echo Request messages are transmitted on this SDP
Hello Msg Len	Displays the length of the SDP Echo Request messages transmitted on this SDP
Max Drop Count	Displays the maximum number of consecutive SDP Echo Request messages that can be unacknowledged before the keepalive protocol reports a fault
Hold Down Time	Displays the amount of time to wait before the keepalive operating status is eligible to enter the alive state
Statistics	
I. Fwd. Pkts.	Displays the number of forwarded ingress packets
I. Fwd. Octs.	Displays the number of forwarded ingress octets
E. Fwd. Pkts.	Displays the number of forwarded egress packets
E. Fwd. Octets	Displays the number of forwarded egress octets
Extra-Tag-Drop-Pkts	Displays the number of packets that were dropped because the number of tags exceeded the number of tags supported by the SAP
Extra-Tag-Drop-Oc*	Displays the number of octets that were dropped because the number of tags exceeded the number of tags supported by the SAP
Control Channel Status	
PW Status	Displays the status of the pseudowire (Active or Standby)
Refresh Timer	Displays the configured refresh timer. The refresh timer is the interval at which the control channel status messages are sent between peers.
Peer Status Expire	False—The timer for receiving the control channel status bits from the peer has not expired; this is the default setting

Label	Description
	True —The timer for receiving the control channel status bits from the peer has expired; this field is set to true if the bits are not received from the peer
Request Timer	Displays the configured request timer, which is based on the control channel status request messages sent to the peer
Acknowledgment	False — The node does not send an acknowledgment to the peer; this is the default setting True — The node sends an acknowledgment to the peer
RSVP/Static LSPs	
Associated LSP List	Displays the associated LSPs
Lsp Name	Displays the name of the static LSP
Admin State	Displays the configured state of the service
Oper State	Displays the actual state of the service
Time Since Last Tr*	Displays the time that the associated static LSP has been in service
Number of SDPs	Displays the number of SDPs
Service Access Points	
Service Id	Displays the service ID
SAP	Displays the SAP ID
Encap	Displays the encapsulation type of the SAP
Description	Displays the description of the SAP
Admin State	Displays the administrative state of the SAP
Oper State	Displays the operating state of the SAP
Flags	Displays the conditions that affect the operating status of this SAP
Last Status Change	Displays the time of the most recent operating status change to this SAP
Last Mgmt Change	Displays the time of the most recent management-initiated change to this SAP
Dot1Q Ethertype	Displays the value of the dot1q Ethertype
QinQ Ethertype	Displays the value of the qinq Ethertype

Label	Description
Split Horizon Group	Displays the name of the split horizon group for this service
Admin MTU	Displays the configured largest service frame size (in octets) that can be transmitted through the SAP to the far-end router without requiring the packet to be fragmented
Oper MTU	Displays the actual largest service frame size (in octets) that can be transmitted through the SAP to the far-end router, without requiring the packet to be fragmented
Ingr IP Fltr-Id	Displays the ingress filter policy ID assigned to the SAP
Egr IP Fltr-Id	Displays the egress filter policy ID assigned to the SAP
Ingr Mac Fltr-Id	Displays the ingress MAC filter policy ID assigned to the SAP
Egr Mac Fltr-Id	Displays the egress MAC filter policy ID assigned to the SAP
Ingr IPv6 Fltr-Id	Displays the ingress IPv6 filter policy ID assigned to the SAP
Egr IPv6 Fltr-Id	Displays the egress IPv6 filter policy ID assigned to the SAP
tod-suite	Displays whether a time-based policy is applied to a multiservice site
Egr Agg Rate CIR	Displays the CIR rate limit in the access egress direction for the aggregate of the SAP queues
Egr Agg Rate PIR	Displays the PIR rate limit in the access egress direction for the aggregate of the SAP queues
Endpoint	Displays the endpoint configured in the service
Acct. Pol	Displays the accounting policy applied to the SAP
Collect Stats	Displays whether accounting statistics are collected on the SAP
QoS	
Ingress qos-policy	Displays the SAP ingress QoS policy ID
Egress qos-policy	Displays the SAP egress QoS policy ID
Table-based	Enabled — Table-based classification has been configured in the QoS policy that has been applied on the SAP Disabled — Table-based classification has not been configure in the QoS policy that has been applied on the SAP
Aggregate Policer	
Rate	Displays the aggregate policer rate
Burst	Displays the aggregate policer burst size

Label	Description
Egress Aggregate Meter	
Rate	Displays the egress aggregate meter rate
Burst	Displays the egress aggregate meter burst size
Ingress QoS Classifier Usage	
Classifiers Allocated	Displays the number of classifiers allocated to the ingress QoS policy
Meters Allocated	Displays the number of meters allocated to the ingress QoS policy
Classifiers Used	Displays the number of classifiers in use by the ingress QoS policy
Meters Used	Displays the number of meters in use by the ingress QoS policy
SAP Statistics	
Packets	(Header) Displays the number of packets counted for the statistic after the last counter reset
Octets	(Header) Displays the number of octets counted for the statistic after the last counter reset
Ingress Stats	Indicates that the following statistics are ingress statistics
Egress Stats	Indicates that the following statistics are egress statistics
Extra-Tag Drop Stats	Displays the number of packets that were dropped because they exceeded the number of tags supported on the SAP
Ingress Drop Stats	Displays the number of packets dropped because of policers that are applied on the SAP
Extra-Tag Drop Stats	Displays the number of packets dropped because they had more tags than the maximum number of tags supported on the SAP
Sap per Meter stats (in/out counter mode)	
Packets	(Header) Displays the number of packets counted for the statistic after the last counter reset
Octets	(Header) Displays the number of octets counted for the statistic after the last counter reset
For. InProf	Displays the number of in-profile packets or octets (rate below CIR) forwarded
For. OutProf	Displays the number of out-of-profile packets or octets (rate above CIR) forwarded

Label	Description
Sap per Egress Queue stats	
Packets	(Header) Displays the number of packets counted for the statistic after the last counter reset
Octets	(Header) Displays the number of octets counted for the statistic after the last counter reset
Fwd Stats	Displays the number of forwarded packets and octets
Drop Stats	Displays the number of dropped packets and octets
VLL Sites	
Site-Id	Displays the site ID
Admin	Displays the administrative state of the VLL site
Oper	Displays the operational state of the VLL site

arp

Syntax

arp [*ip-address*] | [**mac** *ieee-address*] | [**sap** *sap-id*] | [**interface** *ip-int-name*]

Context

show>service>id

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays the ARP table for the VPLS instance. The ARP entries for a subscriber interface are displayed uniquely. Each MAC associated with the subscriber interface child group-interfaces is displayed with each subscriber interface ARP entry for easy lookup.

Parameters

ip-address

Displays all IP addresses.

mac ieee-address

Displays only ARP entries in the ARP table with the specified 48-bit MAC address. The MAC address is in the form aa:bb:cc:dd:ee:ff or aa-bb-cc-dd-ee-ff, where aa, bb, cc, dd, ee and ff are hexadecimal numbers.

Default All MAC addresses.

sap *sap-id*

Displays SAP information for the specified SAP ID.

interface

Specifies matching service ARP entries associated with the IP interface.

ip-address

Specifies the IP address of the interface for which to display matching ARP entries.

Values a.b.c.d

ip-int-name

Specifies the IP interface name for which to display matching ARPs.

Output

The following table describes the show service-id ARP output fields.

Sample output

Table 62: Output fields: service ID ARP

Label	Description
IP Address	The IP address.
MAC Address	The specified MAC address.
	Type Static — FDB entries created by management.
	Learned — Dynamic entries created by the learning process.
	Other — Local entries for the IP interfaces created.
Expiry	The age of the ARP entry.
Interface	The interface applied to the service.
SAP	The SAP ID.

base

Syntax

base [**msap**]

Context

show>service>id

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays basic information about the service ID including service type, description, SAPs and SDPs.

Output

The following output is an example of basic service information, and Table 63: Output fields: service ID base describes the output fields.

Sample output

```
*A:7210SAS# show service id 10 base

===============================================================================
Service Basic Information
===============================================================================
Service Id        : 10                  Vpn Id            : 0
Service Type      : VPLS
Name              : (Not Specified)
Description       : (Not Specified)
Customer Id       : 1
Last Status Change: 02/06/2106 06:28:12
Last Mgmt Change  : 01/10/1970 01:55:31
Admin State       : Down                Oper State        : Down
MTU               : Not Applicable      Def. Mesh VC Id   : 10
SAP Count         : 0
Uplink Type:      : L2
SAP Type:         : dot1q Range         Customer vlan:    : n/a

-------------------------------------------------------------------------------
Service Access & Destination Points
-------------------------------------------------------------------------------
Identifier                             Type         AdmMTU  OprMTU  Adm  Opr
-------------------------------------------------------------------------------
No Matching Entries
===============================================================================
*A:7210SAS# show service id 10 base

A:Dut-A# show service id 1 base
===============================================
Service Basic Information
===============================================================================
Service Id : 1 Vpn Id : 0
Service Type : Epipe
Customer Id : 1
Last Status Change: 06/24/2001 00:57:55
Last Mgmt Change : 06/24/2001 00:51:36
Admin State : Up Oper State : Up
MTU : 1514
MTU Check : Disabled
Vc Switching : False
SAP count : 1 SDP Bind Count : 1
-------------------------------------------------------------------------------
Service Access and Destination Points
-------------------------------------------------------------------------------
Identifier Type AdmMTU OprMTU Adm Opr
-------------------------------------------------------------------------------
sap:1/1/21:1 q-tag 1518 1518 Up Up
sdp:1:1 S<100.1.12> n/a 1518 1518 Up Up
===============================================================-----------------
A:Dut-A#
```

Table 63: Output fields: service ID base

Label	Description
Service Id	The service identifier.
Service Type	Displays the type of service.
Description	Generic information about the service.
Customer Id	The customer identifier.
Last Mgmt Change	The date and time of the most recent management-initiated change to this customer.
Adm	The administrative state of the service.
Oper	The operational state of the service.
Mtu	The largest frame size (in octets) that the can handle.
Adm	The largest frame size (in octets) that the SAP can handle.
SAP Count	The number of SAPs defined on the service.
SAP Type	The type of SAPs allowed in the service. It also describes the applied processing by the node to the packets received on these SAPs.
Identifier	Specifies the service access (SAP).
OprMTU	Specifies the actual largest service frame size (in octets) that can be transmitted through this SAP, without requiring the packet to be fragmented.
Opr	The operating state of the SAP.

fdb

Syntax

fdb [**sap** *sap-id* [**expiry**]] | [**mac** *ieee-address* [**expiry**]] | [**detail**] [**expiry**]

Context

show>service>id

show>service>fdb-mac

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays FDB entries for a specific MAC address.

Parameters

sap *sap-id*

Specifies the physical port identifier portion of the SAP. See Common CLI command descriptions for command syntax.

detail

Keyword to display detailed information.

expiry

Keyword to display the time until the MAC is aged out.

Output

The following output is an example of FDB information, and Table 64: Output fields: service FDB describes the output fields.

Sample output

```
A:Dut-A# show service id 305 fdb
===============================================================================
Forwarding Database, Service 305
===============================================================================
Service Id        : 305                Mac Move          : Disabled
Mac Move Rate     : 2                  Mac Move Timeout  : 10
Table Size        : 500                Total Count       : 375
Learned Count     : 375                Static Count      : 0
Remote Age        : 60                 Local Age         : 60
High WaterMark    : 95%                Low Watermark     : 90%
Mac Learning      : Enabl              Discard Unknown   : Dsabl
Mac Aging         : Enabl              Relearn Only      : False
===============================================================================
A:Dut-A#
```

Table 64: Output fields: service FDB

Label	Description
ServID	Displays the service ID.
MAC	Displays the associated MAC address.
Mac Move	Displays the administrative state of the MAC movement feature associated with this service.
Primary Factor	Displays a factor for the primary ports defining how many MAC-relearn periods should be used to measure the MAC-relearn rate.
Secondary Factor	Displays a factor for the secondary ports defining how many MAC-relearn periods should be used to measure the MAC-relearn rate.

Label	Description
Mac Move Rate	Displays the maximum rate at which MAC's can be relearned in this service, before the SAP where the moving MAC was last seen is automatically disabled to protect the system against undetected loops or duplicate MAs. The rate is computed as the maximum number of relearns allowed in a 5-second interval; for example, the default rate of 2 relearns per second corresponds to 10 relearns in a 5-second period.
Mac Move Timeout	Displays the time in seconds to wait before a SAP that has been disabled after exceeding the maximum relearn rate is re-enabled. A value of zero indicates that the SAP is not automatically re-enabled after being disabled. If after the SAP is re-enabled it is disabled again, the effective retry timeout is doubled to avoid thrashing.
Mac Move Retries	Displays the number of times retries are performed for re-enabling the SAP or SDP.
Table Size	Specifies the maximum number of learned and static entries allowed in the FDB of this service.
Total Count	Displays the total number of learned entries in the FDB of this service.
Learned Count	Displays the current number of learned entries in the FDB of this service.
Static Count	Displays the current number of static entries in the FDB of this service.
OAM-learned Count	Displays the current number of OAM entries in the FDB of this service.
Remote Age	Displays the number of seconds used to age out FDB entries learned on an SDP. These entries correspond to MAC addresses learned on remote SAPs.
Local Age	Displays the number of seconds used to age out FDB entries learned on local SAPs.
High Watermark	Displays the utilization of the FDB table of this service at which a table full alarm is raised by the agent.
Low Watermark	Displays the utilization of the FDB table of this service at which a table full alarm is cleared by the agent.
Mac Learning	Specifies whether the MAC learning process is enabled

Label	Description
Discard Unknown	Specifies whether frames received with an unknown destination MAC are discarded.
Mac Aging	Indicates whether the MAC aging process is enabled.
Relearn Only	Displays, that when enabled, either the FDB table of this service is full, or that the maximum system-wide number of MACs supported by the agent has been reached, and therefore MAC learning is temporary disabled, and only MAC relearns can take place.
Mac Subnet Len	Displays the number of bits to be considered when performing MAC learning or MAC switching.
Source-Identifier	The location where the MAC is defined.
Type/Age	Type — Specifies the number of seconds used to age out TLS FDB entries learned on local SAPs
	Age — Specifies the number of seconds used to age out TLS FDB entries learned on an SDP. These entries correspond to MAC addresses learned on remote SAPs
	L (Learned) — Dynamic entries created by the learning process.
	OAM — Entries created by the OAM process.
	Static — Statically configured.
Last Change	Indicates the time of the most recent state changes.

host

Syntax

host [**sap** *sap-id*] [**detail**]

host summary

Context

show>service>id

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays static host information configured on this service.

Parameters

sap-id

Specifies the physical port identifier portion of the SAP definition. See Common CLI command descriptions for command syntax.

summary

Keyword to display summary host information.

labels

Syntax

labels

Context

show>service>id

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays the labels being used by the service.

Output

The following output is an example of service label information, and Table 65: Output fields: service ID labels describes the output fields.

Sample output

```
A:Dut-A# show service id 305 labels
===============================================================================
Martini Service Labels
===============================================================================
Svc Id     Sdp Binding        Type  I.Lbl                E.Lbl
-------------------------------------------------------------------------------
305        1217:305           Spok  130506               130516
305        1317:305           Spok  130454               130591
305        1417:305           Spok  130428               131015
305        1617:305           Spok  131060               130843
-------------------------------------------------------------------------------
Number of Bound SDPs : 4
===============================================================================
A:Dut-A#
```

Table 65: Output fields: service ID labels

Label	Description
Svc Id	The service identifier.
Sdp Id	The SDP identifier.
Type	Indicates whether the SDP is spoke.
I. Lbl	The VC label used by the far-end device to send packets to this device in this service by the SDP.
E. Lbl	The VC label used by this device to send packets to the far-end device in this service by the SDP.

l2pt

Syntax

l2pt disabled

l2pt [**detail**]

Context

show>service>id

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays Layer 2 Protocol Tunnel (L2-PT) route information associated with this service.

Parameters

disabled

Keyword to display only entries with termination disabled. This helps identify configuration errors.

detail

Keyword to display detailed information.

Output

The following output is an example of L2PT information, and Table 66: Output fields: L2PT describes the output fields.

Sample output

```
*A:7210SAS>show>service# id 1 l2pt detail
```

```
===============================================================================
L2pt details, Service id 1
===============================================================================

Service Access Points
-------------------------------------------------------------------------------
SapId                       L2pt-                       Admin Bpdu-  Oper Bpdu-
                            termination                 translation  translation
-------------------------------------------------------------------------------
1/1/1                       stp cdp vtp dtp pagp udld  disabled     disabled
-------------------------------------------------------------------------------
Number of SAPs : 1
===============================================================================

===============================================================================
L2pt summary, Service id 1
===============================================================================
       L2pt-term   L2pt-term   Bpdu-trans  Bpdu-trans  Bpdu-trans  Bpdu-trans
       enabled     disabled    auto        disabled    pvst        stp
-------------------------------------------------------------------------------
SAP's  1           0           0           1           0           0
SDP's  0           0           0           0           0           0
-------------------------------------------------------------------------------
Total  1           0           0           1           0           0
===============================================================================
*A:7210SAS>show>service#
```

Table 66: Output fields: L2PT

Label	Description
Service id	Displays the 24-bit (0 to 16777215) service instance identifier for the service.
L2pt-term enabled	Indicates if L2-PT-termination and/or BPDU translation is in use in this service by at least one SAP or spoke-SDP binding. If in use, at least one of L2PT-termination or BPDU translation is enabled. When enabled it is not possible to enable STP on this service.
L2pt-term disabled	Indicates that L2-PT-termination is disabled.
Bpdu-trans auto	Specifies the number of L2-PT PDUs that are translated before being sent out on a port or sap.
Bpdu-trans disabled	Indicates that BPDU translation is disabled.
SAPs	Displays the number of SAPs with L2PT or BPDU translation enabled or disabled.
SDPs	Displays the number of SDPs with L2PT or BPDU translation enabled or disabled.
Total	Displays the column totals of L2PT entities.
SapId	The ID of the access point where this SAP is defined.

Label	Description
L2pt-termination	Indicates whether L2pt termination is enabled or disabled.
Admin Bpdu-translation	Specifies whether BPDU translation is administratively enabled or disabled.
Oper Bpdu-translation	Specifies whether BPDU translation is operationally enabled or disabled.
SAP Id	Specifies the SAP ID.

mac-move

Syntax

mac-move

Context

show>service>id

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays information related to the **mac-move** feature for the specified service.

Output

The following output is an example of service MAC move information, and Table 67: Output fields: service MAC move describes the fields.

Sample output

```
*A:ALU-48>show>service>id# mac-move
===============================================================================
Service Mac Move Information
===============================================================================
Service Id        : 5001               Mac Move          : Disabled
Primary Factor    : 3                  Secondary Factor  : 2
Mac Move Rate     : 2                  Mac Move Timeout  : 10
Mac Move Retries  : 3
-------------------------------------------------------------------------------
SAP Mac Move Information: 1/2/4:1/100
-------------------------------------------------------------------------------
Admin State       : Up                 Oper State        : Down
Flags              : ServiceAdminDown
                     PortOperDown L2OperDown
Time to RetryReset: never              Retries Left      : 3
Mac Move          : Blockable          Blockable Level   : Tertiary
-------------------------------------------------------------------------------
SDP Mac Move Information: 5001:100
-------------------------------------------------------------------------------
Admin State       : Up                 Oper State        : Down
```

```
Flags              : SvcAdminDown SdpOperDown
                     NoIngVCLabel NoEgrVCLabel
                     PathMTUTooSmall
Time to RetryReset: never               Retries Left      : 3
Mac Move           : Blockable          Blockable Level   : Tertiary
===============================================================================
*A:ALU-48>show>service>id#
```

Table 67: Output fields: service MAC move

Label	Description
Service Id	The service identifier.
Mac Move	The administrative state of the MAC movement feature associated with this service.
Primary Factor	A factor for the primary ports defining how many MAC relearn periods should be used to measure the MAC relearn rate.
Secondary Factor	A factor for the secondary ports defining how many MAC relearn periods should be used to measure the MAC relearn rate.
Mac Move Rate	The maximum rate at which MACs can be relearned in this service, before the SAP where the moving MAC was last seen is automatically disabled to protect the system against undetected loops or duplicate MACs. The rate is computed as the maximum number of relearns allowed in a 5-second interval: for example, the default rate of 2 relearns per second corresponds to 10 relearns in a 5-second period.
Mac Move Timeout	The time, in seconds, to wait before a SAP that has been disabled after exceeding the maximum relearn rate is re-enabled. A value of 0 indicates that the SAP is not automatically re-enabled after being disabled. If after the SAP is re-enabled it is disabled again, the effective retry timeout is doubled to avoid thrashing.
Mac Move Retries	The number of times retries are performed for re-enabling the SAP or SDP.
SAP Mac Move Information:	
Admin State	The administrative state of the SAP.
Oper State	The operational state of the SAP.

Label	Description
Flags	Specifies the conditions that affect the operating status of this SAP. Display output includes: ServiceAdminDown, Port OperDown, L2OperDown.
Time to RetryReset	The time, in seconds, to wait before a SAP that has been disabled after exceeding the maximum relearn rate is re-enabled. A value of 0 indicates that the SAP is not automatically re-enabled after being disabled. If after the SAP is re-enabled it is disabled again, the effective retry timeout is doubled to avoid thrashing.
Retries Left	The number of remaining attempts to re-enable the SAP.
Mac Move	Specifies whether MAC move is configured as blockable or not blockable on the SAP.
Blockable Level	Specifies the level at which MAC move is blockable on the SAP (primary, secondary, or tertiary).
SDP Mac Move Information	
Admin State	The administrative state of the SDP.
Oper State	The operational state of the SDP.
Flags	Specifies the conditions that affect the operating status of this SDP. Display output includes: SvcAdminDown, SdpOper Down, NoIngVCLabel, NoEgrVCLabel, PathMTUTooSmall.
Time to RetryReset	The time, in seconds, to wait before a SDP that has been disabled after exceeding the maximum relearn rate is re-enabled. A value of 0 indicates that the SDP is not automatically re-enabled after being disabled. If after the SDP is re-enabled it is disabled again, the effective retry timeout is doubled to avoid thrashing.
Retries Left	The number of remaining attempts to re-enable the SDP.
Mac Move	Specifies whether MAC move is configured as blockable or not blockable on the SDP.
Blockable Level	Specifies the level at which MAC move is blockable on the SDP (primary, secondary, or tertiary).

mrouters

Syntax

mrouters [**detail**]

Context

show>service>id>mld-snooping

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays all multicast routers.

sap

Syntax

sap *sap-id* **detail**

Context

show>service>id

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays information for the SAPs associated with the service.

If no optional parameters are specified, a summary of all associated SAPs is displayed.

Parameters

sap sap-id

Specifies the ID that displays SAPs for the service in the *slot*/*mda*/*port*[**.***channel*] form. See Common CLI command descriptions for command syntax.

detail

Keyword to display detailed information for the SAP.

Output

The following outputs are examples of SAP information, and Table 68: Output fields: service SAP describes the output fields.

- Sample output
- Sample output for 7210 SAS-R6 and 7210 SAS-R12, Table 68: Output fields: service SAP

Sample output

```
*A:DUT-B_sasx>show>service>id# sap 1/1/3:63 detail

===============================================================================
Service Access Points(SAP)
===============================================================================
Service Id         : 63
SAP                : 1/1/3:63                Encap            : q-tag
Description        : (Not Specified)
Admin State        : Up                      Oper State       : Up
Flags              : None
Last Status Change : 05/20/2000 13:33:22
Last Mgmt Change   : 05/19/2000 12:13:41
Loopback Mode      : Internal                No-svc-port used : 1/1/13
Loopback Src Addr  : 00:00:00:22:22:22
Loopback Dst Addr  : 00:00:00:11:11:11
Dot1Q Ethertype    : 0x8100                  QinQ Ethertype   : 0x8100

Max Nbr of MAC Addr: No Limit                Total MAC Addr   : 59
Learned MAC Addr   : 59                      Static MAC Addr  : 0
Admin MTU          : 1518                    Oper MTU         : 1518
Ingr IP Fltr-Id    : n/a                     Egr IP Fltr-Id   : n/a
Ingr Mac Fltr-Id   : n/a                     Egr Mac Fltr-Id  : n/a
tod-suite          : None
Egr Agg Rate Limit : 100000                  Host Conn Verify : Enabled
Mac Learning       : Enabled                 Discard Unkwn Srce: Disabled
Mac Aging          : Enabled                 Mac Pinning      : Disabled
BPDU Translation   : Disabled
L2PT Termination   : Disabled

Acct. Pol          : None                    Collect Stats    : Disabled



-------------------------------------------------------------------------------
Stp Service Access Point specifics
-------------------------------------------------------------------------------
Stp Admin State    : Up                      Stp Oper State   : Down
Core Connectivity  : Down
Port Role          : N/A                     Port State       : Forwarding
Port Number        : 2048                    Port Priority    : 128
Port Path Cost     : 10                      Auto Edge        : Enabled
Admin Edge         : Disabled                Oper Edge        : N/A
Link Type          : Pt-pt                   BPDU Encap       : Dot1d
Root Guard         : Disabled                Active Protocol  : N/A
Last BPDU from     : N/A
CIST Desig Bridge  : N/A                     Designated Port  : N/A

Forward transitions: 0                       Bad BPDUs rcvd   : 0
Cfg BPDUs rcvd     : 0                       Cfg BPDUs tx     : 0
TCN BPDUs rcvd     : 0                       TCN BPDUs tx     : 0
RST BPDUs rcvd     : 0                       RST BPDUs tx     : 0
MST BPDUs rcvd     : 0                       MST BPDUs tx     : 0
-------------------------------------------------------------------------------
ARP host
-------------------------------------------------------------------------------
Admin State        : outOfService
Host Limit         : 1                       Min Auth Interval : 15 minutes

-------------------------------------------------------------------------------
QOS
-------------------------------------------------------------------------------
Ingress qos-policy : 1                       Egress qos-policy : 1
```

```
-------------------------------------------------------------------------------
Sap Egress Policy (1)
-------------------------------------------------------------------------------
Scope              : Template
Remark             : False                    Remark Pol Id     : 2
Accounting         : frame-based
Description    : Default SAP egress QoS policy.
-------------------------------------------------------------------------------
Queue Rates and Rules
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
QueueId        CIR          CIR Adpt Rule        PIR          PIR Adpt Rule
-------------------------------------------------------------------------------
Queue1          0              closest            max            closest
Queue2          0              closest            max            closest
Queue3          0              closest            max            closest
Queue4          0              closest            max            closest
Queue5          0              closest            max            closest
Queue6          0              closest            max            closest
Queue7          0              closest            max            closest
Queue8          0              closest            max            closest
-------------------------------------------------------------------------------
Parent Details
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
QueueId          Port       CIR Level      PIR Weight
-------------------------------------------------------------------------------
Queue1          True             1             1
Queue2          True             1             1
Queue3          True             1             1
Queue4          True             1             1
Queue5          True             1             1
Queue6          True             1             1
Queue7          True             1             1
Queue8          True             1             1
-------------------------------------------------------------------------------
High Slope
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
QueueId        State      Start-Avg(%)   Max-Avg(%)   Max-Prob(%)
-------------------------------------------------------------------------------
Queue1          Down            70           90            75
Queue2          Down            70           90            75
Queue3          Down            70           90            75
Queue4          Down            70           90            75
Queue5          Down            70           90            75
Queue6          Down            70           90            75
Queue7          Down            70           90            75
Queue8          Down            70           90            75
-------------------------------------------------------------------------------
Low Slope
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
QueueId        State      Start-Avg(%)   Max-Avg(%)   Max-Prob(%)
-------------------------------------------------------------------------------
Queue1          Down            50           75            75
Queue2          Down            50           75            75
Queue3          Down            50           75            75
Queue4          Down            50           75            75
Queue5          Down            50           75            75
Queue6          Down            50           75            75
Queue7          Down            50           75            75
Queue8          Down            50           75            75
-------------------------------------------------------------------------------
```

```
Burst Sizes and Time Average Factor
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
QueueId         CBS            MBS       Time Average Factor        Queue-Mgmt
-------------------------------------------------------------------------------
Queue1          def              def              7           default
Queue2          def              def              7           default
Queue3          def              def              7           default
Queue4          def              def              7           default
Queue5          def              def              7           default
Queue6          def              def              7           default
Queue7          def              def              7           default
Queue8          def              def              7           default
-------------------------------------------------------------------------------
Aggregate Policer (Not Available)
-------------------------------------------------------------------------------
rate               : n/a                      burst            : n/a
-------------------------------------------------------------------------------
Ingress QoS Classifier Usage
-------------------------------------------------------------------------------
Classifiers Allocated: 4                    Meters Allocated   : 2
Classifiers Used     : 2                    Meters Used        : 2
-------------------------------------------------------------------------------
Sap Statistics
-------------------------------------------------------------------------------
                      Packets                Octets
Ingress Stats:        90551093               135826639500
Egress Stats:         0                      0
-------------------------------------------------------------------------------
Sap per Meter stats
-------------------------------------------------------------------------------
                      Packets                Octets

Ingress Meter 1 (Unicast)
For. InProf          : 0                     0
For. OutProf         : 0                     0

Ingress Meter 11 (Multipoint)
For. InProf          : 3                     4500
For. OutProf         : 90611158              135916737000
-------------------------------------------------------------------------------
Sap per Queue stats
-------------------------------------------------------------------------------
                      Packets                Octets

Egress Queue 1 (be)
Fwd Stats            :  90593283             137701790160
Drop InProf          :  0                    0
Drop OutProf         :  0                    0

Egress Queue 2 (l2)
Fwd Stats            :  0                    0
Drop InProf          :  0                    0
Drop OutProf         :  0                    0

Egress Queue 3 (af)
Fwd Stats            :  0                    0
Drop InProf          :  0                    0
Drop OutProf         :  0                    0

Egress Queue 4 (l1)
Fwd Stats            :  0                    0
Drop InProf          :  0                    0
Drop OutProf         :  0                    0
```

```
Egress Queue 5 (h2)
Fwd Stats            :  0                      0
Drop InProf          :  0                      0
Drop OutProf         :  0                      0

Egress Queue 6 (ef)
Fwd Stats            :  0                      0
Drop InProf          :  0                      0
Drop OutProf         :  0                      0

Egress Queue 7 (h1)
Fwd Stats            :  0                      0
Drop InProf          :  0                      0
Drop OutProf         :  0                      0

Egress Queue 8 (nc)
Fwd Stats            :  0                      0
Drop InProf          :  0                      0
Drop OutProf         :  0                      0
===============================================================================
*A:DUT-B_sasx>show>service>id#
```

Sample output for 7210 SAS-R6 and 7210 SAS-R12

```
*A:Dut-A# show service id 10 sap 5/1/1:800 detail
===============================================================================
Service Access Points(SAP)
===============================================================================
Service Id         : 10
SAP                : 5/1/1:800               Encap             : q-tag
Description        : (Not Specified)
Admin State        : Up                      Oper State        : Down
Flags              : PortOperDown
Last Status Change : 11/07/2017 04:48:25
Last Mgmt Change   : 11/07/2017 05:02:47
Dot1Q Ethertype    : 0x8100                  QinQ Ethertype    : 0x8100
Split Horizon Group: (Not Specified)
Admin MTU          : 1518                    Oper MTU          : 1518
Ingr IP Fltr-Id    : n/a                     Egr IP Fltr-Id    : n/a
Ingr Mac Fltr-Id   : n/a                     Egr Mac Fltr-Id   : n/a
Ingr IPv6 Fltr-Id  : n/a                     Egr IPv6 Fltr-Id  : n/a
BGP IPv4 FlowSpec  : Disabled
BGP IPv6 FlowSpec  : Disabled
tod-suite          : None
Egr Agg Rate CIR   : 0                       Egr Agg Rate PIR  : max
                                             Limit Unused BW   : Disabled
Acct. Pol          : None                    Collect Stats     : Disabled
Anti Spoofing      : None                    Dynamic Hosts     : Enabled
Oper Group         : (none)                  Monitor Oper Grp  : (none)
Host Lockout Plcy  : n/a
Lag Link Map Prof  : (none)
-------------------------------------------------------------------------------
QOS
-------------------------------------------------------------------------------
Ingress qos-policy : 17                      Egress qos-policy : 1
Table-based        : enabled
-------------------------------------------------------------------------------
Aggregate Policer
-------------------------------------------------------------------------------
Rate               : n/a                     Burst             : n/a
-------------------------------------------------------------------------------
Egress Aggregate Meter
```

```
-------------------------------------------------------------------------------
Rate               : n/a                      Burst             : n/a
-------------------------------------------------------------------------------
Ingress QoS Classifier Usage
-------------------------------------------------------------------------------
Classifiers Allocated: 60                   Meters Allocated   : 30
Classifiers Used     : 9                    Meters Used        : 8
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
Sap Statistics
-------------------------------------------------------------------------------
                        Packets                 Octets
Ingress Stats:          0                       0
Egress Stats:           0                       0
Ingress Drop Stats:     0                       0

Extra-Tag Drop Stats:   n/a                     n/a
-------------------------------------------------------------------------------
Sap per Meter stats (in/out counter mode)
-------------------------------------------------------------------------------
                        Packets                 Octets
Ingress Meter 1
For. InProf           : 0                       0
For. OutProf          : 0                       0

Ingress Meter 2
For. InProf           : 0                       0
For. OutProf          : 0                       0

Ingress Meter 3
For. InProf           : 0                       0
For. OutProf          : 0                       0

Ingress Meter 4
For. InProf           : 0                       0
For. OutProf          : 0                       0

Ingress Meter 5
For. InProf           : 0                       0
For. OutProf          : 0                       0

Ingress Meter 6
For. InProf           : 0                       0
For. OutProf          : 0                       0

Ingress Meter 7
For. InProf           : 0                       0
For. OutProf          : 0                       0

Ingress Meter 8
For. InProf           : 0                       0
For. OutProf          : 0                       0
===============================================================================
```

Table 68: Output fields: service SAP

Label	Description
Service Id	The service identifier.
SAP	The SAP and qtag.

Label	Description
Encap	The encapsulation type of the SAP.
Ethertype	Specifies an Ethernet type II Ethertype value.
Admin State	The administrative state of the SAP.
Oper State	The operational state of the SAP.
Flags	Specifies the conditions that affect the operating status of this SAP. Display output includes: ServiceAdminDown, SapAdminDown, InterfaceAdminDown, PortOperDown, L2OperDown, Relearn LimitExceeded, ParentIfAdminDown, TodResourceUnavail, Tod MssResourceUnavail, SapParamMismatch, SapIngressNamed PoolMismatch, SapEgressNamedPoolMismatch, NoSapEpipe RingNode.
Last Status Change	Specifies the time of the most recent operating status change to this SAP
Last Mgmt Change	Specifies the time of the most recent management-initiated change to this SAP.
Ingress qos-policy	The ingress QoS policy ID assigned to the SAP.
Ingress Filter-Id	The ingress filter policy ID assigned to the SAP.
Egress Filter-Id	The egress filter policy ID assigned to the SAP.
Acct. Pol	The accounting policy ID assigned to the SAP.
Collect Stats	Specifies whether collect stats is enabled.
SAP per Meter stats	
Ingress Meter	Specifies the meter ID.
For. InProf	The number of in-profile packets and octets (rate below CIR) forwarded.
For. OutProf	The number of out-of-profile packets and octets.
Ingress TD Profile	The profile ID applied to the ingress SAP.
Egress TD Profile	The profile ID applied to the egress SAP.
Alarm Cell Handling	The indication that OAM cells are being processed.
AAL-5 Encap	The AAL-5 encapsulation type.
Aggregate Policer	rate-indicates the rate of the aggregate policer. burst-indicates the burst-size of the aggregate policer.

Label	Description
Loopback Mode	Displays the Ethernet port loopback mode.
Loopback Src Addr	Displays the configured loopback source address.
Loopback Dst Addr	Displays the configured loopback destination address.
No-svc-port used	Displays the port ID of the port on which no service is configured. This port is used for the port loop back with MAC swap functionality.
Egr Agg Rate Limit	Displays the egress aggregate rate limit.
Loopback Mode	Displays the Ethernet port loopback mode.
Loopback Src Addr	Displays the configured loopback source address.
Loopback Dst Addr	Displays the configured loopback destination address.
No-svc-port used	Displays the port ID of the port on which no service is configured. This port is used for the port loop back with MAC swap functionality.
Table-based	Indicates the use of table-based resource classification: Enabled (table-based) or Disabled (CAM-based).

sdp

Syntax

sdp [*sdp-id* | **far-end** *ip-addr*] [**detail**]

Context

show>service>id

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays information for the SDPs associated with the service. If no optional parameters are specified, a summary of all associated SDPs is displayed.

Parameters

sdp-id

Displays information for only the specified SDP ID.

Default All SDPs

Values 1 to 17407

far-end *ip-addr*

Displays only SDPs matching with the specified far-end IP address.

Default SDPs with any far-end IP address.

detail

Keyword to display detailed SDP information.

Output

The following output is an example of SDP information, and Table 69: Output fields: service ID SDP describes the output fields.

Sample output

```
A:Dut-A>show>service>id# sdp 1217:305
===============================================================================
Service Destination Point (Sdp Id : 1217:305)
===============================================================================
SdpId            Type IP address      Adm     Opr       I.Lbl       E.Lbl
-------------------------------------------------------------------------------
1217:305         Spok 10.20.1.2       Up      Up        130506      130516
-------------------------------------------------------------------------------
Number of SDPs : 1
===============================================================================
A:Dut-A>show>service>id# sdp 1217:305  detail


A:Dut-A>show>service>id#
===============================================================================
Service Destination Point (Sdp Id : 1217:305) Details
-------------------------------------------------------------------------------
 Sdp Id 1217:305  -(10.20.1.2)
-------------------------------------------------------------------------------
Description     : Default sdp description
SDP Id             : 1217:305                Type              : Spoke
VC Type            : Ether                   VC Tag            : n/a
Admin Path MTU     : 0                       Oper Path MTU     : 9186
Far End            : 10.20.1.2               Delivery          : MPLS

Admin State        : Up                      Oper State        : Up
Acct. Pol          : None                    Collect Stats     : Disabled
Managed by Service : 300                     Prune State       : Not Pruned
Managed by Spoke   : 1217:300
Ingress Label      : 130506                  Egress Label      : 130516
Admin ControlWord  : Not Preferred           Oper ControlWord  : False
Last Status Change : 07/07/2009 18:49:40     Signaling         : TLDP
Last Mgmt Change   : 07/07/2009 14:39:14     Force Vlan-Vc     : Disabled
Last Mgmt Change   : 07/07/2009 14:39:14
Flags              : None
Peer Pw Bits       : None
Peer Fault Ip      : None
Max Nbr of MAC Addr: No Limit                Total MAC Addr    : 0
Learned MAC Addr   : 0                       Static MAC Addr   : 0

MAC Learning       : Enabled                 Discard Unkwn Srce: Disabled
MAC Aging          : Enabled
L2PT Termination   : Disabled                BPDU Translation  : Disabled
MAC Pinning        : Disabled
```

```
KeepAlive Information :
Admin State        : Enabled                 Oper State        : Alive
Hello Time         : 10                      Hello Msg Len     : 0
Max Drop Count     : 3                       Hold Down Time    : 10

Statistics            :
I. Fwd. Pkts.      : 13601                   I. Fwd. Octs.     : 10676338
E. Fwd. Pkts.      : 83776987                E. Fwd. Octets    : 51589499116

Associated LSP LIST :
Lsp Name           : A_B_17
Admin State        : Up                      Oper State        : Up
Time Since Last Tr*: 08h31m06s
-------------------------------------------------------------------------------
Stp Service Destination Point specifics
-------------------------------------------------------------------------------
Mac Move           : Blockable
Stp Admin State    : Down                    Stp Oper State    : Down
Core Connectivity  : Down
Port Role          : N/A                     Port State        : Forwarding
Port Number        : 2049                    Port Priority     : 128
Port Path Cost     : 10                      Auto Edge         : Enabled
Admin Edge         : Disabled                Oper Edge         : N/A
Link Type          : Pt-pt                   BPDU Encap        : Dot1d
Root Guard         : Disabled                Active Protocol   : N/A
Last BPDU from     : N/A
Designated Bridge  : N/A                     Designated Port Id: 0

Fwd Transitions    : 0                       Bad BPDUs rcvd    : 0
Cfg BPDUs rcvd     : 0                       Cfg BPDUs tx      : 0
TCN BPDUs rcvd     : 0                       TCN BPDUs tx      : 0
RST BPDUs rcvd     : 0                       RST BPDUs tx      : 0
-------------------------------------------------------------------------------
Number of SDPs : 1
-------------------------------------------------------------------------------
===============================================================================
* indicates that the corresponding row element may have been truncated.
A:Dut-A>show>service>id#
```

Table 69: Output fields: service ID SDP

Label	Description
Sdp Id	The SDP identifier.
Type	Indicates whether the SDP is spoke.
VC Type	Displays the VC type: Ether, VLAN, or VPLS.
VC Tag	Displays the explicit dot1Q value used when encapsulating to the SDP far end.
I. Lbl	The VC label used by the far-end device to send packets to this device in this service by the SDP.
Admin Path MTU	The operating path MTU of the SDP is equal to the admin path MTU (when one is set) or the dynamically computed tunnel MTU, when no admin path MTU is set (the default case.)

Label	Description
Oper Path MTU	The actual largest service frame size (in octets) that can be transmitted through this SDP to the far-end router, without requiring the packet to be fragmented.
Far End	Specifies the IP address of the remote end of the MPLS tunnel defined by this SDP.
Delivery	Specifies the type of delivery used by the SDP: MPLS.
Admin State	The administrative state of this SDP.
Oper State	The current status of the SDP.
Ingress Label	The label used by the far-end device to send packets to this device in this service by this SDP.
Egress Label	The label used by this device to send packets to the far-end device in this service by the SDP.
Last Changed	The date and time of the most recent change to the SDP.
Signaling	Specifies the signaling protocol used to obtain the ingress and egress labels used in frames transmitted and received on this SDP.
Admin State	The administrative state of the keepalive process.
Oper State	The operational state of the keepalive process.

split-horizon-group

Syntax

split-horizon-group [*group-name*]

Context

show>service>id

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays service split horizon groups.

Parameters

group-name

Specifies a split horizon group name.

Output

The following output is an example of service split horizon group information, and Table 70: Output fields: split horizon group describes the fields.

Sample output

```
*A:ALU-48>show>service>id# split-horizon-group
===============================================================================
Service: Split Horizon Group
===============================================================================
Name                                Description
-------------------------------------------------------------------------------
R   shg5001
-------------------------------------------------------------------------------
R = Residential Split Horizon Group
A = Auto Created Split Horizon Group
No. of Split Horizon Groups: 1
```

```
*A:ALU-48>show>service>id# split-horizon-group shg5001
===============================================================================
Service: Split Horizon Group
===============================================================================
Name                                Description
-------------------------------------------------------------------------------
R   shg5001
-------------------------------------------------------------------------------
Associations
-------------------------------------------------------------------------------
SAP                                 1/2/4:1/100
SDP                                 5001:100
-------------------------------------------------------------------------------
R = Residential Split Horizon Group
SAPs Associated : 1                 SDPs Associated : 1
===============================================================================
*A:ALU-48>show>service>id#
```

Table 70: Output fields: split horizon group

Label	Description
Name	The name of the split horizon group. When preceded by "R", the group is a residential split horizon group.
Description	A description of the split horizon group as configured by the user.
Associations	A list of SAPs and SDPs associated with the split horizon group.

stp

Syntax

stp [**detail**]

stp mst-instance *mst-inst-number*

Context

show>service>id

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays information for the STP instance for the service.

Parameters

detail

Keyword to display detailed information.

mst-inst-number

Displays information about the specified MST.

Values 1 to 4094

Output

The following output is an example of STP information, and Table 71: Output fields: service ID STP describes the output fields.

Sample output

```
A:Dut-A>show>service>id# stp
===============================================================================
Stp info, Service 305
===============================================================================
Bridge Id          : 00:0d.00:20:ab:cd:00:01  Top. Change Count : 5
Root Bridge        : This Bridge              Stp Oper State    : Up
Primary Bridge     : N/A                      Topology Change   : Inactive
Mode               : Rstp                     Last Top. Change  : 0d 08:35:16
Vcp Active Prot.   : N/A
Root Port          : N/A                      External RPC      : 0
===============================================================================
Stp port info
===============================================================================
Sap/Sdp Id         Oper-     Port-      Port-       Port-  Oper-  Link-  Active
                   State     Role       State       Num    Edge   Type   Prot.
-------------------------------------------------------------------------------
1/1/16:305         Up        Designated Forward     2048   False  Pt-pt  Rstp
lag-4:305          Up        Designated Forward     2000   False  Pt-pt  Rstp
1217:305           Up        N/A        Forward     2049   N/A    Pt-pt  N/A
1317:305           Up        N/A        Forward     2050   N/A    Pt-pt  N/A
1417:305           Up        N/A        Forward     2051   N/A    Pt-pt  N/A
1617:305           Pruned    N/A        Discard     2052   N/A    Pt-pt  N/A
===============================================================================
A:Dut-A>show>service>id#


A:Dut-A>show>service>id# stp detail
===============================================================================
Spanning Tree Information
===============================================================================
VPLS Spanning Tree Information
-------------------------------------------------------------------------------
```

```
VPLS oper state    : Up                       Core Connectivity : Down
Stp Admin State    : Up                       Stp Oper State    : Up
Mode               : Rstp                     Vcp Active Prot.  : N/A

Bridge Id          : 00:0d.00:20:ab:cd:00:01  Bridge Instance Id: 13
Bridge Priority    : 0                        Tx Hold Count     : 6
Topology Change    : Inactive                 Bridge Hello Time : 2
Last Top. Change   : 0d 08:35:29              Bridge Max Age    : 20
Top. Change Count  : 5                        Bridge Fwd Delay  : 15
MST region revision: 0                        Bridge max hops   : 20
MST region name    :

Root Bridge        : This Bridge
Primary Bridge     : N/A

Root Path Cost     : 0                        Root Forward Delay: 15
Rcvd Hello Time    : 2                        Root Max Age      : 20
Root Priority      : 13                       Root Port         : N/A
-------------------------------------------------------------------------------
Spanning Tree Sap/Spoke SDP Specifics
-------------------------------------------------------------------------------
SAP Identifier     : 1/1/16:305               Stp Admin State   : Up
Port Role          : Designated               Port State        : Forwarding
Port Number        : 2048                     Port Priority     : 128
Port Path Cost     : 10                       Auto Edge         : Enabled
Admin Edge         : Disabled                 Oper Edge         : False
Link Type          : Pt-pt                    BPDU Encap        : PVST
Root Guard         : Disabled                 Active Protocol   : Rstp
Last BPDU from     : 80:04.00:0a:1b:2c:3d:4e
CIST Desig Bridge  : This Bridge              Designated Port   : 34816
Forward transitions: 5                        Bad BPDUs rcvd    : 0
Cfg BPDUs rcvd     : 0                        Cfg BPDUs tx      : 0
TCN BPDUs rcvd     : 0                        TCN BPDUs tx      : 0
RST BPDUs rcvd     : 29                       RST BPDUs tx      : 23488
MST BPDUs rcvd     : 0                        MST BPDUs tx      : 0

SAP Identifier     : lag-4:305                Stp Admin State   : Up
Port Role          : Designated               Port State        : Forwarding
Port Number        : 2000                     Port Priority     : 128
Port Path Cost     : 10                       Auto Edge         : Enabled
Admin Edge         : Disabled                 Oper Edge         : False
Link Type          : Pt-pt                    BPDU Encap        : Dot1d
Root Guard         : Disabled                 Active Protocol   : Rstp
Last BPDU from     : 80:04.00:0a:1b:2c:3d:4e
CIST Desig Bridge  : This Bridge              Designated Port   : 34768
Forward transitions: 4                        Bad BPDUs rcvd    : 0
Cfg BPDUs rcvd     : 0                        Cfg BPDUs tx      : 0
TCN BPDUs rcvd     : 0                        TCN BPDUs tx      : 0
RST BPDUs rcvd     : 23                       RST BPDUs tx      : 23454
MST BPDUs rcvd     : 0                        MST BPDUs tx      : 0

SDP Identifier     : 1217:305                 Stp Admin State   : Down
Port Role          : N/A                      Port State        : Forwarding
Port Number        : 2049                     Port Priority     : 128
Port Path Cost     : 10                       Auto Edge         : Enabled
Admin Edge         : Disabled                 Oper Edge         : N/A
Link Type          : Pt-pt                    BPDU Encap        : Dot1d
Root Guard         : Disabled                 Active Protocol   : N/A
Last BPDU from     : N/A
Designated Bridge  : N/A                      Designated Port Id: 0
Fwd Transitions    : 0                        Bad BPDUs rcvd    : 0
Cfg BPDUs rcvd     : 0                        Cfg BPDUs tx      : 0
TCN BPDUs rcvd     : 0                        TCN BPDUs tx      : 0
RST BPDUs rcvd     : 0                        RST BPDUs tx      : 0
```

```
SDP Identifier     : 1317:305               Stp Admin State   : Down
Port Role          : N/A                    Port State        : Forwarding
Port Number        : 2050                   Port Priority     : 128
Port Path Cost     : 10                     Auto Edge         : Enabled
Admin Edge         : Disabled               Oper Edge         : N/A
Link Type          : Pt-pt                  BPDU Encap        : Dot1d
Root Guard         : Disabled               Active Protocol   : N/A
Last BPDU from     : N/A
Designated Bridge  : N/A                    Designated Port Id: 0
Fwd Transitions    : 0                      Bad BPDUs rcvd    : 0
Cfg BPDUs rcvd     : 0                      Cfg BPDUs tx      : 0
TCN BPDUs rcvd     : 0                      TCN BPDUs tx      : 0
RST BPDUs rcvd     : 0                      RST BPDUs tx      : 0

SDP Identifier     : 1417:305               Stp Admin State   : Down
Port Role          : N/A                    Port State        : Forwarding
Port Number        : 2051                   Port Priority     : 128
Port Path Cost     : 10                     Auto Edge         : Enabled
Admin Edge         : Disabled               Oper Edge         : N/A
Link Type          : Pt-pt                  BPDU Encap        : Dot1d
Root Guard         : Disabled               Active Protocol   : N/A
Last BPDU from     : N/A
Designated Bridge  : N/A                    Designated Port Id: 0
Fwd Transitions    : 1                      Bad BPDUs rcvd    : 0
Cfg BPDUs rcvd     : 0                      Cfg BPDUs tx      : 0
TCN BPDUs rcvd     : 0                      TCN BPDUs tx      : 0
RST BPDUs rcvd     : 0                      RST BPDUs tx      : 0

SDP Identifier     : 1617:305               Stp Admin State   : Down
Port Role          : N/A                    Port State        : Discarding
Port Number        : 2052                   Port Priority     : 128
Port Path Cost     : 10                     Auto Edge         : Enabled
Admin Edge         : Disabled               Oper Edge         : N/A
Link Type          : Pt-pt                  BPDU Encap        : Dot1d
Root Guard         : Disabled               Active Protocol   : N/A
Last BPDU from     : N/A
Designated Bridge  : N/A                    Designated Port Id: 0
Fwd Transitions    : 0                      Bad BPDUs rcvd    : 0
Cfg BPDUs rcvd     : 0                      Cfg BPDUs tx      : 0
TCN BPDUs rcvd     : 0                      TCN BPDUs tx      : 0
RST BPDUs rcvd     : 0                      RST BPDUs tx      : 0
===============================================================================
A:Dut-A>show>service>id#
```

Table 71: Output fields: service ID STP

Label	Description
Bridge-id	Specifies the MAC address used to identify this bridge in the network.
Bridge fwd delay	Specifies how fast a bridge changes its state when moving toward the forwarding state.
Bridge Hello time	Specifies the amount of time between the transmission of configuration BPDUs.

Label	Description
Bridge max age	Specifies the maximum age of STP information learned from the network on any port before it is discarded. This is the actual value that this bridge is currently using.
Bridge priority	Defines the priority of the STP instance associated with this service.
Topology change	Specifies whether a topology change is currently in progress.
Last Top. change	Specifies the time (in hundredths of a second) after the last time a topology change was detected by the STP instance associated with this service.
Top. change count	Specifies the total number of topology changes detected by the Spanning Tree Protocol instance associated with this service after the management entity was last reset or initialized.
Root bridge-id	Specifies the bridge identifier of the root of the spanning tree as determined by the STP instance associated with this service. This value is used as the Root Identifier parameter in all configuration BPDUs originated by this node.
Root path cost	Specifies the cost of the path to the root bridge as seen from this bridge.
Root forward delay	Specifies how fast the root changes its state when moving toward the forwarding state.
hello time	Specifies the amount of time between the transmission of configuration BPDUs.
Root max age	Specifies the maximum age of STP information learned from the network on any port before it is discarded.
Root priority	This object specifies the priority of the bridge that is currently selected as root-bridge for the network.
Root port	Specifies the port number of the port which provides the lowest cost path from this bridge to the root bridge.
SAP Identifier	The ID of the access port where this SAP is defined.
BPDU encap	Specifies the type of encapsulation used on BPDUs sent out and received on this SAP.
Port Number	Specifies the value of the port number field that is contained in the least significant 12 bits of the 16-bit port ID associated with this SAP.
Priority	Specifies the value of the port priority field that is contained in the most significant 4 bits of the 16-bit port ID associated with this SAP.

Label	Description
Cost	Specifies the contribution of this port to the path cost of paths toward the spanning tree root which include this port.
Designated Port	Specifies the port identifier of the port on the designated bridge for this port segment.
Designated Bridge	Specifies the bridge identifier of the bridge which this port considers to be the designated bridge for this port segment.

mstp-configuration

Syntax

mstp-configuration

Context

show>service>id

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays the MSTP specific configuration data. This command is valid only on a management VPLS.

Output

The following table describes the show service ID MSTP command output fields.

Show output

Table 72: Output fields: service ID MSTP configuration

Label	Description
Region Name	Displays the MSTP region name.
Region Revision	Displays the MSTP region revision.
MST Max Hops	Displays the MSTP maximum hops specified.
Instance	Displays the MSTP instance number.
Priority	Displays the MSTP priority.
Vlans mapped	Displays the VLAN range of the MSTP instance.

dhcp

Syntax

dhcp

Context

show>service>id

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

Commands in this context display DHCP information for the specified service.

statistics

Syntax

statistics [**sap** *sap-id*]

statistics [**sdp** *sdp-id:vc-id*]

statistics [**interface** *interface-name*]

Context

show>service>id>dhcp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

Displays DHCP statistics information.

Parameters

sap-id

Specifies the physical port identifier portion of the SAP definition.

sdp-id

Specifies the SDP identifier.

Values 1 to 17407

interface-name

Specifies an IP interface for which to display information.

Output

The following output is an example of DHCP statistics information, and Table 73: Output fields: DHCP statistics describes the output fields.

Sample output

```
*A:7210SAS>show>service>id>dhcp# statistics

===============================================================
DHCP Global Statistics, service 1
===============================================================
Rx Packets                          : 416554
Tx Packets                          : 206405
Rx Malformed Packets                : 0
Rx Untrusted Packets                : 0
Client Packets Discarded            : 0
Client Packets Relayed              : 221099
Client Packets Snooped              : 0
Client Packets Proxied (RADIUS)     : 0
Client Packets Proxied (Lease-Split) : 0
Server Packets Discarded            : 0
Server Packets Relayed              : 195455
Server Packets Snooped              : 0
DHCP RELEASEs Spoofed               : 0
DHCP FORCERENEWs Spoofed            : 0
===============================================================
*A:7210SAS>show>service>id>dhcp#
```

Table 73: Output fields: DHCP statistics

Label	Description
Received Packets	The number of packets received from the DHCP clients. Includes DHCP packets received from both DHCP client and DHCP server.
Transmitted Packets	The number of packets transmitted to the DHCP clients. Includes DHCP packets transmitted from both DHCP client and DHCP server.
Received Malformed Packets	The number of corrupted/invalid packets received from the DHCP clients. Includes DHCP packets received from both DHCP client and DHCP server.
Received Untrusted Packets	The number of untrusted packets received from the DHCP clients. In this case, a frame is dropped because of the client sending a DHCP packet with Option 82 filled in before "trust" is set under the DHCP interface command.
Client Packets Discarded	The number of packets received from the DHCP clients that were discarded.
Client Packets Relayed	The number of packets received from the DHCP clients that were forwarded.

Label	Description
Client Packets Snooped	The number of packets received from the DHCP clients that were snooped.
Server Packets Discarded	The number of packets received from the DHCP server that were discarded.
Server Packets Relayed	The number of packets received from the DHCP server that were forwarded.
Server Packets Snooped	The number of packets received from the DHCP server that were snooped.

summary

Syntax

summary [**interface** *interface-name*]

Context

show>service>id>dhcp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays DHCP configuration summary information.

Parameters

interface interface-name

Specifies an IP interface for which to display information.

Output

The following output is an example of summary DHCP information, and Table 74: Output fields: DHCP summary describes the output fields.

Sample output

```
A:7210SAS# show service id 1 dhcp summary
DHCP Summary, service 1
===============================================================================

Interface Name                  Arp      Used/                Info    Admin
  SapId/Sdp                     Populate Provided             Option  State
-------------------------------------------------------------------------------
egr_1                           No       0/0                  Replace Up
i_1                             No       0/0                  Replace Up
-------------------------------------------------------------------------------
Interfaces: 2
===============================================================================
```

```
*A:7210SAS>show>service>id>dhcp#
```

Table 74: Output fields: DHCP summary

Label	Description
Interface Name	Name of the router interface.
Arp Populate	Specifies whether ARP populate is enabled. 7210 SAS does not support ARP populate.
Used/Provided	7210 SAS does not maintain lease state.
Info Option	Indicates whether Option 82 processing is enabled on the interface.
Admin State	Indicates the administrative state.

5.7.2.3.2 IGMP snooping show commands

igmp-snooping

Syntax

igmp-snooping

Context

show>service>id

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

Commands in this context display IGMP snooping information.

all

Syntax

all

Context

show>service>id>igmp-snooping

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays detailed information for all aspects of IGMP snooping on the VPLS service.

Output

The following output is an example of detailed IGMP snooping information, and Table 75: Output fields: service ID IGMP snooping describes the output fields.

Sample output

```
*A:SAS-R2-043# show service id 100 igmp-snooping all

===============================================================================
IGMP Snooping info for service 100
===============================================================================

-------------------------------------------------------------------------------
IGMP Snooping Base info
-------------------------------------------------------------------------------
Admin State : Up
Querier     : 10.20.20.7 on SAP 1/1/1:100
-------------------------------------------------------------------------------
Sap/Sdp                    Oper  MRtr Send  Max  MVR       Num
Id                         State Port Qries Grps From-VPLS Grps
-------------------------------------------------------------------------------
sap:1/1/1:100              Up    Yes  No    None Local     0
sap:1/1/4:100              Up    No   No    None Local     2
sap:1/1/5                  Up    No   No    None Local     0
sap:1/1/10:100             Up    No   No    None Local     0
sap:2/1/1                  Up    No   No    None Local     0

-------------------------------------------------------------------------------
IGMP Snooping Querier info
-------------------------------------------------------------------------------
Sap Id                  : 1/1/1:100
IP Address              : 10.20.20.7
Expires                 : 254s
Up Time                 : 0d 00:26:11
Version                 : 2

General Query Interval  : 125s
Query Response Interval : 10.0s
Robust Count            : 2
-------------------------------------------------------------------------------
IGMP Snooping Multicast Routers
-------------------------------------------------------------------------------
MRouter          Sap/Sdp Id                Up Time        Expires   Version
-------------------------------------------------------------------------------
10.20.20.7       1/1/1:100                 0d 00:26:11    255s      2
-------------------------------------------------------------------------------
Number of mrouters: 1

-------------------------------------------------------------------------------
IGMP Snooping Proxy-reporting DB
-------------------------------------------------------------------------------
Group Address    Up Time
-------------------------------------------------------------------------------
239.4.4.4        0d 00:21:59
```

```
239.4.4.5        0d 00:21:53
-------------------------------------------------------------------------------
Number of groups: 2

-------------------------------------------------------------------------------
IGMP Snooping SAP 1/1/1:100 Port-DB
-------------------------------------------------------------------------------
Group Address   Type    From-VPLS  Up Time        Expires  MC
                                                  Stdby
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
Number of groups: 0

-------------------------------------------------------------------------------
IGMP Snooping SAP 1/1/4:100 Port-DB
-------------------------------------------------------------------------------
Group Address   Type    From-VPLS  Up Time        Expires  MC
                                                  Stdby
-------------------------------------------------------------------------------
239.4.4.4       static  local      0d 00:21:59    never
239.4.4.5       static  local      0d 00:21:53    never
-------------------------------------------------------------------------------
Number of groups: 2
-------------------------------------------------------------------------------
IGMP Snooping SAP 1/1/5 Port-DB
-------------------------------------------------------------------------------
Group Address   Type    From-VPLS  Up Time        Expires  MC
                                                  Stdby
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
Number of groups: 0

-------------------------------------------------------------------------------
IGMP Snooping SAP 1/1/10:100 Port-DB
-------------------------------------------------------------------------------
Group Address   Type    From-VPLS  Up Time        Expires  MC
                                                  Stdby
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
Number of groups: 0

-------------------------------------------------------------------------------
IGMP Snooping SAP 2/1/1 Port-DB
-------------------------------------------------------------------------------
Group Address   Type    From-VPLS  Up Time        Expires  MC
                                                  Stdby
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
Number of groups: 0
-------------------------------------------------------------------------------
IGMP Snooping Static Groups
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
IGMP Snooping Static Groups for SAP 1/1/4:100
-------------------------------------------------------------------------------
Group
-------------------------------------------------------------------------------
239.4.4.4
239.4.4.5
-------------------------------------------------------------------------------
Static (*,G) entries: 2

-------------------------------------------------------------------------------
IGMP Snooping Statistics
```

```
-------------------------------------------------------------------------------
Message Type            Received      Transmitted   Forwarded
-------------------------------------------------------------------------------
General Queries         1269          0             5075
Group Queries           0             0             0
V1 Reports              0             0             0
V2 Reports              0             464           0
V2 Leaves               0             0             0
Unknown Type            0             N/A           0
-------------------------------------------------------------------------------
Drop Statistics
Bad Length               : 0
Bad IP Checksum          : 0
Bad IGMP Checksum        : 0
Bad Encoding             : 0
No Router Alert          : 0
Zero Source IP           : 0
Wrong Version            : 0
Lcl-Scope Packets        : 0

Send Query Cfg Drops     : 0
Import Policy Drops      : 0
Exceeded Max Num Groups  : 0
MCS Failures             : 0

MVR From VPLS Cfg Drops  : 0
MVR To SAP Cfg Drops     : 0

-------------------------------------------------------------------------------
IGMP Snooping Multicast VPLS Registration info
-------------------------------------------------------------------------------
IGMP Snooping Admin State : Up

MVR Admin State           : Down
MVR Policy                : None
-------------------------------------------------------------------------------
Local SAPs/SDPs
-------------------------------------------------------------------------------
Svc Id     Sap/Sdp                   Oper      From       Num Local
           Id                        State     VPLS       Groups
-------------------------------------------------------------------------------
100        sap:1/1/1:100             Up        Local      0
100        sap:1/1/4:100             Up        Local      2
100        sap:1/1/5                 Up        Local      0
100        sap:1/1/10:100            Up        Local      0
100        sap:2/1/1                 Up        Local      0
-------------------------------------------------------------------------------
MVR SAPs (from-vpls=100)
-------------------------------------------------------------------------------
Svc Id     Sap/Sdp                   Oper      From       Num MVR
           Id                        State     VPLS       Groups
-------------------------------------------------------------------------------
No MVR SAPs found.
===============================================================================
*A:SAS-R2-043#
```

Table 75: Output fields: service ID IGMP snooping

Label	Description
Admin State	The administrative state of the IGMP instance.

Label	Description
Querier	Displays the address of the IGMP querier on the IP subnet to which the interface is attached.
Sap or SDP Id	Displays the SAP or SDP IDs of the service ID.
Oper State	Displays the operational state of the SAP or SDP IDs of the service ID.
Mrtr Port	Specifies if the port is a multicast router port.
Send Queries	Specifies whether the send-queries command is enabled or disabled.
Max Num Groups	Specifies the maximum number of multicast groups that can be joined on this SAP or SDP.
MVR From VPLS	Specifies MVR from VPLS.
Num MVR Groups	Specifies the actual number of multicast groups that can be joined on this SAP or SDP.
MVR From VPLS Cfg Drops	Displays the from VPLS drop count.
MVR To SAP Cfg Drops	Displays the to SAP drop count.
MVR Admin State	Displays the administrative state of MVR.
MVR Policy	The MVR policy name.

mfib

Syntax

mfib [**brief**] [**ip** | **mac**] **brief**

mfib [**group** *grp-address*]

Context

show>service>id

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays the multicast FIB on the VPLS service.

Parameters

brief

Keyword to display a brief output.

group grp *grp-address*

Specifies a specific multicast group address for which to displays the FIB.

Output

The following output is an example of multicast FIB information, and Table 76: Output fields: service ID MFIB describes the output fields.

Sample output

```
*A:SAS# show service id 1 mfib

===============================================================================
Multicast FIB, Service 1
===============================================================================
Group Address         Sap/Sdp Id              Svc Id   Fwd/Blk
-------------------------------------------------------------------------------
239.4.4.4             sap:1/1/1               Local    Fwd
-------------------------------------------------------------------------------
Number of entries: 1
===============================================================================
A:7210-SAS>show>service>id#
```

Table 76: Output fields: service ID MFIB

Label	Description
Group Address	IPv4 multicast group address.
SAP ID	Indicates the SAP or SDP to which the corresponding multicast stream is forwarded or blocked.
Forwarding/Blocking	Indicates whether the corresponding multicast stream is blocked or forwarded.
Number of Entries	Specifies the number of entries in the MFIB.
Forwarded Packets	Indicates the number of multicast packets forwarded for the corresponding source or group.
Forwarded Octets	Indicates the number of octets forwarded for the corresponding source or group.
Svc ID	Indicates the service to which the corresponding multicast stream is forwarded or blocked. Local means that the multicast stream is forwarded or blocked to a SAP or SDP local to the service.

mrouters

Syntax

mrouters [**detail**]

Context

show>service>id>igmp-snooping

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays all multicast routers.

Parameters

detail

Keyword to display detailed information.

Output

The following output is an example of multicast router information.

Sample output

```
A:7210-SAS>show>service>id>igmp-snooping# mrouters

===============================================================================
IGMP Snooping Multicast Routers for service 1
===============================================================================
MRouter          Sap/Sdp Id             Up Time        Expires   Version
-------------------------------------------------------------------------------
10.1.1.1         1/1/2                  0d 18:31:30    254s      2
-------------------------------------------------------------------------------
Number of mrouters: 1
===============================================================================
A:7210-SAS>show>service>id>igmp-snooping#
```

mvr

Syntax

mvr

Context

show>service>id>igmp-snooping

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays Multicast VPLS Registration (MVR) information.

Output

The following output is an example of IGMP snooping MVR information, and Table 77: Output fields: IGMP-snooping MVR describes the fields.

Sample output

```
A:ALA-1>show>service>id>snooping# mvr
===============================================================================
IGMP Snooping Multicast VPLS Registration info for service 10
===============================================================================
IGMP Snooping Admin State : Up

MVR Admin State           : Up
MVR Policy                : mvr-policy
-------------------------------------------------------------------------------
Local SAPs/SDPs
-------------------------------------------------------------------------------
Svc Id     Sap/Sdp                Oper      From       Num Local
           Id                     State     VPLS       Groups
-------------------------------------------------------------------------------
100         sap:1/1/10:10         Up       Local      100
100         sap:1/1/10:20         Up       Local      100
-------------------------------------------------------------------------------
MVR SAPs (from-vpls=10)
-------------------------------------------------------------------------------
Svc Id     Sap/Sdp                Oper      From       Num MVR
           Id                     State     VPLS       Groups
-------------------------------------------------------------------------------
20         sap:1/1/4:100          Up        10         100
30         sap:1/1/31:10.10       Up        10         100
===============================================================================
A:ALA-1>show>service>id>snooping#
```

Table 77: Output fields: IGMP-snooping MVR

Label	Description
IGMP Snooping Admin State	Displays the IGMP snooping administrative state.
MVR Admin State	Displays the MVR administrative state.
MVR Policy	Displays the MVR policy name.
Svc ID	Displays the service ID.
Sap/SDP	Displays the SAP or SDP ID.
Oper State	Displays the operational state.
From VPLS	Displays the originating VPLS name.
Num Local Groups	Displays the number of local groups.

port-db

Syntax

port-db sap *sap-id* [**detail**]

port-db sap *sap-id* **group** *grp-address*

port-db sdp *sdp-id*:*vc-id* [**detail**]

port-db sdp *sdp-id*:*vc-id* **group** *grp-address*

Context

show>service>id>igmp-snooping

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays information about the IGMP snooping port database for the VPLS service.

Parameters

group *grp-ip-address*

Displays the IGMP snooping port database for a specific multicast group address.

sap *sap-id*

Displays the IGMP snooping port database for a specific SAP. See Common CLI command descriptions for command syntax.

sdp *sdp-id*

Displays only IGMP snooping entries associated with the specified mesh SDP or spoke-SDP. For a spoke-SDP, the VC ID must be specified, for a mesh SDP, the VC ID is optional.

Values 1 to 17407

vc-id

Specifies the virtual circuit ID on the SDP ID for which to display information.

Default For mesh SDPs only, all VC IDs.

Values 1 to 4294967295

Output

The following output is an example of port database information, and Table 78: Output fields: IGMP snooping port DB describes the output fields.

Sample output

```
*A:MTU-T2#  show service id 100 igmp-snooping port-db sap 1/1/2 detail
===============================================================================
```

```
IGMP Snooping SAP 1/1/2 Port-DB for service 100
===============================================================================
-------------------------------------------------------------------------------
IGMP Group 239.7.7.7
-------------------------------------------------------------------------------
Type             : dynamic
Up Time          : 0d 00:06:17          Expires          : 30s
Compat Mode      : IGMP Version 2
V1 Host Expires  : 0s                   V2 Host Expires  : 30s
-------------------------------------------------------------------------------
IGMP Group 239.7.7.8
-------------------------------------------------------------------------------
Type             : dynamic
Up Time          : 0d 00:06:17          Expires          : 30s
Compat Mode      : IGMP Version 2
V1 Host Expires  : 0s                   V2 Host Expires  : 30s
-------------------------------------------------------------------------------
IGMP Group 239.8.8.8
-------------------------------------------------------------------------------
Type             : static
Up Time          : 0d 00:04:29          Expires          : never
Compat Mode      : IGMP Version 2
V1 Host Expires  : 0s                   V2 Host Expires  : 0s
-------------------------------------------------------------------------------
Number of groups: 3
===============================================================================
*A:MTU-7210#
```

Table 78: Output fields: IGMP snooping port DB

Label	Description
Group Address	The IP multicast group address for which this entry contains information.
Mode	Specifies the type of membership reports received on the interface for the group. In the include mode, reception of packets sent to the specified multicast address is requested only from those IP source addresses listed in the source-list parameter of the IGMP membership report. In the exclude mode, reception of packets sent to the specific multicast address is requested from all IP source addresses except those listed in the source-list parameter.
Type	Indicates how this group entry was learned. If this group entry was learned by IGMP, the value is set to dynamic. For statically configured groups, the value is set to static.
Compatibility mode	Specifies the IGMP mode. This is used in order for routers to be compatible with earlier version routers. IGMPv3 hosts must operate in Version 1 and Version 2 compatibility modes. IGMPv3 hosts must keep state per local interface based on the compatibility

Label	Description
	mode of each attached network. A host's compatibility mode is determined from the host compatibility mode variable which can be in one of three states: IGMPv1, IGMPv2 or IGMPv3. This variable is kept per interface and is dependent on the version of general queries heard on that interface as well as the earlier VERSION querier present timers for the interface.
V1 host expires	The time remaining until the local router assumes that there are no longer any IGMPv1 members on the IP subnet attached to this interface. Upon hearing any IGMPv1 membership report, this value is reset to the group membership timer. While this time remaining is non-zero, the local router ignores any IGMPv2 leave messages for this group that it receives on this interface.
V2 host expires	The time remaining until the local router assumes that there are no longer any IGMPv2 members on the IP subnet attached to this interface. Upon hearing any IGMPv2 membership report, this value is reset to the group membership timer. While this time remaining is non-zero, the local router ignores any IGMPv3 leave messages for this group that it receives on this interface.
Up Time	The time after the source group entry was created.
Expires	The amount of time remaining before this entry is aged out.
Forwarding/Blocking	Indicates whether this entry is on the forward list or block list.
Number of groups	Indicates the number of groups configured for this SAP.

proxy-db

Syntax

proxy-db [**detail**]

proxy-db group *grp-address*

Context

show>service>id>igmp-snooping

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays information about the IGMP snooping proxy reporting database for the VPLS service.

Parameters

group *grp-ip-address*

Displays the IGMP snooping proxy reporting database for a specific multicast group address.

Output

The following output is an example of proxy database information, and Table 79: Output fields: IGMP snooping proxy DB describes the output fields.

Sample output

```
*A:MTU-7210#  show service id 100 igmp-snooping proxy-db
===============================================================================
IGMP Snooping Proxy-reporting DB for service 100
===============================================================================
Group Address    Up Time
-------------------------------------------------------------------------------
239.7.7.7        0d 00:05:30
239.7.7.8        0d 00:05:30
239.8.8.8        0d 00:03:42
-------------------------------------------------------------------------------
Number of groups: 3
===============================================================================
*A:MTU-7210#


*A:MTU-T2#  show service id 100 igmp-snooping proxy-db detail
===============================================================================
IGMP Snooping Proxy-reporting DB for service 100
===============================================================================
-------------------------------------------------------------------------------
IGMP Group 239.7.7.7
-------------------------------------------------------------------------------
Up Time : 0d 00:05:43
-------------------------------------------------------------------------------
IGMP Group 239.7.7.8
-------------------------------------------------------------------------------
Up Time : 0d 00:05:43
-------------------------------------------------------------------------------
IGMP Group 239.8.8.8
-------------------------------------------------------------------------------
Up Time : 0d 00:03:55
-------------------------------------------------------------------------------
Number of groups: 3
===============================================================================
*A:MTU-7210#
```

Table 79: Output fields: IGMP snooping proxy DB

Label	Description
Group Address	The IP multicast group address for which this entry contains information.
Mode	Specifies the type of membership reports received on the interface for the group. In the include mode, reception of packets sent to the specified multicast address is requested

Label	Description
	only from those IP source addresses listed in the source-list parameter of the IGMP membership report.
	In the exclude mode, reception of packets sent to the specific multicast address is requested from all IP source addresses except those listed in the source-list parameter.
Up Time	The total operational time in seconds.
Number of groups	Number of IGMP groups.

querier

Syntax

querier

Context

show>service>id>igmp-snooping

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays information about the IGMP snooping queries for the VPLS service.

Output

The following output is an example of IGMP snooping querier information, and Table 80: Output fields: IGMP snooping querier describes the output fields.

Sample output

```
*A:MTU-7210#  show service id 100 igmp-snooping querier
===============================================================================
IGMP Snooping Querier info for service 100
===============================================================================
Sap Id                  : 1/1/1
IP Address              : 10.10.9.9
Expires                 : 24s
Up Time                 : 0d 00:05:20
Version                 : 2

General Query Interval  : 10s
Query Response Interval : 10.0s
Robust Count            : 2
===============================================================================
*A:MTU-7210#


*A:MTU-T2#  show service id 100 igmp-snooping proxy-db
===============================================================================
```

```
IGMP Snooping Proxy-reporting DB for service 100
===============================================================================
Group Address    Up Time
-------------------------------------------------------------------------------
239.7.7.7        0d 00:05:30
239.7.7.8        0d 00:05:30
239.8.8.8        0d 00:03:42
-------------------------------------------------------------------------------
Number of groups: 3
===============================================================================
*A:MTU-T2#
```

Table 80: Output fields: IGMP snooping querier

Label	Description
SAP Id	Specifies the SAP ID of the service.
IP address	Specifies the IP address of the querier.
Expires	The time left, in seconds, until the query expires.
Up time	The length of time the query has been enabled.
Version	The configured version of IGMP.
General Query Interval	The frequency at which host-query packets are transmitted.
Query Response Interval	The time to wait to receive a response to the host-query message from the host.
Robust Count	Specifies the value used to calculate several IGMP message intervals.

static

Syntax

static [**sap** *sap-id* | **sdp** *sdp-id:vc-id*]

Context

show>service>id>igmp-snooping

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays information about static IGMP snooping source groups for the VPLS service.

Parameters

sap *sap-id*

Displays static IGMP snooping source groups for a specific SAP. See Common CLI command descriptions for command syntax.

sdp *sdp-id*

Displays the IGMP snooping source groups for a specific spoke or mesh SDP.

Values 1 to 17407

vc-id

Specifies the virtual circuit ID on the SDP ID for which to display information.

Default For mesh SDPs only, all VC IDs.

Values 1 to 4294967295

Output

The following output is an example of static IGMP snooping information, and Table 81: Output fields: IGMP snooping static describes the output fields.

Sample output

```
*A:MTU-7210#  show service id 100 igmp-snooping static

===============================================================================
IGMP Snooping Static Groups for service 100
===============================================================================
-------------------------------------------------------------------------------
IGMP Snooping Static Groups for SAP 1/1/2
-------------------------------------------------------------------------------
Group
-------------------------------------------------------------------------------
239.8.8.8
-------------------------------------------------------------------------------
Static (*,G) entries: 1
===============================================================================
*A:MTU-7210#
```

Table 81: Output fields: IGMP snooping static

Label	Description
Source	Displays the IP source address used in IGMP queries.
Group	Displays the static IGMP snooping source groups for a specified SAP.

statistics

Syntax

statistics [**sap** *sap-id* | **sdp** *sdp-id:vc-id*]

Context

show>service>id>igmp-snooping

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays IGMP snooping statistics for the VPLS service.

Parameters

sap *sap-id*

Displays IGMP snooping statistics for a specific SAP. See Common CLI command descriptions for command syntax.

sdp *sdp-id*

Displays the IGMP snooping statistics for a specific spoke or mesh SDP.

Values 1 to 17407

vc-id

Specifies the virtual circuit ID on the SDP ID for which to display information.

Default For mesh SDPs only, all VC IDs.

Values 1 to 4294967295

Output

The following output is an example of IGMP snooping statistics, and Table 82: Output fields: service-ID IGMP statistics describes the output fields.

Sample output

```
A:7210-SAS>show>service>id>igmp-snooping# statistics

===============================================================================
IGMP Snooping Statistics for service 1
===============================================================================
Message Type            Received      Transmitted   Forwarded
-------------------------------------------------------------------------------
General Queries         1987001       0             1987001
Group Queries           0             0             0
V1 Reports              0             0             0
V2 Reports              1987002       13200         0
V2 Leaves               0             0             0
Unknown Type            0             N/A           0
-------------------------------------------------------------------------------
Drop Statistics
-------------------------------------------------------------------------------
Bad Length               : 0
Bad IP Checksum          : 0
Bad IGMP Checksum        : 0
Bad Encoding             : 0
No Router Alert          : 0
Zero Source IP           : 0
```

```
Wrong Version            : 0
Lcl-Scope Packets        : 0

Send Query Cfg Drops     : 0
Import Policy Drops      : 0
Exceeded Max Num Groups  : 0
MCS Failures             : 0
===============================================================================
A:7210-SAS>show>service>id>igmp-snooping#
```

Table 82: Output fields: service-ID IGMP statistics

Label	Description
Message Type	The column heading for IGMP snooping messages.
General Queries	The number of general query messages received, transmitted, and forwarded.
Group Queries	The number of group query messages received, transmitted, and forwarded.
Group-Source Queries	The number of group-source query messages received, transmitted, and forwarded.
V1 Reports	The number of IGMPv1 report messages received, transmitted, and forwarded.
V2 Reports	The number of IGMPv2 report messages received, transmitted, and forwarded.
V2 Leaves	The number of IGMP leave messages received, transmitted, and forwarded.
Unknown Type	The number of unknown type messages received, transmitted, and forwarded.
Drop Statistics	
Bad Length	The number of packets dropped because of bad length.
Bad IP Checksum	The number of packets dropped because of a bad IP checksum.
Bad IGMP Checksum	The number of packets dropped because of a bad IGMP checksum.
Bad Encoding	The number of packets dropped because of bad encoding.
No Router Alert	The number of packets dropped because there was no router alert.
Zero Source IP	The number of packets dropped because of a source IP address of 0.0.0.0 or 00:00:00:00:00:00:00:00.

Label	Description
Send Query Cfg Drops	The number of messages dropped because of send query configuration errors.
Import Policy Drops	The number of messages dropped because of import policy.
Exceeded Max Num Groups	The number of packets dropped because the maximum number of groups has been exceeded.
MVR From VPLS Cfg Drops	The number of packets dropped because of VPLS configuration multicast VPLS registration (MVR).
MVR To SAP Cfg Drops	The number of packets dropped because of SAP configuration.

endpoint

Syntax

endpoint [*endpoint-name*]

Context

show>service>id

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays service endpoint information.

Parameters

endpoint-name

Specifies an endpoint name created in the **config>service>vpls** context.

Output

The following output is an example of endpoint information, and Table 83: Output fields: service-ID endpoint describes the output fields.

Sample output

```
*A:Dut-B# show service id 1 endpoint
===============================================================================
Service 1 endpoints
===============================================================================
Endpoint name               : mcep-t1
Description                 : (Not Specified)
Revert time                 : 0
Act Hold Delay              : 0
```

```
Ignore Standby Signaling     : false
Suppress Standby Signaling   : false
Block On Mesh Fail           : true
Psv Mode Active              : No
Tx Active                    : 231:1
Tx Active Up Time            : 0d 00:06:57
Revert Time Count Down       : N/A
Tx Active Change Count       : 5
Last Tx Active Change        : 02/13/2009 22:08:33
-------------------------------------------------------------------------------
Members
-------------------------------------------------------------------------------
Spoke-sdp: 221:1 Prec:1                          Oper Status: Up
Spoke-sdp: 231:1 Prec:2                          Oper Status: Up
===============================================================================
*A:Dut-B#
```

Table 83: Output fields: service-ID endpoint

Label	Description
Endpoint name	The name of the endpoint.
Description	A description of the endpoint.
Revert time	The programmable time delay to switch back to the primary spoke SDP.
Act Hold Delay	Not applicable.
Ignore Standby Signaling	Specifies whether ignore standby signaling is configured. True — standby signaling is ignored False — standby signaling is not ignored
Suppress Standby Signaling	Specifies whether suppress standby signaling is configured. True — standby signaling is suppressed False — standby signaling is not suppressed
Block On Mesh Fail	Specifies whether to take down the spoke SDP when the mesh SDP is down. True — the spoke SDP is not taken down False — the spoke SDP is taken down
Tx Active	The identifier of the active spoke SDP.
Tx Active Up Time	The total amount of time that a spoke SDP remains the active spoke SDP.
Revert Time Count Down	The amount of time remaining before active transmission reverts to the primary spoke SDP.

Label	Description
Tx Active Change Count	The number of times that the active spoke SDP has changed.
Last Tx Active Change	The timestamp of the last active spoke SDP change.
Members	
Spoke-sdp	Identifies the spoke SDP.
Prec	Specifies the precedence of this SDP binding when there are multiple SDP bindings attached to one service endpoint.
Oper Status	Indicates the operational status of the endpoint.

5.7.2.4 Clear commands

id

Syntax

id *service-id*

Context

clear>service

clear>service>statistics

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command clears commands for a specific service.

Parameters

service-id

Specifies the ID that uniquely identifies a service.

Values *service-id*: 1 to 214748364 *svc-name*: A string up to 64 characters.

statistics

Syntax

statistics

Context

clear>service>stats

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command clears session statistics for this service.

fdb

Syntax

fdb {**all** | **mac** *ieee-address* | **sap** *sap-id*] | **mesh-sdp** *sdp-id*[**:***vc-id*] | **spoke-sdp** *sdp-id*:*vc-id*}

Context

clear>service>id

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command clears FDB entries for the service.

Parameters

all

Clears all FDB entries.

mac *ieee-address*

Clears only FDB entries in the FDB table with the specified 48-bit MAC address. The MAC address can be expressed in the form *aa*:*bb*:*cc*:*dd*:*ee*:*ff* or *aa-bb-cc-dd-ee-ff* where *aa*, *bb*, *cc*, *dd*, *ee* and *ff* are hexadecimal numbers.

sap-id

Specifies the physical port identifier portion of the SAP definition. See Common CLI command descriptions for command syntax.

mesh-sdp

Clears only service FDB entries associated with the specified mesh SDP ID. For a mesh SDP, the VC ID is optional.

spoke-sdp

Clears only service FDB entries associated with the specified spoke-SDP ID. For a spoke-SDP, the VC ID must be specified.

sdp-id

Specifies the SDP ID for which to clear associated FDB entries.

vc-id

Specifies the virtual circuit ID on the SDP ID for which to clear associated FDB entries.

Values *sdp-id*[:*vc-id*] *sdp-id*: 1 to 17407
vc-id: 1 to 4294967295
sdp-id:vc-id sdp-id: 1 to 17407
vc-id: 1 to 4294967295

mesh-sdp

Syntax

mesh-sdp *sdp-id*[**:***vc-id*] **ingress-vc-label**

Context

clear>service>id

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command clears and resets the mesh SDP bindings for the service.

Parameters

sdp-id

Specifies the mesh SDP ID to be reset.

Values 1 to 17407

vc-id

Specifies the virtual circuit ID on the SDP ID to be reset.

Default All VC IDs on the SDP ID.

Values 1 to 4294967295

spoke-sdp

Syntax

spoke-sdp *sdp-id*[*:vc-id*] {**all** | **counters** | **stp** | **l2pt**}}

Context

clear>service>id

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command clears and resets the spoke-SDP bindings for the service.

Parameters

sdp-id

Specifies the spoke-SDP ID to be reset.

Values 1 to 17407

vc-id

Specifies the virtual circuit ID on the SDP ID to be reset.

Values 1 to 4294967295

all

Clears all queue statistics and STP statistics associated with the SDP.

counters

Clears all queue statistics associated with the SDP.

stp

Clears all STP statistics associated with the SDP.

l2pt

Clears all L2PT statistics associated with the SDP.

sap

Syntax

sap *sap-id*

Context

clear>service>statistics

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command clears statistics for the SAP bound to the service.

Parameters

sap-id

Clears statistics for a specified SAP. See Common CLI command descriptions for command syntax.

all

Clears all queue statistics and STP statistics associated with the SAP.

counters

Clears all queue statistics associated with the SAP.

counters

Syntax

counters

Context

clear>service>statistics>id

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command clears all traffic queue counters associated with the service ID.

l2pt

Syntax

l2pt

Context

clear>service>statistics>id

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command clears the l2pt statistics for this service.

mesh-sdp

Syntax

mesh-sdp *sdp-id*[*:vc-id*] {**all** | **counters** | **stp** | **mrp**}

Context

clear>service>statistics>id

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command clears the statistics for a particular mesh SDP bind.

Parameters

sdp-id

Specifies the mesh SDP ID for which to clear statistics.

Values 1 to 17407

vc-id

Specifies the virtual circuit ID on the mesh SDP ID to be reset.

Values 1 to 4294967295

all

Clears all queue statistics and STP statistics associated with the SDP.

counters

Clears all queue statistics associated with the SDP.

stp

Clears all STP statistics associated with the SDP.

mrp

Clears all MRP statistics associated with the SDP.

spoke-sdp

Syntax

spoke-sdp *sdp-id*[**:***vc-id*] {**all** | **counters** | **stp**| **l2pt**}

Context

clear>service>statistics>id

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command clears statistics for the spoke-SDP bound to the service.

Parameters

sdp-id

Specifies the spoke-SDP ID for which to clear statistics.

Values 1 to 17407

vc-id

Specifies the virtual circuit ID on the SDP ID to be reset.

Values 1 to 4294967295

all

Clears all queue statistics and STP statistics associated with the SDP.

counters

Clears all queue statistics associated with the SDP.

stp

Clears all STP statistics associated with the SDP.

l2pt

Clears all L2PT statistics associated with the SDP.

stp

Syntax

stp

Context

clear>service>statistics>id

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command clears all STP statistics for the service ID.

detected-protocols

Syntax

detected-protocols {**all** | **sap** *sap-id*}

Context

clear>service>id>stp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

RSTP automatically falls back to STP mode when it receives an STP BPDU. The **clear detected-protocols** command forces the system to revert to the default RSTP mode on the SAP.

Parameters

all

Clears all detected protocol statistics.

sap-id

Clears the specified lease state SAP information. See Common CLI command descriptions for command syntax.

igmp-snooping

Syntax

igmp-snooping

Context

clear>service>id

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

Commands in this context clear IGMP snooping data.

port-db

Syntax

port-db [**sap** *sap-id*] [**group** *grp-address*]

port-db sdp *sdp-id:vc-id* [**group** *grp-address*]

Context

clear>service>id>igmp-snooping

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command clears the information about the IGMP snooping port database for the VPLS service.

Parameters

sap *sap-id*

Clears IGMP snooping statistics matching the specified SAP ID and optional encapsulation value. See Common CLI command descriptions for command syntax.

sdp-id

Clears only IGMP snooping entries associated with the specified mesh SDP or spoke-SDP. For a spoke-SDP, the VC ID must be specified, for a mesh SDP, the VC ID is optional.

Values 1 to 17407

vc-id

Specifies the virtual circuit ID on the SDP ID for which to clear information.

Default For mesh SDPs only, all VC IDs.

Values 1 to 4294967295

group *grp-address*

Clears IGMP snooping statistics matching the specified group address.

querier

Syntax

querier

Context

clear>service>id>igmp-snooping

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command clears the information about the IGMP snooping queries for the VPLS service.

5.7.2.5 Debug commands

id

Syntax

id *service-id*

Context

debug>service

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command debugs commands for a specific service.

Parameters

service-id

Specifies the ID that uniquely identifies a service.

Values *service-id*: 1 to 214748364 *svc-name*: A string up to 64 characters.

event-type

Syntax

[**no**] **event-type** {**config-change** | **svc-oper-status-change** | **sap-oper-status-change** | **sdpbind-oper-status-change**}

Context

debug>service>id

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables a particular debugging event type. The **no** form of this command disables the event type debugging.

Parameters

config-change

Debugs configuration change events.

svc-oper-status-change

Debugs service operational status changes.

sap-oper-status-change

Debugs SAP operational status changes.

sdpbind-oper-status-change

Debugs SDP operational status changes.

sap

Syntax

[**no**] **sap** *sap-id*

Context

debug>service>id

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables debugging for a particular SAP.

Parameters

sap-id

Specifies the SAP ID.

stp

Syntax

stp

Context

debug>service>id

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables the context for debugging STP.

all-events

Syntax

all-events

Context

debug>service>id>stp

Platforms
Supported on all 7210 SAS platforms as described in this document

Description
This command enables STP debugging for all events.

bpdu

Syntax
[**no**] **bpdu**

Context
debug>service>id>stp

Platforms
Supported on all 7210 SAS platforms as described in this document

Description
This command enables STP debugging for received and transmitted BPDUs.

core-connectivity

Syntax
[**no**] **core-connectivity**

Context
debug>service>id>stp

Platforms
Supported on all 7210 SAS platforms as described in this document

Description
This command enables STP debugging for core connectivity.

exception

Syntax
[**no**] **exception**

Context
debug>service>id>stp

Platforms
Supported on all 7210 SAS platforms as described in this document

Description
This command enables STP debugging for exceptions.

fsm-state-changes

Syntax
[**no**] **fsm-state-changes**

Context
debug>service>id>stp

Platforms
Supported on all 7210 SAS platforms as described in this document

Description
This command enables STP debugging for FSM state changes.

fsm-timers

Syntax
[**no**] **fsm-timers**

Context
debug>service>id>stp

Platforms
Supported on all 7210 SAS platforms as described in this document

Description
This command enables STP debugging for FSM timer changes.

port-role

Syntax
[**no**] **port-role**

Context
debug>service>id>stp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables STP debugging for changes in port roles.

port-state

Syntax

[**no**] **port-state**

Context

debug>service>id>stp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables STP debugging for port states.

sap

Syntax

[**no**] **sap** *sap-id*

Context

debug>service>id>stp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables STP debugging for a specific SAP.

Parameters

sap-id

Specifies the physical port identifier portion of the SAP definition. See Common CLI command descriptions for command syntax.

sdp

Syntax

[**no**] **sdp** *sdp-id:vc-id*

Context

debug>service>stp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables STP debugging for a specific SDP.

6 Internet Enhanced Service

This chapter provides information about Internet Enhanced Services the process overview, and implementation notes.

6.1 IES service overview

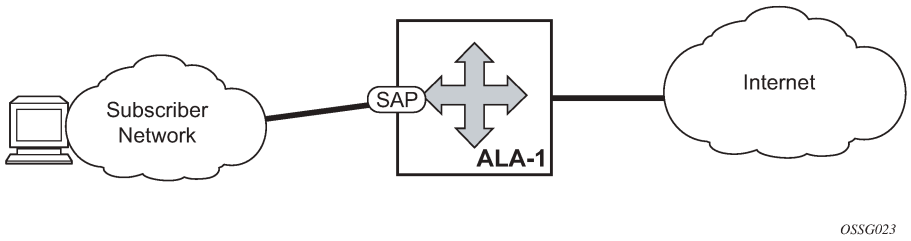
Internet Enhanced Service (IES) is a routed connectivity service where the subscriber communicates with an IP router interface to send and receive Internet traffic. An IES has one or more logical IP routing interfaces each with a SAP which acts as the access point to the subscriber network.

IES allows IP interfaces to participate in the same routing instance used for service network core routing connectivity. IES services require that the IP addressing scheme used by the subscriber be unique between other provider addressing schemes and potentially the entire Internet. While IES is part of the routing domain, the usable IP address space may be limited. This allows a portion of the service provider address space to be reserved for service IP provisioning, and be administered by a separate, but subordinate address authority.

IP interfaces defined within the context of an IES service must have a SAP associated as the uplink access point to the subscriber network. Multiple IES services are created to segregate subscriber owned IP interfaces.

The following figure shows Internet enhanced service.

Figure 66: Internet Enhanced Service



The IES service provides in-band management connectivity. Other features include:

- Multiple IES services are created to separate IP interfaces.
- More than one IES service can be created for a single customer ID.
- More than one IP interface can be created within a single IES service ID. All IP interfaces created within an IES service ID belong to the same customer.

6.2 IES features

This section describes various general service features and any special capabilities or considerations as they relate to IES services.

6.2.1 IP interfaces

IES customer IP interfaces can be configured with most of the options found on the core IP interfaces. The advanced configuration options supported are:

- VRRP - for IES services with more than one IP interface
- Secondary IP addresses
- ICMP Options

NTP broadcase receipt configuration options found on core IP interfaces are not supported on IES IP interfaces.

6.2.2 IPv6 support for IES IP interfaces (in network mode)

IES IPv6 IP interfaces provide IPv6 connectivity in the routing base instance. It can be used to connect IPv6 networks over an IPv4 cloud using 6PE mechanisms. For more information about the 6PE, see the *7210 SAS-Mxp, R6, R12, S, Sx, T Router Configuration Guide*.

IPv4 and IPv6 route table lookup entries are shared. Before adding routes for IPv6 destinations, route entries in the routed lookup table needs to be allocated for IPv6 addresses. This can be done using the CLI command **configure>system>resource-profile>router max-ipv6-routes** and **configure>system>global-res-profile>max-ipv6-routes** for 7210 SAS-R6 and 7210 SAS-R12. This command allocates route entries for /64 IPv6 prefix route lookups. The system does not allocate any IPv6 route entries by default and user needs to allocate some resources before using IPv6. For the command to take effect the node must be rebooted after making the change. For more information, see the following example and the *7210 SAS-Mxp, R6, R12, S, Sx, T Basic System Configuration Guide*.

A separate route table (or a block in the route table) is used for IPv6 /128-bit prefix route lookup. A limited amount of IPv6 /128 prefixes route lookup entries is supported. The software enables lookups in this table by default (that is, no user configuration is required to enable IPv6 /128-bit route lookup).

In addition, the number IP subnets can be configured by the user using the command **configure>system>resource-profile>router>max-ip-subnets** and **configure>system>global-res-profile>max-ip-subnet** for 7210 SAS-R6 and 7210 SAS-R12. Suitable default are assigned to this parameter. Users can increase the number of subnets if they plan to more IPv6 addresses per IPv6 interface.

Following features and restrictions is applicable for IPv6 IES IP interfaces:

- IPv6 interfaces supports static routing, OSPv3, and IS-IS.
- A limited amount of IPv6 /128 prefixes route lookup entries is supported on 7210 SAS platforms.

6.3 SAPs

This section provides information about SAPs on IES services.

6.3.1 Encapsulations

The following SAP encapsulation is supported on IES services.

- Ethernet null
- Ethernet dot1q
- Ethernet QinQ

6.3.2 Routing protocols

IES IP interfaces are restricted to routing protocols that can be configured on the interface. IES IP interfaces support the following routing protocols:

- OSPF
- IS-IS
- eBGP for the IPv4 and IPv6 address families (MPBGP is not supported)
- IGMP
- PIM
- BFD

Note: The SAP for the IES IP interface is created at the IES service level, but the routing protocols for the IES IP interface are configured at the routing protocol level for the main router instance.

6.3.2.1 CPE connectivity check

Static routes are used within many IES services. Unlike dynamic routing protocols, there is no way to change the state of routes based on availability information for the associated CPE. CPE connectivity check adds flexibility so that unavailable destinations are removed from the service provider routing tables dynamically and minimize wasted bandwidth.

The availability of the far-end static route is monitored through periodic polling. The polling period is configured. If the poll fails a specified number of sequential polls, the static route is marked as inactive.

An ICMP ping mechanism is used to test the connectivity. If the connectivity check fails and the static route is de-activated, the router continues to send polls and reactivate any routes that are restored.

6.3.3 QoS policies

When applied to 7210 SAS IES services, service ingress QoS policies only create the unicast meters defined in the policy. The multipoint meters are not created on the service. With IES services, service egress QoS policies function as with other services where the class-based queues are created as defined in the policy.

On 7210 SAS ingress, only meters are supported on all the platforms.

Note: QoS policies only create the unicast meters defined in the policy if PIM is not configured on the associated IP interface; if PIM is configured, the multipoint meters are applied as well.

Both MAC and IPv4 criteria can be used in the QoS policies for traffic classification in an IES.

6.3.3.1 CPU QoS for IES access interfaces in network mode

Traffic bound to CPU received on IES access interfaces are policed/rate-limited and queued into CPU queues. The software allocates a policer per IP application or a set of IP applications, for rate-limiting CPU bound IP traffic from all IES access SAPs. The policers CIR/PIR values are set to appropriate values based on feature scaling and these values are not user configurable. The software allocates a set of queues for CPU bound IP traffic from all IES access SAPs. The queues are either shared by a set of IP applications or in some cases allocated to an IP application. The queues are shaped to appropriate rate based on feature scaling. The shaper rate is not user-configurable.

Note:

- The instance of queues and policers used for traffic received on network port IP interfaces is different for traffic received from access port IP interfaces. Additionally the network CPU queues receive higher priority than the access CPU queues. This is done to provide better security and mitigate the risk of access traffic affecting the network side.
- On the 7210 SAS-R6, the user can configure the IP DSCP value for self-generated traffic.

6.3.4 Filter policies

In network mode, only IP filter policies can be applied to IES services.

6.3.5 VRRP support for IES IP interfaces in network mode

Note: VRRP for IPv4 is supported for IES IPv4 interfaces in network mode only.

The Virtual Router Redundancy Protocol (VRRP) for IPv4 is defined in the IETF RFC 3768, *Virtual Router Redundancy Protocol*. VRRP describes a method of implementing a redundant IP interface shared between two or more routers on a common LAN segment, allowing a group of routers to function as one virtual router. When this IP interface is specified as a default gateway on hosts directly attached to this LAN, the routers sharing the IP interface prevent a single point of failure by limiting access to this gateway address. For more information about use of VRRP, see the *7210 SAS-Mxp, R6, R12, S, Sx, T Router Configuration Guide*.

6.4 Configuring an IES service with CLI

This section provides information to configure IES services using the CLI.

6.4.1 Basic configuration

The most basic IES service configuration has the following entities:

- Customer ID (see Configuring customer accounts).
- An interface to create and maintain IP routing interfaces within IES service ID.
- A SAP on the interface specifying the access port and encapsulation values.

Example: IES service configuration on ALA-50

```
*A:ALA-50>config>service# info
----------------------------------------------
ies 1000 customer 50 vpn 1000 create
description "to internet"
interface "to-web" create
address 10.1.1.1/24
sap 1/1/10:100 create
exit
exit
no shutdown
----------------------------------------------
*A:ALA-50>config>service#
```

6.4.2 Common configuration tasks

About this task

This section provides a brief overview of the tasks that must be performed to configure IES services and provides the CLI commands:

Procedure

Step 1. Associate an IES service with a customer ID.

Step 2. Associate customer ID with the service.

Step 3. Assign an IP address.

Step 4. Create an interface.

Step 5. Define SAP parameters on the interface:

- Select nodes and ports.
- Optional - select filter policies (configured in the **config>filter** context).

Step 6. Enable service.

6.4.3 Configuring IES components

6.4.3.1 Configuring an IES service

The following example shows basic IES service configuration output.

Example: Basic IES service configuration

```
A:ALA-48>config>service#
----------------------------------------------
...
ies 1001 customer 1730 create
            description "to-internet"
            no shutdown
exit
----------------------------------------------
```

```
A:ALA-48>config>service#
```

6.4.3.2 Configuring IES interface parameters

The following example shows an IES configuration with interface parameters.

Example: IES configuration with interface parameters

```
*A:7210-SAS>config>service>ies>if# info
----------------------------------------------
arp-timeout 10000
allow-directed-broadcasts
icmp
ttl-expired 120 38
exit
ip-mtu 1000
----------------------------------------------
*A:7210-SAS>config>service>ies>if#
```

6.4.3.3 Configuring SAP parameters

A SAP is a combination of a port and encapsulation parameters which identifies the service access point on the interface and within the router. Each SAP must be unique within a router.

When configuring IES access SAP parameters, a default QoS policy is applied to each SAP ingress and SAP egress. Additional QoS policies must be configured in the **config>qos** context. Filter policies are configured in the **config>filter** context and must be explicitly applied to a SAP. There are no default filter policies.

Example: IES SAP configuration

```
----------------------------------------------
*A:ALA-A>config>service>ies>if# info
----------------------------------------------
address 10.10.36.2/24
sap 1/1/3:100 create
ingress
qos 101
exit
----------------------------------------------
*A:ALA-A>config>service>ies>if#
```

6.4.3.4 Configuring VRRP

Configuring VRRP parameters on an IES interface is optional and is available only in network mode. VRRP can be configured in either an owner or non-owner mode. The owner is the VRRP router whose virtual router IP address is the same as the real interface IP address. This is the router that responds to packets addressed to one of the IP addresses for ICMP pings, TCP connections and related addresses. All other virtual router instances participating in this message domain should have the same VRID configured and cannot be configured as an owner.

Example: IES configuration

```
*A:ALA-A>config>service>ies>if# info
----------------------------------------------
address 10.10.36.2/24
vrrp 2 owner
backup 10.10.36.2
authentication-type password
authentication-key "3WErEDozxyQ" hash
exit
----------------------------------------------
*A:ALA-A>config>service#
```

6.4.4 Service management tasks

This section describes the service management tasks.

6.4.4.1 Modifying IES service parameters

Existing IES service parameters in the CLI or NMS can be modified, added, removed, enabled or disabled. The changes are applied immediately to all services when the charges are applied.

To display a list of customer IDs, use the **show service customer** command. Enter the parameters (such as description SAP information) and then enter the new information.

Example: Modified service configuration

```
*A:ALA-A>config>service>ies# info
----------------------------------------------
ies 1000 customer 50 create
           description "This is a new description"
           interface "to-web" create
               address 10.1.1.1/24
               mac 00:dc:98:1d:00:00
               exit
           exit
           no shutdown
exit
----------------------------------------------
*A:ALA-A>config>service#
```

6.4.4.2 Deleting an IES service

An IES service cannot be deleted until SAPs and interfaces are shut down and deleted and the service is shutdown on the service level.

Use the following syntax to delete an IES service.

```
config>service#
    [no] ies service-id
    shutdown
    [no] interface ip-int-name
    shutdown
        [no] sap sap-id
```

```
        shutdown
```

6.4.4.3 Disabling an IES service

Use the following syntax to shut down an IES service without deleting the service parameters.

```
config>service> ies service-id
    shutdown
```

6.4.4.4 Re-enabling an IES service

Use the following syntax to re-enable an IES service that was shut down.

```
config>service> ies service-id
    [no] shutdown
```

Example: Re-enabling an IES service

```
config>service# ies 2000
    config>service>ies# no shutdown
    config>service>ies# exit
```

6.5 IES services command reference

6.5.1 Command hierarchies

- Global commands
- Interface commands
- Interface SAP commands
- Interface SAP filter and QoS commands
- VRRP commands (applicable only for network mode)
- Routed VPLS commands
- Show commands

6.5.1.1 Global commands

```
config
    - service
        - ies service-id [customer customer-id] [create] [vpn vpn-id]
        - no ies service-id
            - description description-string
            - no description
            - interface
            - no interface
```

```
            - service-name service-name
            - no service-name
            - [no] shutdown
```

6.5.1.2 Interface commands

```
config
    - service
        - ies service-id [customer customer-id] [create] [vpn vpn-id]
            - [no] interface ip-int-name [create]
                - address {ip-address/mask | ip-address netmask}
                - no address
                - arp-timeout seconds
                - no arp-timeout
                - bfd transmit-interval [receive receive-interval] [multiplier multiplier]
 [echo-receive echo-interval]
                - no bfd
                - dhcp
                    - delayed-enable seconds [init-only]
                    - no delayed-enable
                    - description description-string
                    - no description
                    - gi-address ip-address [src-ip-addr]
                    - no gi-address
                    - [no] option
                        - action {replace | drop | keep}
                        - no action
                        - [no] circuit-id [ascii-tuple | ifindex | sap-id | vlan-ascii-tuple]
                        - [no] remote-id  [mac | string string]
                        - [no] vendor-specific-option
                            - [no] client-mac-address
                            - [no] sap-id
                            - [no] service-id
                            - string text
                            - no string
                            - [no] system-id
                    - no relay-plain-bootp
                    - relay-plain-bootp
                    - no server
                    - server server1 [server2...(upto 8 max)]
                    - [no] shutdown
                    - [no] trusted
                - description description-string
                - no description
                - icmp
                    - redirects [number seconds]
                    - no redirects
                    - ttl-expired [number seconds]
                    - no ttl-expired
                    - unreachables [number seconds]
                    - no unreachables
                - ip-mtu octets
                - no ip-mtu
                - [no] loopback
                - [no] sap sap-id [create]
                - secondary {ip-address/mask | ip-address netmask} [broadcast {all-ones | host-
ones}] [igp-inhibit]
                - no secondary {ip-address/mask | ip-address netmask}
                - [no] shutdown
                - [no] static-arp ip-address
```

6.5.1.3 Interface SAP commands

```
config
    - service
        - ies service-id [customer customer-id] [create]
            - [no] interface ip-int-name
                - [no] sap sap-id [create]
                    - accounting-policy acct-policy-id
                    - no accounting-policy
                    - collect-stats
                    - no collect-stats
                    - description description-string
                    - no description
                    - dist-cpu-protection policy-name
                    - no dist-cpu-protection
                    - ingress
                        - meter-override
                        - no meter-override
                            - meter meter-id [create]
                            - no meter meter-id
                                - adaptation-rule  [pir adaptation-rule] [cir adaptation-rule]
                                -  cbs size [kbits | bytes | kbytes]
                                - no cbs
                                - mbs size [kbits | bytes | kbytes]
                                - no mbs
                                - mode mode
                                - no mode
                                - rate cir cir-rate [pir pir-rate]
                        - queue-override
                            - queue queue-id [create]
                                - adaptation-rule  [pir adaptation-rule] [cir adaptation-rule]
                                - no port-parent
                                - port-parent [cir-level cir-level]  [pir-weight pir-weight]
                                - queue-mgmt name
                                - no queue-mgmt
                                - no rate
                                - rate [cir cir-rate] [pir pir-rate]
                    - statistics
                        - ingress
                            - counter-mode {in-out-profile-count| forward-drop-count}
                    - [no] tod-suite tod-suite-name
                    - [no] shutdown
```

6.5.1.4 Interface SAP filter and QoS commands

```
config
    - service
        - ies service-id [customer customer-id] [vpn vpn-id] [create]
            - [no] interface ip-int-name
                - [no] sap sap-id [create]
                    - egress
                        - agg-rate-limit agg-rate
                        - no agg-rate-limit
                        - aggregate-meter-rate rate-in-kbps [burst burst-in-kbits] [enable-
stats]
                        - no aggregate-meter-rate
                        - filter ip ip-filter-id
                        - filter ipv6 ipv6 -filter-id
                        - no filter [ip ip-filter-id] [ipv6 ipv6 -filter-id]
```

```
                        - qos policy-id
                        - no qos
                    - ingress
                        - aggregate-meter-rate rate-in-kbps [burst burst-in-kbits]
                        - no aggregate-meter-rate
                        - filter ip ip-filter-id
                        - filter ipv6 ipv6-filter-id
                        - no filter [ip ip-filter-id] [ ipv6 ipv6-filter-id]
                        - qos policy-id [enable-table-classification]
                        - no qos
```

6.5.1.5 VRRP commands (applicable only for network mode)

```
config
    - service
        - ies service-id [customer customer-id] [vpn vpn-id]
            - interface ip-int-name
                - vrrp virtual-router-id [owner]
                - no vrrp virtual-router-id
                    - authentication-key {authentication-key | hash-key} [hash | hash2]
                    - no authentication-key
                    - [no] backup ip-address
                    - [no] init-delay [service-id] interface interface-name dst-ip ip-address
                    - init-delay seconds
                    - no init-delay
                    - mac ieee-address
                    - no mac
                    - [no] master-int-inherit
                    - message-interval {[seconds] [milliseconds milliseconds]}
                    - no message-interval
                    - [no] ping-reply
                    - policy vrrp-policy-id
                    - no policy
                    - [no] preempt
                    - priority priority
                    - no priority
                    - [no] shutdown
                    - [no] ssh-reply
                    - [no] standby-forwarding
                    - [no] telnet-reply
                    - [no] traceroute-reply
```

6.5.1.6 Routed VPLS commands

```
config
    - service
        - ies service-id [customer customer-id] [vpn vpn-id]
            - interface ip-interface-name [create]
            - no interface ip-interface-name
                - vpls service-name
                - no vpls
                    - ingress
                        - [no] enable-table-classification
                        - routed-override-qos-policy policy-id
                        - no routed-override-qos-policy
                        - v4-routed-override-filter ip-filter-id
                        - no v4-routed-override-filter
```

6.5.1.7 Show commands

```
show
    - service
        - customer [customer-id] [site customer-site-name]
        - id service-id
            - all
            - arp [ip-address] | [mac ieee-address] | [sap sap-id] | [interface ip-int-name]
            - base
            - dhcp
                - statistics [sap sap-id] | [sdp sdp-id:vc-id] | [interface interface-name]
                - summary [interface interface-name | saps]
            - interface [ip-address | ip-int-name] [detail]
        - sap-using [sap sap-id]
        - sap-using interface [ip-address | ip-int-name]
        - sap-using [ingress | egress] filter filter-id
        - sap-using [ingress] qos-policy qos-policy-id
        - service-using [ies] [customer customer-id]
```

6.5.2 Command descriptions

6.5.2.1 Configuration commands

6.5.2.1.1 Generic commands

shutdown

Syntax

[**no**] **shutdown**

Context

config>service>ies

config>service>ies>if

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command administratively disables an entity. When disabled, an entity does not change, reset, or remove any configuration settings or statistics. The operational state of the entity is disabled as well as the operational state of entities contained within. Many objects must be shut down before they may be deleted.

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

Note:

- See the *7210 SAS-Mxp, R6, R12, S, Sx, T Basic System Configuration Guide* for information about how to allocate addresses toward IP subnets using the **configure system resource-profile router max-ip-subnets** and **config system global-res-profile max-ip-subnets** CLI commands for the 7210 SAS-R6 and 7210 SAS-R12.
- Before using IPv6, resources for IPv6 routes must be allocated. See the *7210 SAS-Mxp, R6, R12, S, Sx, T Basic System Configuration Guide* for more information about how to use the **configure system resource-profile router max-ipv6-routes** and **config system global-res-profile max-ipv6-routes** CLI commands for the 7210 SAS-R6 and 7210 SAS-R12.

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

Special Cases

IES

The default administrative status of an IES service is down. While the service is down, all its associated virtual router interfaces are operationally down. The administrative state of the service is not reflected in the administrative state of the virtual router interface; for example, if:

- IES service is operational and an associated interface is shut down
- IES service is administratively shutdown and brought back up
- interface shutdown remains in administrative shutdown state

A service is regarded as operational as long as one IP Interface is operational.

IES IP Interfaces

When the IP interface is shut down, it enters the administratively and operationally down states. For a SAP bound to the IP interface, no packets are transmitted out the SAP and all packets received on the SAP are dropped while incrementing the packet discard counter.

description

Syntax

description *long description-string*

no description

Context

config>service>ies

config>service>ies>if>dhcp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

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

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

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

Parameters

string

Specifies the description character string. Allowed values are any string up to 80 characters composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

dhcp

Syntax

dhcp

Context

config>service>ies >if

config>service>vprn >if

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

Commands in this context configure DHCP parameters.

gi-address

Syntax

gi-address *ip-address* [*src-ip-addr*]

no gi-address

Context

config>service>ies>if>dhcp

config>service>vprn >if>dhcp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the gateway interface address for the DHCP relay. A subscriber interface can include multiple group interfaces with multiple SAPs. When the router functions as a DHCP relay, the GI address is needed to distinguish between different interfaces.

By default, the GI address used in the relayed DHCP packet is the primary IP address of a normal IES interface. Specifying the GI address allows the user to choose a secondary address. For group interfaces, a GI address must be specified in the group interface DHCP context or subscriber-interface DHCP context for DHCP to function.

Default

no gi-address

Parameters

ip-address

Specifies the host IP address to be used for DHCP relay packets.

src-ip-address

Specifies that this GI address is to be the source IP address for DHCP relay packets.

action

Syntax

action {**replace** | **drop** | **keep**}

no action

Context

config>service>ies >if>dhcp>option

config>service>vprn >if>dhcp>option

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures Relay Agent Information Option (Option 82) processing.

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

Default

no action

Parameters

replace

Keyword to specify that, in the upstream direction (from the user), the Option 82 field from the router is inserted in the packet (overwriting any existing Option 82 field). In the

downstream direction (toward the user) the Option 82 field is stripped (in accordance with RFC 3046).

drop

Keyword to specify the DHCP packet is dropped if an Option 82 field is present, and a counter is incremented.

keep

Keyword to specify that existing information is kept in the packet and the router does not add more information. In the downstream direction, the Option 82 field is not stripped and is forwarded toward the client.

The behavior is slightly different in case of Vendor Specific Options (VSOs). When the **keep** parameter is specified, the router inserts its VSO into the Option 82 field. This is done only when the incoming message already has an Option 82 field.

If no Option 82 field is present, the router does not create the Option 82 field. In this case, no VSO is added to the message.

circuit-id

Syntax

circuit-id [**ascii-tuple** | **ifindex** | **sap-id** | **vlan-ascii-tuple**]

no circuit-id

Context

config>service>ies >if>dhcp>option

config>service>vprn >if>dhcp>option

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the router to send either an ASCII tuple or the interface index (If Index) on the specified SAP ID in the **circuit-id** sub-option of the DHCP packet.

If disabled, the **circuit-id** sub-option of the DHCP packet is left empty.

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

Default

circuit-id ascii-tuple

Parameters

ascii-tuple

Specifies that the ASCII-encoded concatenated tuple is used, which consists of the access-node-identifier, service-id, and interface-name, separated by "|".

ifindex

Specifies that the interface index is used. Display the If Index of a router interface using the **show router if detail** command.

sap-id

Specifies that the SAP ID is used.

vlan-ascii-tuple

Specifies that the format includes VLAN ID, dot1p bits in addition to what is already included in the ascii-tuple. The format is supported on dot1q and qinq ports only. Therefore, when the Option 82 bits are stripped, dot1p bits are copied to the Ethernet header of an outgoing packet.

option

Syntax

[**no**] **option**

Context

config>service>ies >if>dhcp

config>service>vprn >if>dhcp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables DHCP Option 82 (Relay Agent Information Option) parameters processing and enables the context for configuring Option 82 sub-options.

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

Default

no option

remote-id

Syntax

remote-id [**mac** | **string** *string*]

no remote-id

Context

config>service>ies >if>dhcp>option

config>service>vprn >if>dhcp>option

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command identifies the host at the other end of the circuit. When enabled, the router sends the MAC address of the remote end (typically the DHCP client) in the **remote-id** sub-option of the DHCP packet.

If disabled, the **remote-id** sub-option of the DHCP packet is left empty.

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

Default

remote-id

Parameters

mac

Specifies that the MAC address of the remote end is encoded in the sub-option.

string *string*

Specifies the remote-id.

vendor-specific-option

Syntax

[**no**] **vendor-specific-option**

Context

config>service>ies >if>dhcp>option

config>service>vprn >if>dhcp>option

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the vendor-specific sub-option of the DHCP relay packet.

client-mac-address

Syntax

[**no**] **client-mac-address**

Context

config>service>ies >if>dhcp>option>vendor

config>service>vprn >if>dhcp>option>vendor

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables the sending of the MAC address in the vendor-specific sub-option of the DHCP relay packet.

The **no** form of this command disables the sending of the MAC address in the vendor-specific sub-option of the DHCP relay packet.

sap-id

Syntax

[**no**] **sap-id**

Context

config>service>ies >if>dhcp>option>vendor

config>service>vprn >if>dhcp>option>vendor

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables the sending of the SAP ID in the vendor-specific suboption of the DHCP relay packet.

The **no** form of this command disables the sending of the SAP ID in the vendor-specific suboption of the DHCP relay packet.

6.5.2.1.2 IES global commands

ies

Syntax

ies *service-id* **customer** *customer-id* [**create**] [**vpn** *vpn-id*]

no ies *service-id*

Context

config>service

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command creates or edits an IES 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.

IP interfaces defined within the context of an IES service ID must have a SAP created.

When a service is created, the **customer** keyword and *customer-id* must be specified that 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 has been created with a customer association, it is not possible to edit the customer association. The service must be deleted and recreated with a new customer association.

When a service is created, the use of the **customer** *customer-id* parameter is optional for navigating into the service configuration context. Attempting to edit a service with the incorrect *customer-id* specified results in an error.

More than one IP interface may be created within a single IES service ID.

By default, no IES service instances exist until they are explicitly created.

The **no** form of this command deletes the IES service instance with the specified *service-id*. The service cannot be deleted until all the IP interfaces defined within the service ID have been shutdown and deleted.

Parameters

service-id

Specifies the service identification number or string for the service in the service domain. This ID must be unique to this service and may not be used for another service of any type. The *service-id*must be the same number used for every router on which this service is defined.

Values 1 to 2147483648

customer *customer-id*

Specifies the customer ID number to be associated with the service. This parameter is required during service creation and optional for service editing or deleting.

Values 1 to 2147483647

vpn vpn-id

Specifies the VPN ID assigned to the service.

Values 1 to 2147483647

service-name

Syntax

service-name *service-name*

no service-name

Context

config>service>epipe

config>service>ies

config>service>vpls

config>service>vprn

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures an optional service name that adds a name identifier to a specific service to then use that service name in configuration references, as well as display and use service names in show commands throughout the system. This helps the service provider or administrator to identify and manage services within the 7210 SAS platforms.

All services are required to assign a service ID to initially create a service; however, either the service ID or the service name can be used to identify and reference a specific service when it is initially created.

Parameters

service-name

Specifies a unique service name, of up to 64 characters, to identify the service. Service names may not begin with an integer (0 to 9).

6.5.2.1.3 IES interface IPv6 commands

ipv6

Syntax

[**no**] **ipv6**

Context

config>service>ies>if

config>service>vprn>if

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables IPv6 for an IES interface.

address

Syntax

address *ipv6-address/prefix-length* [**eui-64**]

no address *ipv6-address/prefix-length*

Context

config>service>ies>if>ipv6

config>service>vprn>if>ipv6

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command assigns an IPv6 address to the IES interface.

Parameters

ipv6-address/prefix-length

Specify the IPv6 address on the interface.

Values ipv6-address/prefix: ipv6-address x:x:x:x:x:x:x:x (eight 16-bit pieces)

x:x:x:x:x:x:d.d.d.d

x [0 — FFFF]H

d [0 — 255]D

prefix-length 1 to 128

eui-64

Keyword to specify that a complete IPv6 address from the supplied prefix and 64-bit interface identifier is formed. The 64-bit interface identifier is derived from MAC address on Ethernet interfaces. For interfaces without a MAC address, for example ATM interfaces, the Base MAC address of the chassis is used.

icmp6

Syntax

icmp6

Context

config>service>ies>if>ipv6

config>service>vprn>if>ipv6

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures ICMPv6 parameters for the IES interface.

packet-too-big

Syntax

packet-too-big [*number seconds*]

no packet-too-big

Context

config>service>ies>if>ipv6>icmp6

config>service>vprn>if>ipv6>icmp6

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command specifies whether "packet-too-big" ICMPv6 messages should be sent. When enabled, ICMPv6 "packet-too-big" messages are generated by this interface.

The **no** form of this command disables the sending of ICMPv6 "packet-too-big" messages.

Default

100 10

Parameters

number

Specifies the number of "packet-too-big" ICMPv6 messages to send in the time frame specified by the *seconds* parameter.

Values 10 to 1000

Default 100

seconds

Specifies the time frame in seconds that is used to limit the number of "packet-too-big" ICMPv6 messages issued.

Values 1 to 60

Default 10

param-problem

Syntax

param-problem [*number seconds*]

no packet-too-big

Context

config>service>ies>if>ipv6>icmp6

config>service>vprn>if>ipv6>icmp6

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command specifies whether "parameter-problem" ICMPv6 messages should be sent. When enabled, "parameter-problem" ICMPv6 messages are generated by this interface.

The **no** form of this command disables the sending of "parameter-problem" ICMPv6 messages.

Default

100 10

Parameters

number

Specifies the number of "parameter-problem" ICMPv6 messages to send in the time frame specified by the *seconds* parameter.

Values 10 to 1000

Default 100

seconds

Specifies the time frame in seconds that is used to limit the number of "parameter-problem" ICMPv6 messages issued.

Values 1 to 60

Default 10

redirects

Syntax

redirects [*number seconds*]

no redirects

Context

config>service>ies>if>ipv6>icmp6

config>service>vprn>if>ipv6>icmp6

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures ICMPv6 redirect messages. When enabled, ICMPv6 redirects are generated when routes are not optimal on this router, and another router on the same subnetwork has a better route to alert the node that a better route is available.

When disabled, ICMPv6 redirects are not generated.

Default

redirects 100 10

Parameters

number

Specifies the number of version 6 redirects that are to be issued in the time frame specified by the *seconds* parameter.

Values 10 to 1000

Default 100

seconds

Specifies the time frame in seconds that is used to limit the number of version 6 redirects issued.

Values 1 to 60

Default 10

time-exceeded

Syntax

time-exceeded [*number seconds*]

no time-exceeded

Context

config>service>ies>if>ipv6>icmp6

config>service>vprn>if>ipv6>icmp6

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command specifies whether "time-exceeded" ICMPv6 messages should be sent. When enabled, ICMPv6 "time-exceeded" messages are generated by this interface.

When disabled, ICMPv6 "time-exceeded" messages are not sent.

Default

time-exceeded 100 10

Parameters

number

Specifies the number of "time-exceeded" ICMPv6 messages that are to be issued in the time frame specified by the *seconds* parameter.

Values 10 to 1000

Default 100

seconds

Specifies the time frame in seconds that is used to limit the number of "time-exceeded" ICMPv6 message to be issued.

Values 1 to 60

Default 10

unreachables

Syntax

unreachables [*number seconds*]

no unreachables

Context

config>service>ies>if>ipv6>icmp6

config>service>vprn>if>ipv6>icmp6

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command specifies that ICMPv6 host and network unreachable messages are generated by this interface.

When disabled, ICMPv6 host and network unreachable messages are not sent.

Default

unreachables 100 10

Parameters

number

Specifies the number of destination unreachable ICMPv6 messages that are issued in the time frame specified by the *seconds* parameter.

Values 10 to 1000

Default 100

seconds

Specifies the time frame in seconds that is used to limit the number of destination unreachable ICMPv6 messages to be issued.

Values 1 to 60

Default 10

link-local-address

Syntax

link-local-address *ipv6-address* [**preferred**]

no link-local-address

Context

config>service>ies>if>ipv6

config>service>vprn>if>ipv6

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the IPv6 link local address.

local-proxy-nd

Syntax

[**no**] **local-proxy-nd**

Context

config>service>ies>if>ipv6

config>service>vprn>if>ipv6

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables local proxy neighbor discovery on the interface.

The **no** form of this command disables local proxy neighbor discovery.

proxy-nd-policy

Syntax

proxy-nd-policy *policy-name* [*policy-name*...(**up to 5 max**)]

no proxy-nd-policy

Context

config>service>ies>if>ipv6

config>service>vprn>if>ipv6

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command applies a proxy neighbor discovery policy for the interface.

Parameters

policy-name

Specifies an existing neighbor discovery policy name. Allowed values are any string up to 32 characters composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes. The specified policy names must already be defined.

neighbor

Syntax

neighbor *ipv6-address mac-address*

no neighbor *ipv6-address*

Context

config>service>ies>if>ipv6

config>service>vprn>if>ipv6

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures IPv6-to-MAC address mapping on the IES interface.

Parameters

ipv6-address

Specifies the IPv6 address of the interface for which to display information.

Values x:x:x:x:x:x:x:x (eight 16-bit pieces)

x:x:x:x:x:x:d.d.d.d

x: [0 to FFFF]H

d: [0 to 255]D

prefix-length [1 to 128]

mac-address

Specifies the 48-bit MAC address for the IPv6-to-MAC address mapping 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.

6.5.2.1.4 IES interface commands

interface

Syntax

interface *ip-int-name*

no interface *ip-int-name*

Context

config>service>ies

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command creates a logical IP routing interface for an IES. When created, attributes like an IP address and service access point (SAP) can be associated with the IP interface.

The **interface** command, under the context of services, is used to create and maintain IP routing interfaces within IES service IDs. The **interface** command can be executed in the context of an IES service ID. The IP interface created is associated with the service core network routing instance and default routing

Interface names are case sensitive and must be unique within the group of defined IP interfaces defined for the **config service ies interface** command (that is, the network core router instance). Interface names must not be in the dotted decimal notation of an IP address. For example, the name "1.1.1.1" is not allowed, but "int-1.1.1.1" is allowed. Show commands for router interfaces use either interface names or the IP addresses. Use unique IP address values and IP address names to maintain clarity. It could be unclear to the user if the same IP address and IP address name values are used. Although not recommended, duplicate interface names can exist in different router instances.

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.

No default IP interface names are defined within the system; all IES IP interfaces must be explicitly defined. Interfaces are created in an enabled state.

Note:

- See the *7210 SAS-Mxp, R6, R12, S, Sx, T Basic System Configuration Guide* for information about allocating addresses toward IP subnets using the **configure system resource-profile router max-ip-subnets** command.
- Before using IPv6, resources for IPv6 routes must be allocated. See the *7210 SAS-Mxp, R6, R12, S, Sx, T Basic System Configuration Guide* for information about how to use the **configure system resource-profile router max-ipv6-routes** command

The **no** form of this command removes the IP interface and all the associated configuration. The interface must be administratively shutdown before issuing the **no interface** command.

For IES services, the IP interface must be shut down before the SAP on that interface may be removed.

Parameters

ip-int-name

Specifies the name of the IP interface. Interface names must be unique within the group of defined IP interfaces for **config router interface** and **config service ies interface** commands. An interface name cannot be in the form of an IP address. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

If *ip-int-name* already exists within the service ID, the context is changed to maintain that IP interface. If *ip-int-name* already exists within another service ID, an error occurs and the context are not changed to that IP interface. If *ip-int-name* does not exist, the interface is created and context is changed to that interface for further command processing.

Values 1 to 32 alphanumeric characters

address

Syntax

address {*ip-address/mask* | *ip-address netmask*}

address *ip-address mask*

no address

Context

config>service>ies>if

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command assigns an IP address IP subnet, to an IES IP router interface. Only one IP address can be associated with an IP interface. An IP address must be assigned to each IES IP interface. An IP address and a mask are used together to create a local IP prefix. The defined IP prefix must be unique within the context of the routing instance. It cannot overlap with other existing IP prefixes defined as local subnets on other IP interfaces in the same routing context.

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.

Parameters

ip-address

Specifies 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.

Values 1.0.0.0 to 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

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 to 30. Note that a mask length of 32 is reserved for system IP addresses.

netmask

Specifies 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 is used in a logical "AND" function to derive the local subnet of the IP address. Allowed values are dotted-decimal addresses. A mask of 255.255.255.255 is reserved for system IP addresses.

Values 128.0.0.0 to 255.255.255.254

arp-timeout

Syntax

arp-timeout *seconds*

no arp-timeout

Context

config>service>ies>if

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the minimum time in seconds an ARP entry learned on the IP interface is 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 the **arp-timeout** command is set to a value of zero seconds, ARP aging is disabled.

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

Default

arp-timeout 14400

Parameters

seconds

Specifies the minimum number of seconds a learned ARP entry is stored in the ARP table, expressed as a decimal integer. A value of zero specifies that the timer is inoperative and learned ARP entries are not aged.

Values 0 to 65535

allow-directed-broadcasts

Syntax

[**no**] **allow-directed-broadcasts**

Context

config>service>ies>if

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables the forwarding of directed broadcasts out of the IP interface. A directed broadcast is a packet received on a local router interface destined for the subnet broadcast address on another IP interface. This command on an IP interface enables or disables the transmission of packets destined for the subnet broadcast address of the egress IP interface.

When enabled, a frame destined for the local subnet on this IP interface is sent as a subnet broadcast out this interface. Care should be exercised when allowing directed broadcasts because this is a well-known mechanism used for denial-of-service attacks.

When disabled, directed broadcast packets discarded at this egress IP interface are counted in the normal discard counters for the egress SAP.

By default, directed broadcasts are not allowed and are 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

delayed-enable

Syntax

delayed-enable *seconds* [**init-only**]

no delayed-enable

Context

config>service>ies>if

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command delays making an 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 (for example, after a reboot). To ensure that the state has time to be synchronized, the **delayed-enable** timer can be specified. The optional **init-only** parameter specifies to use the **delayed-enable** 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 to 1200

init-only

Keyword that delays the initialization of the subscriber interface to give the system time to complete necessary tasks, such as allowing routing protocols to converge or MCS to synchronize the subscriber information. The delay occurs only immediately after a reboot.

ip-mtu

Syntax

ip-mtu *octets*

no ip-mtu

Context

config>service>ies>if

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the maximum IP transmit unit (packet) for the interface.

The MTU that is advertised from the IES size is:

MINIMUM((SdpOperPathMtu - EtherHeaderSize), (Configured ip-mtu))

By default (for Ethernet network interface) if no ip-mtu is configured, the packet size is (1568 - 14) = 1554.

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

Default

no ip-mtu

Parameters

octets

Specifies the number of octets in the IP-MTU.

Values 512 to 9000

loopback

Syntax

[**no**] **loopback**

Context

config>service>ies>if

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command specifies that the associated interface is a loopback interface that has no associated physical interface. As a result, the associated IES interface cannot be bound to a SAP.

Note that you can configure an IES interface as a loopback interface by issuing the **loopback** command instead of the **sap** command. The loopback flag cannot be set on an interface where a SAP is already defined, and a SAP cannot be defined on a loopback interface.

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>ies>if

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command assigns up to 64 secondary IP addresses to the interface, including the primary IP address. Each address can be configured in an IP address, IP subnet, or broadcast address format.

Parameters

ip-address

Specifies the IP address of the IP interface. The IP address portion of the address command specifies the IP host address that is used by the IP interface within the subnet. This address must be unique within the subnet and specified in dotted-decimal notation.

Values 1.0.0.0 to 223.255.255.255

/

The forward slash is a parameter delimiter that 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* parameter. If a forward slash does not immediately follow the *ip-address*, a dotted decimal *netmask* must follow the prefix.

mask

Specifies 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* parameter. The *mask* 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. A mask length of 32 is reserved for system IP addresses.

Values 1 to 32

netmask

Specifies 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 *netmask* parameter indicates the complete mask that is used in a logical "AND" function to derive the local subnet of the IP address. A netmask of 255.255.255.255 is reserved for system IP addresses.

Values a.b.c.d (network bits all 1 and host bits all 0)

broadcast {all-ones | host-ones}

This optional 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 to a broadcast address of **host-ones**.

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 configured as **all-ones**, the **address** command must be executed with the **broadcast** parameter defined. 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**) is received by the IP interface

Values **all-ones** — Specifies that the broadcast address used by the IP interface for this IP address is 255.255.255.255, also known as the local broadcast. **host-ones** — Specifies that the broadcast address used by the IP interface for this IP address is the subnet broadcast

address. This is an IP address that corresponds to the local subnet described by the *ip-address* and *mask* or *netmask* with all of the host bits set to binary 1. This is the default broadcast address used by an IP interface.

Default host-ones

igp-inhibit

Specifies that the secondary IP address should not be recognized as a local interface by the running IGP.

static-arp

Syntax

static-arp *ip-address ieee-mac-address*

no static-arp *ip-address*

Context

config>service>ies>if

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures a static address resolution protocol (ARP) entry associating a subscriber IP address with a MAC address for the core router instance. This static ARP appears in the core routing ARP table. A static ARP can be configured only 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 is replaced with the new MAC address.

The **no** form of this command removes a static ARP entry.

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.

vpls

Syntax

vpls *service-name*

Context

config>service

config>service>ies>if

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command binds 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**). When the IP interface is administratively up, the system scans 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 immediately attempts to resolve the specific name.

If a VPLS service is found associated with the name and with the **allow-ip-int-binding** flag set, the IP interface is attached to the VPLS service allowing routing to and from the service virtual ports when 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 is ignored and is not 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 is 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 does 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 is 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.

When 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.

Parameters

service-name

Required when using the IP interface **vpls** command and specifies the service name that the system attempts to resolve to an **allow-ip-int-binding** enabled VPLS service associated with the name. The specified name is expressed as an ASCII string consisting

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.

6.5.2.1.5 IES interface ICMP commands

icmp

Syntax

icmp

Context

config>service>ies>if

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

Commands in this context configure Internet Control Message Protocol (ICMP) parameters on an IES service.

mask-reply

Syntax

[**no**] **mask-reply**

Context

config>service>ies>if>icmp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables responses to 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 replies to mask requests.

The **no** form of this command disables replies to ICMP mask requests on the router interface.

Default

mask-reply

redirects

Syntax

redirects [*number seconds*]

no redirects

Context

config>service>ies>if>icmp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the rate for 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. Control the rate at which ICMP redirects are issued using the optional *number* and *seconds* parameters by indicating the maximum number of redirect messages that can be issued on the interface for a specific 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

Parameters

number

Specifies the maximum number of ICMP redirect messages to send. This parameter must be specified with the *seconds* parameter.

Values 10 to 1000

seconds

Specifies the time frame in seconds used to limit the *number* of ICMP redirect messages that can be issued.

Values 1 to 60

ttl-expired

Syntax

ttl-expired *number seconds*

no ttl-expired

Context

config>service>ies>if>icmp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the rate 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

Specifies 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 to 1000

seconds

Specifies 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 to 60

unreachables

Syntax

unreachables [*number seconds*]

no unreachables

Context

config>service>ies>if>icmp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the rate for ICMP host and network destination unreachable messages issued on the router interface.

This command enables the generation of ICMP destination unreachables on the router interface. Control the rate at which ICMP unreachables are issued using the optional *number* and *time* parameters by indicating the maximum number of destination unreachable messages that can be issued on the interface for a specific time interval.

By default, generation of ICMP destination unreachable 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 destination unreachable messages on the router interface.

Default

unreachables 100 10

Parameters

number

Specifies the maximum number of ICMP unreachable messages to send. This parameter must be specified with the *seconds* parameter.

Values 10 to 1000

seconds

Specifies the time frame in seconds used to limit the *number* of ICMP unreachable messages that can be issued.

Values 1 to 60

6.5.2.1.6 IES SAP commands

sap

Syntax

sap *sap-id* [**create**]

no sap *sap-id*

Context

config>service>ies>if

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command creates a Service Access Point (SAP) within a service. A SAP is a combination of port and encapsulation parameters that identify 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 does 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 be defined only on a port that has been configured as an access port using the command.

If a port is shut down, 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 is 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 are also deleted.

Special Cases

IES

A SAP is defined within the context of an IP routed interface. Each IP interface is limited to a single SAP definition. Attempts to create a second SAP on an IP interface fail and generate an error; the original SAP is not affected.

Parameters

sap-id

Specifies the physical port identifier portion of the SAP definition. See Common CLI command descriptions for command syntax.

port-id

Specifies the physical port ID in the *slot/mda/port* format.

If the card in the slot has Media Dependent Adapters (MDAs) installed, the *port-id* must be in the slot_number/MDA_number/port_number format. For example 1/1/1 specifies port 1 on MDA 1 in slot 1.

create

Keyword to create a SAP instance. The **create** keyword requirement can be enabled or disabled in the **environment>create** context.

accounting-policy

Syntax

accounting-policy *acct-policy-id*

no accounting-policy

Context

config>service>ies>if>sap

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables the accounting policy context that can be applied to a SAP.

An accounting policy must be defined before it can be associated with a SAP. If the *policy-id* does not exist, an error message is generated.

A maximum of one accounting policy can be associated with a SAP at one time. Accounting policies are configured in the **config>log** context.

The **no** form of this command removes the accounting policy association from the SAP, and the accounting policy reverts to the default.

Parameters

acct-policy-id

Specifies the accounting *policy-id* as configured in the **config>log> accounting-policy** context.

Values 1 to 99

collect-stats

Syntax

[**no**] **collect-stats**

Context

config>service>ies>if>sap

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables accounting and statistical data collection for either the SAP, network port, or IP interface. When applying accounting policies the data, by default, is collected in the appropriate records and written to the designated billing file.

When the **no collect-stats** command is issued, the statistics are still accumulated by the cards. However, the CPU does not obtain the results and write them to the billing file. If a subsequent **collect-stats** command is issued, the counters written to the billing file include all the traffic while the **no collect-stats** command was in effect.

Default

no collect-stats

dist-cpu-protection

Syntax

dist-cpu-protection *policy-name*

no dist-cpu-protection

Context

config>service>ies>if>sap

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command assigns a valid existing Distributed CPU Protection (DCP) policy to the SAP. By default, no DCP policy is associated with the SAP.

The **no** form of this command disables the use of DCP policies for the SAP.

Default

no dist-cpu-protection

Parameters

policy-name

Specifies the name of the DCP policy, up to 32 characters.

6.5.2.1.7 IES interface filter and QoS policy commands

egress

Syntax

egress

Context

config>service>ies>if>sap

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

Commands in this context apply egress policies.

agg-rate-limit

Syntax

agg-rate-limit *agg-rate*

no agg-rate-limit

Context

config>service>ies>if>sap>egress

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command defines a maximum total rate for all egress queues on a service SAP.

Set the port scheduler to "sap-based" scheduling mode before using this command. The egress port scheduler enforces the aggregate queue rate for the SAP as it distributes its bandwidth to all the SAPs configured on the port. The port scheduler stops distributing bandwidth to member queues when it has detected that the aggregate rate limit has been reached.

A SAP aggregate scheduler is created for each instance of the SAP queues created on each of the member ports of the LAG. For a LAG, the port scheduler-mode configured for the primary port is used for all the member ports of the LAG.

Specify the scheduler mode using the **scheduler-mode** command. To implement the aggregate-rate-limit, the scheduler mode must be specified as "sap-based". For more information about the **scheduler-mode** command, see the *7210 SAS-Mxp, R6, R12, S, Sx, T Interface Configuration Guide*.

The **no** form of this command removes the aggregate rate limit from the SAP or multi-service site.

Parameters

agg-rate

Specifies the rate, in kilobits-per-second, that the maximum aggregate rate that the queues on the SAP or MSS can operate.

Values 1 to 10000000, max

aggregate-meter-rate

Syntax

aggregate-meter-rate *rate-in-kbps* [**burst** *burst-in-kbits*] [**enable-stats**]

no aggregate-meter-rate

Context

config>service>ies>if>sap>egress

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command associates a set of two counters to count total forwarded packets and octets and total dropped packets and octets. When the counter is enabled, the amount of resources required increases by twice the amount of resources taken up when counter is not used. If **enable-stats** keyword is specified during the creation of the meter, the counter is allocated by software, if available. To free up the counter and relinquish its use, the user can use the **no aggregate-meter-rate** command, and then recreate the meter using the **aggregate-meter-rate** command.

If egress Frame-based accounting is used, the SAP egress aggregate meter rate accounts for the Ethernet frame overhead. The system accounts for 12 bytes of IFG and 8 bytes of start delimiter. Frame-based counting does not affect the count of octets maintained by the counter, if in use.

Note:

- Before enabling this command for a SAP, resources must be allocated to this feature from the egress internal TCAM resource pool using the **configure system resource-profile egress-internal-tcam egress-sap-aggregate-meter** command. See the *7210 SAS-Mxp, R6, R12, S, Sx, T Basic System Configuration Guide* for more information.
- The egress aggregate meter is not FC aware. The forward and drop decisions are taken based on the order the packets are sent out of the SAP by the egress port scheduler.

The **no** form of this command removes the egress aggregate policer from use.

Default

no aggregate-meter-rate

Parameters

rate-in-kbps

Specifies the rate in kilobits/s.

Values 1 to 100000000 | max

Default max

burst-in-kbits

Specifies the burst size for the policer in kilobits. The burst size cannot be configured without configuring the rate.

Values 4 to 2146959 | default

Default 512

enable-stats

Specifies whether the counter is to count forwarded and dropped packets must be allocated.

filter

Syntax

filter ip *ip-filter-id*

filter ipv6 *ipv6-filter-id*

no filter [**ip** *ip-filter-id*] [**ipv6** *ipv6-filter-id*]

Context

config>service>ies>if>sap>egress

config>service>ies>if>sap>ingress

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command associates a filter policy with an ingress or egress SAP. Filter policies control the forwarding and dropping of packets based on the matching criteria.

The **filter** command is used to associate a filter policy with a specified *ip-filter-id* with an ingress or egress SAP. The filter policy must already be defined before the **filter** command is run. If the filter policy does not exist, the operation fails and an error message returned.

In general, filters applied to SAPs (ingress or egress) apply to all packets on the SAP. One exception is non-IP packets are not applied to the match criteria, so the default action in the filter policy applies to these packets.

The **no** form of this command removes any configured filter ID association with the SAP. The filter ID is not removed from the system.

Special Cases

IES

Only IP filters are supported on an IES IP interface, and the filters only apply to routed traffic.

Parameters

ip

Keyword indicating the filter policy is an IP filter.

ip-filter-id

Specifies the ID for the IP filter policy. Allowed values are an integer in the range of 1 and 65535 that corresponds to a previously created IP filter policy in the **configure>filter>ip-filter** context.

Values 1 to 65535

ipv6 ***ipv6-filter-id***

Specifies the IPv6 filter policy. The filter ID must already exist within the created IPv6 filters.

Values 1 to 65535

qos

Syntax

qos *policy-id*

qos *policy-id* [**enable-table-classification**]

no qos *policy-id*

Context

config>service>ies>if>sap>egress

config>service>ies>if>sap>ingress

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command associates a Quality of Service (QoS) policy with an ingress or egress SAP or IP interface.

QoS ingress and egress policies are important for the enforcement of SLA agreements. The policy ID must be defined before associating the policy with a SAP or IP interface. If the *policy-id* does not exist, an error is 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 only allows 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 policy of same or different type replaces the earlier one with the new policy.

On the 7210 SAS-R6 and 7210 SAS-R12 (ingress), using the **enable-table-classification** keyword enables the use of IP DSCP tables to assign FC and profile on a per-SAP ingress basis. The match-criteria configured in the service ingress policy, which require CAM resources, are ignored. Only meters from the service ingress policy are used (and the meters still require CAM resources). The IP DSCP classification policy configured in the SAP ingress policy is used to assign FC and profile. The default FC is assigned from the SAP ingress policy.

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.

Note: On the 7210 SAS-R6 and 7210 SAS-R12, when the interface is associated with RVPLS, the behavior of the **qos** command is affected. See the enable-table-classification and routed-override-qos-policy commands for more information about classification behavior for RVPLS.

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

Specifies the ingress or egress policy ID to associate with a SAP or IP interface on ingress or egress. The policy ID must already exist.

Values 1 to 65535

enable-table-classification

Keyword to enable the use of table-based classification at SAP ingress instead of CAM-based classification at SAP ingress. The FC and profile are taken from the IP DSCP classification policy configured in the ingress policy, along with the meters from the SAP ingress policy. Match-criteria entries in the SAP ingress policy are ignored.

ingress

Syntax

ingress

Context

config>service>ies>if>sap>egress

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

Commands in this context configure ingress SAP 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.

aggregate-meter-rate

Syntax

aggregate-meter-rate *rate-in-kbps* [**burst** *burst-in-kbits*]

no aggregate-meter-rate

Context

config>service>ies>if>sap>ingress

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

Note: The sum of the CIRs of the individual FCs configured under the SAP cannot exceed the PIR rate configured for the SAP. Although the 7210 SAS software does not block this configuration, it is not recommended for use.

When the SAP aggregate policer is configured, per FC policer can be only configured in "trtcm2" mode (RFC 4115).

The meter modes "srtcm" and "trtcm1" are used in the absence of an aggregate meter.

The SAP ingress meter counters increment the packet or octet counts based on the final disposition of the packet.

If ingress Frame-based accounting is used, the SAP aggregate meter rate accounts for the Ethernet frame overhead. The system accounts for 12 bytes of IFG and 8 bytes of start delimiter.

The **no** form of this command removes the aggregate policer from use.

Default

no aggregate-meter-rate

Parameters

rate-in-kbps

Specifies the rate in kilobits per second.

Values 0 to 20000000 | max

Default max

burst-in-kilobits

Specifies the burst size for the policer in kilobits. The burst size cannot be configured without configuring the rate.

Values 4 to 2146959

Default 512

The following table lists the final disposition of the packet based on the operating rate of the per FC policer and the per-SAP aggregate policer.

Table 84: Final disposition of the packet based on per FC and per SAP policer or meter

Per FC meter operating rate	Per FC assigned color	SAP aggregate meter operating rate	SAP aggregate meter color	Final packet color
Within CIR	Green	Within PIR	Green	Green or In-profile
Within CIR[16]	Green	Above PIR	Red	Green or In-profile
Above CIR, Within PIR	Yellow	Within PIR	Green	Yellow or Out-of-Profile
Above CIR, Within PIR	Yellow	Above PIR	Red	Red or Dropped
Above PIR	Red	Within PIR	Green	Red or Dropped
Above PIR	Red	Above PIR	Red	Red or Dropped

meter-override

Syntax

[**no**] **meter-override**

Context

config>service>ies>if>sap>ingress

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables the context for specific overrides to one or more meters created on the SAP through the sap-ingress QoS policies.

[16] This row is not recommended for use. See the note in the aggregate-meter-rate description for more information.

The **no** form of this command is used to remove any existing meter overrides.

Default

no meter-override

meter

Syntax

meter *meter-id* [**create**]

no meter *meter-id*

Context

config>service>ies>if>sap>ingress>meter-override

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command, within the SAP ingress contexts, creates a CLI node for specific overrides to a specific meter created on the SAP through sap-ingress QoS policies.

The **no** form of this command removes existing overrides for the specified meter-id.

Parameters

meter-id

Required when executing the meter command within the meter-overrides context. The *meter-id* must exist within the sap-ingress QoS policy applied to the SAP. If the meter is not currently used by any forwarding class or forwarding type mappings, the meter does not actually exist on the SAP. This does not preclude creating an override context for the *meter-id*.

create

Keyword required when a meter *meter-id* override node is being created and the system is configured to expect explicit confirmation that a new object is being created. When the system is not configured to expect explicit confirmation, the **create** keyword is not required.

adaptation-rule

Syntax

adaptation-rule [**pir** *adaptation-rule* [**max** | **min** | **closest**]] [**cir** *adaptation-rule* [**max** | **min** | **closest**]]

no adaptation-rule

Context

config>service>ies>if>sap>ingress>meter-override>meter

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command overrides specific attributes of the specified meter adaptation rule parameters. The adaptation rule controls the method used by the system to derive the operational CIR and PIR settings when the meter is provisioned in hardware. For the CIR and PIR parameters individually, the system attempts to find the best operational rate depending on the defined constraint.

The **no** form of this command removes any explicitly defined constraints used to derive the operational CIR and PIR created by the application of the policy. When a specific **adaptation-rule** is removed, the default constraints for **rate** and **cir** apply.

Default

no adaptation-rule

Parameters

pir

Specifies the constraints enforced when adapting the PIR rate defined within the meter-override meter *meter-id* command. The **pir** parameter requires a qualifier that defines the constraint used when deriving the operational PIR for the queue. When the **meter-override** command is not specified, the default applies.

Note: When the meter mode in use is "trtcm2," this parameter is interpreted as EIR value. See the description and relevant notes for meter modes in the *7210 SAS-Mxp, R6, R12, S, Sx, T Quality of Service Guide* for more information.

cir

Defines the constraints enforced when adapting the CIR rate defined within the meter-override meter *meter-id* command. The **cir** parameter requires a qualifier that defines the constraint used when deriving the operational CIR for the queue. When the **cir** parameter is not specified, the default constraint applies.

adaptation-rule

Specifies the criteria to use to compute the operational CIR and PIR values for this meter, while maintaining a minimum offset.

Values **max** — The **max**, **min**, and **closest** parameters are mutually exclusive. When **max** is defined, the operational PIR for the meter is equal to or less than the administrative rate specified using the **meter-override** command.

Values **min** — The **min**, **max**, and **closest** parameters are mutually exclusive. When **min** is defined, the operational PIR for the queue is equal to or greater than the administrative rate specified using the **meter-override** command.

Values **closest** — The **closest**, **min**, and **max** parameters are mutually exclusive. When **closest** is defined, the operational PIR for the meter

is the rate closest to the rate specified using the **meter-override** command.

cbs

Syntax

cbs *size* [**kbits** | **bytes** | **kbytes**]

no cbs

Context

config>service>ies>if>sap>ingress>meter-override>meter

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command overrides the default CBS for the meter. The committed burst size parameter specifies the maximum burst size that can be transmitted by the source while still complying with the CIR. If the transmitted burst is lower than the CBS value, the packets are marked as in-profile by the meter to indicate that the traffic is complying with meter configured parameters.

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

Default

cbs 32

Parameters

size

Specifies the value in kilobits, bytes, or kilobytes.

Values kbits: 4 to 2146959 | default

bytes: 512 to 274810752

kbytes: 1 to 268369

mbs

Syntax

mbs *size* [**kbits** | **bytes** | **kbytes**]

no mbs

Context

config>service>ies>if>sap>ingress>meter-override>meter

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command overrides the default MBS for the meter. The maximum burst size parameter specifies the maximum burst size that can be transmitted by the source while still complying with the CIR. If the transmitted burst is lower than the MBS value, the packets are marked as in-profile by the meter to indicate that the traffic is complying meter configured parameters.

The **no** form of this command returns the MBS size to the default value.

Default

mbs 512

Parameters

size

Specifies the value in kilobits, bytes, or kilobytes.

Values kbits: 4 to 2146959 | default

bytes: 512 to 274810752

kbytes: 1 to 268369

mode

Syntax

mode *mode*

no mode

Context

config>service>ies>if>sap>ingress>meter-override>meter

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command is used to override the sap-ingress QoS policy configured mode parameters for the specified meter-id.

The **no** form of this command reverts the policy defined metering and profiling mode to a meter.

Parameters

mode

Specifies the rate mode of the meter-override.

Values trtcm1, trtcm2, srtcm

rate

Syntax

rate cir *cir-rate* [**pir** *pir-rate*]

no rate

Context

config>service>ies>if>sap>ingress>meter-override>meter

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command is used to override the sap-ingress QoS policy configured rate parameters for the specified meter-id.

The **max** default specifies the amount of bandwidth in kilobits per second (thousand bits per second). The **max** value is mutually exclusive to the *pir-rate* value.

The **no** form of this command reverts the policy defined metering and profiling rate to a meter.

Default

max

Parameters

pir-rate

Specifies the administrative PIR rate, in kilobits, for the queue. When the **rate** command is run, a valid PIR setting must be explicitly defined. When the **rate** command has not been run, the default PIR of **max** is assumed.

Fractional values are not allowed and must be specified as a positive integer.

Note: When the meter mode is set to "trtcm2," the PIR value is interpreted as the EIR value. See the *7210 SAS-Mxp, R6, R12, S, Sx, T Quality of Service Guide* for more information.

The actual PIR rate is dependent on the queue **adaptation-rule** parameters and the hardware where the queue is provisioned.

Values 0 to 20000000 | max

Default max

cir-rate

The **cir** parameter overrides the default administrative CIR used by the queue. When the **rate** command is executed, a CIR setting is optional. When the **rate** command has not been executed or the **cir** parameter is not explicitly specified, the default CIR (0) is assumed.

Fractional values are not allowed and must be specified as a positive integer.

Values 0 to 20000000 | max

Default 0

counter-mode

Syntax

counter-mode {**in-out-profile-count** | **forward-drop-count**}

Context

config>service>ies>sap>statistics>ingress

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command sets the counter mode for the counters associated with sap ingress meters or policers. A pair of counters is available with each meter. These counters count different events based on the counter mode value.

Note:
The counter mode can be changed if an accounting policy is associated with a SAP. If the counter mode is changed, the counters associated with the meter are reset and the counts are cleared. If an accounting policy is in use when the counter mode is changed, a new record is written into the current accounting file.

Perform the following sequence of commands on the specified SAP to ensure the correct statistics are collected when the counter-mode is changed.

1. Run the **config service ies interface sap no collect-stats** command, to disable writing of accounting records for the SAP.
2. Change the counter mode to the desired option by running the **config service vprn interface sap counter-mode** {**in-out-profile-count** | **forward-drop-count**} command.
3. Run the **config service ies interface sap collect-stats** command to enable writing of accounting records for the SAP.

The **no** form of this command restores the counter mode to the default value.

Default

in-out-profile-count

Parameters

in-out-profile-count

Specifies that one counter counts the total in-profile packets and octets received on ingress of a SAP and another counts the total out-of-profile packets and octets received

on ingress of a SAP. A packet is determined to be in-profile or out-of-profile based on the meter rate parameters configured. A packet is dropped by the policer if it exceeds the configured PIR rate. Dropped counts are not maintained in hardware when this mode is used. It is obtained by subtracting the sum of in-profile count and out-of-profile count from the total SAP ingress received count and displayed.

forward-drop-count

Specifies that one counter counts the forwarded packets and octets received on ingress of a SAP and another counts the dropped packets. The forwarded count is the sum of in-profile and out-of-profile packets/octets received on SAP ingress. The dropped count is count of packets/octets dropped by the policer. A packet is determined to be in-profile or out-of-profile based on the meter rate parameters configured. A packet is dropped by the policer if it exceeds the configured PIR rate. The in-profile count and out-of-profile count is not individually available when operating in this mode.

tod-suite

Syntax

tod-suite *tod-suite-name*

no tod-suite

Context

config>service>ies>if>sap

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

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

Default

no tod-suite

Parameters

tod-suite-name

Specifies collection of policies (ACLs, QoS) including time-ranges that define the full or partial behavior of a SAP. The suite can be applied to more than one SAP.

6.5.2.2 Routed VPLS commands

ingress

Syntax

ingress

Context

config>service>ies>if>vpls

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

Commands in this context define the routed ip-filter-id optional filter overrides.

enable-table-classification

Syntax

[**no**] **enable-table-classification**

Context

config>service>ies>if>vpls>ingress

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables and disables the use of IP DSCP table-based classification to assign FC and profile on a per-interface ingress basis.

The match-criteria configured in the service ingress policy, which require CAM resources, are ignored. Only meters from the service ingress policy are used (and the meters still require CAM resources). If an IP DSCP classification policy is configured in the VPLS SAP ingress policy, it is not used to assign FC and profile.

The **no** form of this command disables table-based classification. When disabled, the IP ingress packets within a VPLS service attached to the IP interface use the SAP ingress QoS policy applied to the virtual port used by the packets, when defined.

Default

no enable-table-classification

routed-override-qos-policy

Syntax

routed-override-qos-policy *policy-id*

no routed-override-qos-policy

Context

config>service>ies>if>vpls>ingress

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command specifies an IP DSCP classification policy that is applied to all ingress packets entering the VPLS service. The DSCP classification policy overrides any existing SAP ingress QoS policy applied to SAPs for packets associated with the routing IP interface. The routed override QoS policy is optional and when it is not defined or it is removed, the IP routed packets use the existing SAP ingress QoS policy configured on the VPLS virtual port.

The **no** form of this command is used to remove the IP DSCP classification policy from the ingress IP interface. When removed, the IP ingress routed packets within a VPLS service attached to the IP interface use the SAP ingress QoS policy applied to the virtual port used by the packets, when defined.

Default

no routed-override-qos-policy

Parameters

policy-id

Specifies the ID for the routed override QoS policy. Allowed values are an integer in the range of 1 and 65535 that corresponds to a previously created IP DSCP classification policy in the **configure>qos>dscp-classification** context.

Values 1 to 65535

v4-routed-override-filter

Syntax

v4-routed-override-filter *ip-filter-id*

no v4-routed-override-filter

Context

config>service>ies>if>vpls>ingress

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command specifies an IP filter ID that is applied to all ingress packets entering the VPLS service. The filter overrides any existing ingress IP 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 IP routed packets uses the any existing ingress IP filter on the VPLS virtual port.

The **no** form of this command is used to remove the IP routed override filter from the ingress IP interface. When removed, the IP ingress routed packets within a VPLS service attached to the IP interface uses the IP ingress filter applied to the packets virtual port when defined.

Parameters

ip-filter-id

Specifies the ID for the IP filter policy. Allowed values are an integer that corresponds to a previously created IP filter policy in the **configure>filter>ip-filter** context.

Values 1 to 65535

6.5.2.3 IES show commands

customer

Syntax

customer [*customer-id*] [**site** *customer-site-name*]

Context

show>service

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays service customer information.

Parameters

customer-id

Displays only information for the specified customer ID.

Values 1 to 2147483647

Default All customer IDs display

site *customer-site-name*

Specifies the customer site, which is an anchor point for an ingress and egress virtual scheduler hierarchy.

Output

The following output is an example of customer information, and Table 85: Output fields: customer describes the output fields.

Sample output

```
*A:ALA-12# show service customer
============================================================
Customers
============================================================
Customer-ID : 1
Contact     : Manager
Description : Default customer
Phone       : (123) 555-1212

Customer-ID : 2
Contact     : Tech Support
Description : TiMetra Networks
Phone       : (234) 555-1212

Customer-ID : 3
Contact     : Fred
Description : TiMetra Networks
Phone       : (345) 555-1212

Customer-ID : 6
Contact     : Ethel
Description : Epipe Customer
Phone       : (456) 555-1212

Customer-ID : 7
Contact     : Lucy
Description : ABC Customer
Phone       : (567) 555-1212

Customer-ID : 8
Contact     : Customer Service
Description : IES Customer
Phone       : (678) 555-1212

Customer-ID : 274
Contact     : Mssrs. Beaucoup
Description : ABC Company
Phone       : 650 123-4567

Customer-ID : 94043
Contact     : Test Engineer on Duty
Description : TEST Customer
Phone       : (789) 555-1212

------------------------------------------------------
Total Customers : 8
------------------------------------------------------------
*A:ALA-12#


*A:ALA-12# show service customer 274
============================================================================
```

```
Customer  274
===============================================================================
Customer-ID : 274
Contact     : Mssrs. Beaucoup
Description : ABC Company
Phone       : 650 123-4567
-------------------------------------------------------------------------------
Multi Service Site
-------------------------------------------------------------------------------
Site        : west
Description : (Not Specified)
===============================================================================
*A:ALA-12#


*A:ALA-12# show service customer 274 site west
===============================================================================
Customer  274
===============================================================================
Customer-ID : 274
Contact     : Mssrs. Beaucoup
Description : ABC Company
Phone       : 650 123-4567
-------------------------------------------------------------------------------
Multi Service Site
-------------------------------------------------------------------------------
Site        : west
Description : (Not Specified)
Assignment  : Card 5
I. Sched Pol: SLA1
E. Sched Pol: (Not Specified)
-------------------------------------------------------------------------------
Service Association
-------------------------------------------------------------------------------
No Service Association Found.
===============================================================================
*A:ALA-12#
```

Table 85: Output fields: customer

Label	Description
Customer-ID	The ID that uniquely identifies a customer.
Contact	The name of the primary contact person.
Description	Generic information about the customer.
Phone	The phone/pager number to reach the primary contact person.
Total Customers	The total number of customers configured.
Multi Service Site	
Site	Multi-service site name. A multi-service customer site is a group of SAPs with common origination and termination points.
Description	Information about a specific customer multi-service site.

Label	Description
Assignment	The port ID, MDA, or card number, where the SAPs that are members of this multiservice site are defined.
I. Sched Pol	The ingress QoS scheduler policy assigned to this multiservice site.
E. Sched Pol	The egress QoS scheduler policy assigned to this multiservice site.
Service Association	
Service-ID	The ID that uniquely identifies a service.
SAP	Specifies the SAP assigned to the service.

sap-using

Syntax

sap-using [**sap** *sap-id*]

sap-using interface [*ip-address* | *ip-int-name*]

sap-using [**ingress** | **egress**] **filter** *filter-id*

sap-using [**ingress**] **qos-policy** *qos-policy-id*

Context

show>service

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays SAP information.

If no optional parameters are specified, the command displays a summary of all defined SAPs. The optional parameters restrict output to only SAPs matching the specified properties.

Parameters

sap sap-id

Specifies the physical port identifier portion of the SAP definition. See Common CLI command descriptions for command syntax.

ingress

Specifies matching an ingress policy.

egress

Specifies matching an egress policy.

filter *filter-id*

Specifies the ingress or egress filter policy ID for which to display matching SAPs.

Values 1 to 65535

interface

Specifies matching SAPs with the specified IP interface.

ip-addr

Specifies the IP address of the interface for which to display matching SAPs.

Values a.b.c.d

ip-int-name

Specifies the IP interface name for which to display matching SAPs.

Output

The following output is an example of service SAP information, and Table 86: Output fields: service SAP describes the output fields.

Sample output

```
*A:DUT-B# show service sap-using sap 1/1/3:100.*
===============================================================================
Service Access Points
===============================================================================
PortId                          SvcId      Ing.  Ing.    Egr.   Adm  Opr
                                           QoS   Fltr    Fltr
-------------------------------------------------------------------------------
1/1/1                           6          1     none    none   Up   Down
1/1/2                           700        1     none    none   Up   Down
-------------------------------------------------------------------------------
Number of SAPs : 2
===============================================================================
*A:DUT-B#
```

Table 86: Output fields: service SAP

Label	Description
Port ID	The ID of the access port where the SAP is defined.
Svc ID	The value that identifies the service.
SapMTU	The SAP MTU value.
Igr.QoS	The SAP ingress QoS policy number specified on the ingress SAP.
Ing.Fltr	The MAC or IP filter policy ID applied to the ingress SAP.
E.QoS	The SAP egress QoS policy number specified on the egress SAP.
Egr.Fltr	The MAC or IP filter policy ID applied to the egress SAP.

Label	Description
A.Pol	The accounting policy ID assigned to the SAP.
Adm	The administrative state of the SAP.
Opr	The actual state of the SAP.

service-using

Syntax

service-using [**ies**] [**customer** *customer-id*]

Context

show>service

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays the services matching certain usage properties. If no optional parameters are specified, the output displays all services defined on the system.

Parameters

ies

Displays matching IES services.

customer *customer-id*

Displays services only associated with the specified customer ID.

Values 1 to 2147483647

Default Services associated with an customer.

Output

The following output is an example of service information, and Table 87: Output fields: service-using describes the output fields.

Sample output

```
A:ALA-48# show service service-using ies
===============================================================================
Services [ies]
===============================================================================
ServiceId    Type      Adm    Opr        CustomerId        Last Mgmt Change
-------------------------------------------------------------------------------
88           IES       Up     Down       8                 07/25/2006 15:46:28
89           IES       Up     Down       8                 07/25/2006 15:46:28
104          IES       Up     Down       1                 07/25/2006 15:46:28
```

```
200          IES       Up     Down       1                  07/25/2006 15:46:28
214          IES       Up     Down       1                  07/25/2006 15:46:28
321          IES       Up     Down       1                  07/25/2006 15:46:28
322          IES       Down   Down       1                  07/25/2006 15:46:28
1001         IES       Up     Down       1730               07/25/2006 15:46:28
-------------------------------------------------------------------------------
Matching Services : 8
-------------------------------------------------------------------------------
A:ALA-48#
```

Table 87: Output fields: service-using

Label	Description
Service Id	The value that identifies the service.
Type	Specifies the service type configured for the service ID.
Adm	The administrative state of the service.
Opr	The operating state of the service.
CustomerID	The ID of the customer who owns this service.
Last Mgmt Change	The date and time of the most recent management-initiated change to this service.

id

Syntax

id *service-id* {**all** | **arp** | **base** | **sap**}

Context

show>service

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays information for a particular service ID.

Parameters

service-id

Specifies the unique service identification number to identify the service in the service domain.

all

Displays detailed information about the service.

arp

Displays ARP entries for the service.

base

Displays basic service information.

sap

Displays SAPs associated with the service.

all

Syntax

all

Context

show>service>id

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays detailed information for all aspects of the service.

Output

Table 88: Output fields: service ID all describes the show all service-id command output fields.

Sample output

Table 88: Output fields: service ID all

Label	Description
Service Detailed Information	
Service Id	The service identifier.
VPN Id	The number that identifies the VPN.
Service Type	Displays the type of service.
SDP Id	The SDP identifier.
Description	Generic information about the service.
Customer Id	The customer identifier.
Last Mgmt Change	The date and time of the most recent management-initiated change to this customer.
SAP Count	The number of SAPs specified for this service.

Label	Description
SDP Bind Count	The number of SDPs bound to this service.
Service Destination Points (SDPs)	
SDP Id	The SDP identifier.
Type	Indicates whether this Service SDP binding is a spoke or a mesh.
Admin Path MTU	The largest service frame size (in octets) that can be transmitted through this SDP to the far-end router, without requiring the packet to be fragmented.
Oper Path MTU	The actual largest service frame size (in octets) that can be transmitted through this SDP to the far-end router, without requiring the packet to be fragmented.
Delivery	Specifies the type of delivery used by the SDP: MPLS.
Admin State	The administrative state of this SDP.
Oper State	The operational state of this SDP.
Ingress Label	The label used by the far-end device to send packets to this device in this service by this SDP.
Egress Label	The label used by this device to send packets to the far-end device in this service by this SDP.
Ingress Filter	The ID of the ingress filter policy.
Egress Filter	The ID of the egress filter policy.
Far End	Specified the IP address of the remote end of the MPLS tunnel defined by this SDP.
Last Changed	The date and time of the most recent change to this customer.
Signaling	Specifies the signaling protocol used to obtain the ingress and egress labels used in frames transmitted and received on this SDP.
Admin State	Specifies the operating status of the service.
Oper State	The current status of the service.
Hello Time	Specifies how often the SDP echo request messages are transmitted on this SDP.
Hello Msg Len	Specifies the length of the SDP echo request messages transmitted on this SDP.

Label	Description
Max Drop Count	Specifies the maximum number of consecutive SDP Echo Request messages that can be unacknowledged before the keepalive protocol reports a fault.
Hold Down Time	Specifies the amount of time to wait before the keepalive operating status is eligible to enter the alive state.
SDP Delivery Mechanism	When the SDP type is MPLS, a list of LSPs used to reach the far-end router displays. All the LSPs in the list must terminate at the IP address specified in the far-end field.
Number of SDPs	The total number SDPs applied to this service ID.
Service Access Points	
Service Id	The service identifier.
Port Id	The ID of the access port where this SAP is defined.
Description	Generic information about the SAP.
Encap	The value of the label used to identify this SAP on the access port.
Admin State	The desired state of the SAP.
Oper State	The operating state of the SAP.
Last Changed	The date and time of the last change.
Admin MTU	The largest service frame size (in octets) that can be transmitted through this SDP to the far-end router, without requiring the packet to be fragmented.
Oper MTU	The actual largest service frame size (in octets) that can be transmitted through this SDP to the far-end router, without requiring the packet to be fragmented.
Ingress qos-policy	The SAP ingress QoS policy ID.
Egress qos-policy	The SAP egress QoS policy ID.
Ingress Filter-Id	The SAP ingress filter policy ID.
Egress Filter-Id	The SAP egress filter policy ID.
Multi Svc Site	Indicates the multi-service site that the SAP is a member.
Ingress sched-policy	Indicates the ingress QoS scheduler for the SAP.
Egress sched-policy	Indicates the egress QoS scheduler for the SAP.

Label	Description
Table-based	Indicates the use of table-based resource classification: Enabled (table-based) or Disabled (CAM-based)
Dscp Class Pol Id	Indicates the DSCP classification policy ID.
Acct. Pol	Indicates the accounting policy applied to the SAP.
Collect Stats	Displays whether accounting statistics are collected on the SAP.
SAP Statistics	
Dropped	The number of packets or octets dropped.
Offered Hi Priority	The number of high priority packets, as determined by the SAP ingress QoS policy.
Offered Low Priority	The number of low priority packets, as determined by the SAP ingress QoS policy.
Forwarded In Profile	The number of in-profile packets or octets (rate below CIR) forwarded.
Forwarded Out Profile	The number of out-of-profile packets or octets (rate above CIR) forwarded.

arp

Syntax

arp [*ip-address*] | [**mac** *ieee-address*] | [**sap** *sap-id*] | [**interface** *ip-int-name*]

Context

show>service>id

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays the ARP table for the IES instance. The ARP entries for a subscriber interface are displayed uniquely. Each MAC associated with the subscriber interface child group-interfaces are displayed with each subscriber interface ARP entry. They do not reflect actual ARP entries but are displayed along the interfaces ARP entry for easy lookup.

Parameters

ip-address

Displays only ARP entries in the ARP table with the specified IP address.

Default All IP addresses.

mac *ieee-address*

Displays only ARP entries in the ARP table with the specified 48-bit MAC address. The MAC address can be expressed in the form aa:bb:cc:dd:ee:ff or aa-bb-cc-dd-ee-ff where aa, bb, cc, dd, ee and ff are hexadecimal numbers.

Default All MAC addresses.

sap *sap-id*

Displays SAP information for the specified SAP ID. See Common CLI command descriptions for command syntax.

interface *ip-int-name*

Specifies matching service ARP entries associated with the IP interface.

ip-address

Specifies the IP address of the interface for which to display matching ARP entries.

Values a.b.c.d

ip-int-name

Specifies the IP interface name for which to display matching ARPs.

Output

The following output is an example of ARP information, and Table 89: Output fields: service ID ARP describes the output fields.

Sample output

```
*A:DUT-B# show service id 100 arp
===============================================================================
ARP Table
===============================================================================
IP Address      MAC Address         Type       Expiry    Interface         SAP
-------------------------------------------------------------------------------
192.168.1.2     00:00:01:00:00:01  Other     00h00m00s   HW                1/1/1:10*
192.168.1.1     32:67:01:01:00:03  Other     00h00m00s   to7x              1/1/3:10*
192.168.2.2     32:68:01:01:00:02  Dynamic   03h59m58s   to7x              1/1/3:10*
===============================================================================
*A:DUT-B#
```

Table 89: Output fields: service ID ARP

Label	Description
IP Address	The IP address.
MAC Address	The specified MAC address.
Type	Static — FDB entries created by management Learned — Dynamic entries created by the learning process Other — Local entries for the IP interfaces created

Label	Description
Expiry	The age of the ARP entry.
Interface	The interface applied to the service.
SAP	The SAP ID.

base

Syntax

base

Context

show>service>id

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays basic information about this IES service.

Output

The following output is an example of basic IES service information, and Table 90: Output fields: service ID base describes the output fields.

Sample output

```
*A:ALA-A# show service id 100 base
-------------------------------------------------------------
Service Basic Information
-------------------------------------------------------------
Service Id        : 100                Vpn Id            : 100
Service Type      : IES
Description       : Default Ies description for service id 100
Customer Id       : 1
Last Status Change: 08/29/2006 17:44:28
Last Mgmt Change  : 08/29/2006 17:44:28
Admin State       : Up                 Oper State        : Up
SAP Count         : 2
-------------------------------------------------------------------------------
Service Access & Destination Points
-------------------------------------------------------------------------------
Identifier                      Type         AdmMTU  OprMTU  Adm     Opr
-------------------------------------------------------------------------------
sap:1/1/3                       null         1514    1514    Up      Up
sap:1/1/4                       null         1514    1514    Up      Up
===============================================================================
*A:ALA-A#
```

Table 90: Output fields: service ID base

Label	Description
Service Basic Information	
Service Id	Service ID number.
Service Type	Type of service.
Description	Generic information about the service.
Customer Id	Customer ID number.
Last Status Change	Date and time of the most recent status change to this service.
Last Mgmt Change	Date and time of the most recent management-initiated change to this service.
Admin State	Configured state of the service.
Oper State	Operating state of the service.
SAP Count	Number of SAPs specified for this service.
Service Access & Destination Points	
Identifier	SAP ID.
Type	Signaling protocol used to obtain the ingress and egress labels used in frames transmitted and received.
AdmMTU	Configured largest service frame size (in octets) that can be transmitted to the far-end router without requiring the packet to be fragmented.
OprMTU	Actual largest service frame size (in octets) that can be transmitted to the far-end router without requiring the packet to be fragmented.
Adm	Administrative state of the SAP.
Opr	Operating state of the SAP.

interface

Syntax

interface [*ip-address* | *ip-int-name*] [**detail**]

Context

show>service>id

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays information for the IP interfaces associated with the IES service. If no optional parameters are specified, the outputs displays a summary of all IP interfaces associated with the service.

Parameters

ip-address

Specifies the IP address of the interface for which to display information.

Values ipv4-address: a.b.c.d (host bits must be 0)

ip-int-name

Specifies the IP interface name for which to display information.

Values 32 characters maximum

detail

Displays detailed IP interface information.

Default IP interface summary output.

Output

The following outputs are examples of IES service interface information, and Table 91: Output fields: service ID interface describes the output fields.

Sample output

```
A:ALA-49# show service id 88 interface
===============================================================================
Interface Table
===============================================================================
Interface-Name Adm Opr(v4/v6) Type Port/SapId
IP-Address PfxState
-------------------------------------------------------------------------------
Sector A Up Down/Down IES 1/1/1.2.2
- -
test Up Down/Down IES 1/1/2:0
10.1.1.1/31 n/a
10.1.1.1/31 n/a
10.1.2.1/31 n/a
test27 Up Up/-- IES Sub subscriber
192.168.10.21/24 n/a
grp-if Up Down/-- IES Grp 1/2/2
Interfaces : 4
===============================================================================
A:ALA-49#
```

Sample output for 7210 SAS-R6 and 7210 SAS-R12

The following output is an example of 7210 SAS-R6 and 7210 SAS-R12 IES routed VPLS interface override.

```
*A:Dut-A# show service id 2000 interface "iesRvplsIngr" detail
```

```
===============================================================================
Interface Table
===============================================================================
-------------------------------------------------------------------------------
Interface
-------------------------------------------------------------------------------
If Name      : iesRvplsIngr
Admin State  : Up                              Oper (v4/v6)     : Down/Down
Down Reason C: assocObjNotReady
Protocols    : None
IP Addr/mask : 10.55.55.2/24                   Address Type     : Primary
IGP Inhibit  : Disabled                        Broadcast Address: Host-ones
HoldUp-Time  : 0                               Track Srrp Inst  : 0
-------------------------------------------------------------------------------
Details
-------------------------------------------------------------------------------
Description  : (Not Specified)
If Index     : 14                              Virt. If Index   : 14
Last Oper Chg: 11/07/2017 04:48:25             Global If Index  : 206
Mon Oper Grp : None
Srrp En Rtng : Disabled                        Hold time        : N/A
Port Id      : rvpls
TOS Marking  : Untrusted                       If Type          : IES
SNTP B.Cast  : False                           IES ID           : 2000
MAC Address  : c4:08:4a:45:c0:e4               Mac Accounting   : Disabled
Ingress stats: Disabled                        IPv6 DAD         : Enabled
ARP Timeout  : 14400s                          IPv6 Nbr ReachTi*: 30s
ARP Retry Ti*: 5000ms                          IPv6 stale time  : 14400s
ARP Limit    : Disabled                        IPv6 Nbr Limit   : Disabled
ARP Threshold: Disabled                        IPv6 Nbr Thresho*: Disabled
ARP Limit Lo*: Disabled                        IPv6 Nbr Log Only: Disabled
IP MTU       : (default)
IP Oper MTU  : 9198
LdpSyncTimer : None
LSR Load Bal*: system
EGR Load Bal*: both
Vas If Type  : none
TEID Load Ba*: Disabled
SPI Load Bal*: Disabled
uRPF Chk     : disabled
uRPF Ipv6 Chk: disabled
Mpls Rx Pkts : 0                               Mpls Rx Bytes    : 0
Mpls Tx Pkts : 0                               Mpls Tx Bytes    : 0

DHCP6 Relay Details
Description  : (Not Specified)
Admin State  : Down                            Lease Populate   : 0
Oper State   : Down                            Nbr Resolution   : Disabled
If-Id Option : None                            Remote Id        : Disabled
Src Addr     : Not configured
Python plcy  : (Not Specified)

DHCP6 Server Details
Admin State  : Down                            Max. Lease States: 8000

ICMP Details
Redirects    : Number - 100                    Time (seconds)   - 10
Unreachables : Number - 100                    Time (seconds)   - 10
TTL Expired  : Number - 100                    Time (seconds)   - 10

Routed VPLS Details
VPLS Name        : ingRvpls
Binding Status   : Up
Reason           : (Not Specified)
```

```
Egr Reclass Plcy : 0
Ing Filter       : none
Ingr IPv6 Flt    : none
EVPN Tunnel      : false
Table-based      : enabled
Dscp Class Pol Id: 1

Network Domains Associated
default

-------------------------------------------------------------------------------
Admin Groups
-------------------------------------------------------------------------------
No Matching Entries
-------------------------------------------------------------------------------

-------------------------------------------------------------------------------
Srlg Groups
-------------------------------------------------------------------------------
No Matching Entries
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
Interfaces : 1
===============================================================================
* indicates that the corresponding row element may have been truncated.
*A:Dut-A#
```

Table 91: Output fields: service ID interface

Label	Description
If Name	The name of the IES interface.
Type	Specifies the interface type.
IP-Address	Specifies the IP address/IP subnet/broadcast address of the interface.
Adm	The administrative state of the interface.
Opr	The operational state of the interface.
Admin State	The administrative state of the interface.
Oper State	The operational state of the interface.
IP Addr/mask	Specifies the IP address/IP subnet/broadcast address of the interface.
If Index	The index corresponding to this IES interface. The primary index is 1; all IES interfaces are defined in the base virtual router context.
If Type	Specifies the interface type.
SAP Id	Specifies the SAP port ID.

Label	Description
SNTP B.Cast	Specifies whether SNTP broadcast client mode is enabled or disabled.
Arp Timeout	Specifies the timeout for an ARP entry learned on the interface.
MAC Address	Specifies the 48-bit IEEE 802.3 MAC address.
ICMP Mask Reply	Specifies whether ICMP mask reply is enabled or disabled.
Cflowd	Specifies whether cflowd collection and analysis on the interface is enabled or disabled.
Redirects	Specifies the rate for ICMP redirect messages.
Unreachables	Specifies the rate for ICMP unreachable messages.
TTL Expired	Specifies the rate for ICMP TTL messages.

7 Virtual Private Routed Network service

This chapter provides information about the Virtual Private Routed Network (VPN) service and implementation notes. VPRN services are supported only in network mode.

7.1 VPRN service overview

RFC2547b is an extension to the original RFC 2547, which details a method of distributing routing information and forwarding data to provide a Layer 3 Virtual Private Network (VPN) service to end customers.

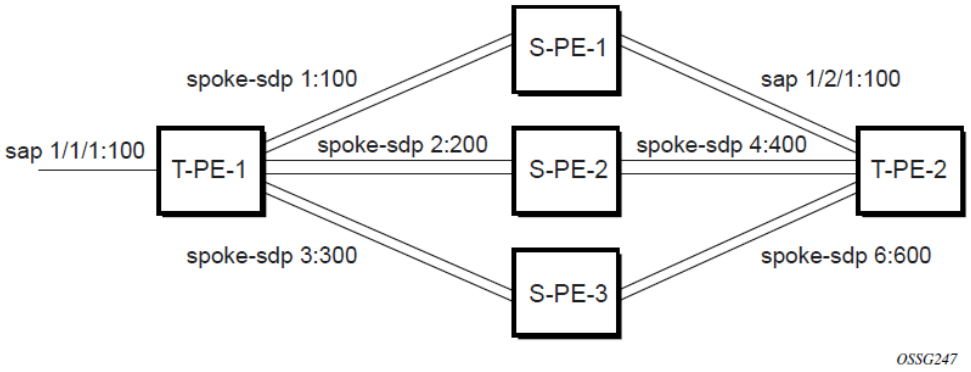
Each Virtual Private Routed Network (VPRN) consists of a set of customer sites connected to one or more PE routers. Each associated PE router maintains a separate IP forwarding table for each VPRN. Additionally, the PE routers exchange the routing information configured or learned from all customer sites via MP-BGP peering. Each route exchanged via the MP-BGP protocol includes a Route Distinguisher (RD), which identifies the VPRN association.

The service provider uses BGP to exchange the routes of a particular VPN among the PE routers that are attached to that VPN. This is done in a way which ensures that routes from different VPNs remain distinct and separate, even if two VPNs have an overlapping address space. The PE routers distribute routes from other CE routers in that VPN to the CE routers in a particular VPN. Because the CE routers do not peer with each other, there is no overlay visible to the VPN routing algorithm.

When BGP distributes a VPN route, it also distributes an MPLS label for that route. On a SR-Series, the label distributed with a VPN route depends on the configured label-mode of the VPRN that is originating the route.

Before a customer data packet travels across the service provider's backbone, it is encapsulated with the MPLS label that corresponds, in the customer's VPN, to the route which best matches the packet's destination address. The MPLS packet is further encapsulated with either another MPLS label header, so that it gets tunneled across the backbone to the correct PE router. Each route exchanged by the MP-BGP protocol includes a route distinguisher (RD), which identifies the VPRN association. Therefore the backbone core routers do not need to know the VPN routes. The following figure shows a VPRN network diagram example.

Figure 67: Virtual Private Routed Network



7.1.1 Routing prerequisites

RFC2547bis requires the following features:

- Multi-protocol extensions
- Extended BGP community support
- BGP capability negotiation
- Parameters defined in RFC 2918

Tunneling protocol options are as follows:

- Label Distribution Protocol (LDP)
- MPLS RSVP-TE tunnels

7.1.2 BGP support

BGP is used with BGP extensions mentioned in Routing prerequisites to distribute VPRN routing information across the service provider network.

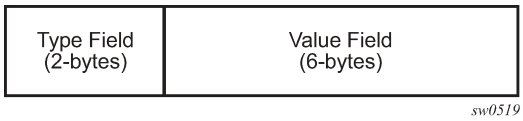
BGP was initially designed to distribute IPv4 routing information. Therefore, multi-protocol extensions and the use of a VPN-IPv4 address were created to extend ability of the BGP to carry overlapping routing information. A VPN-IPv4 address is a 12-byte value consisting of the 8-byte route distinguisher (RD) and the 4-byte IPv4 IP address prefix. The RD must be unique within the scope of the VPRN. This allows the IP address prefixes within different VRFs to overlap.

A VPN-IPv6 address is a 24-byte value consisting of the 8-byte RD and 16-byte IPv6 address prefix. Service providers typically assign one or a small number of RDs per VPN service network-wide.

7.1.3 Route distinguishers

The route distinguisher (RD) is an 8-byte value consisting of 2 major fields, the Type field and Value field, as shown in the following figure. The Type field determines how the Value field should be interpreted. The 7210 SAS implementation supports the three (3) Type values as defined in the Internet draft.

Figure 68: Route distinguisher



The three Type values are:

- **Type 0: Value Field - Administrator subfield (2 bytes)** Assigned number subfield (4 bytes)

  The administrator field must contain an ASN (using private AS numbers is discouraged). The Assigned field contains a number assigned by the service provider.

- **Type 1: Value Field - Administrator subfield (4 bytes)** Assigned number subfield (2 bytes)

  The administrator field must contain an IP address (using private IP address space is discouraged). The Assigned field contains a number assigned by the service provider.

- **Type 2: Value Field - Administrator subfield (4 bytes)** Assigned number subfield (2 bytes)

  The administrator field must contain a 4-byte ASN (using private AS numbers is discouraged). The Assigned field contains a number assigned by the service provider.

7.1.3.1 Route reflector

Per RFC2547bis the use of Route Reflectors is supported in the service provider core. Multiple sets of route reflectors can be used for different types of BGP routes, including IPv4 and VPN-IPv6. 7210 can only be used a route reflector client. It cannot be used as a route reflector ("server").

7.1.3.2 CE to PE route exchange

Routing information between the Customer Edge (CE) and Provider Edge (PE) can be exchanged by the following methods:

- Static Routes (with both IPv4 and IPv6)
- E-BGP (with both IPv4 and IPv6 VPNs)

Each protocol provides controls to limit the number of routes learned from each CE router.

7.1.3.2.1 Route redistribution

Routing information learned from the CE-to-PE routing protocols and configured static routes should be injected in the associated local VPN routing/forwarding (VRF). In the case of dynamic routing protocols, there may be protocol-specific route policies that modify or reject some routes before they are injected into the local VRF.

Route redistribution from the local VRF to CE-to-PE routing protocols is to be controlled via the route policies in each routing protocol instance, in the same manner that is used by the base router instance.

The advertisement or redistribution of routing information from the local VRF to or from the MP-BGP instance is specified per VRF and is controlled by VRF route target associations or by VRF route policies.

VPN-IP routes imported into a VPRN, have the protocol **type bgp-vpn** to denote that it is an VPRN route. This can be used within the route policy match criteria.

7.1.3.2.2 CPE connectivity check

Static routes are used within many IES and VPRN services. Unlike dynamic routing protocols, there is no way to change the state of routes based on availability information for the associated CPE. CPE connectivity check adds flexibility so that unavailable destinations are removed from the VPRN routing tables dynamically and minimize wasted bandwidth.

The following figures show static routes.

Figure 69: Directly connected IP target

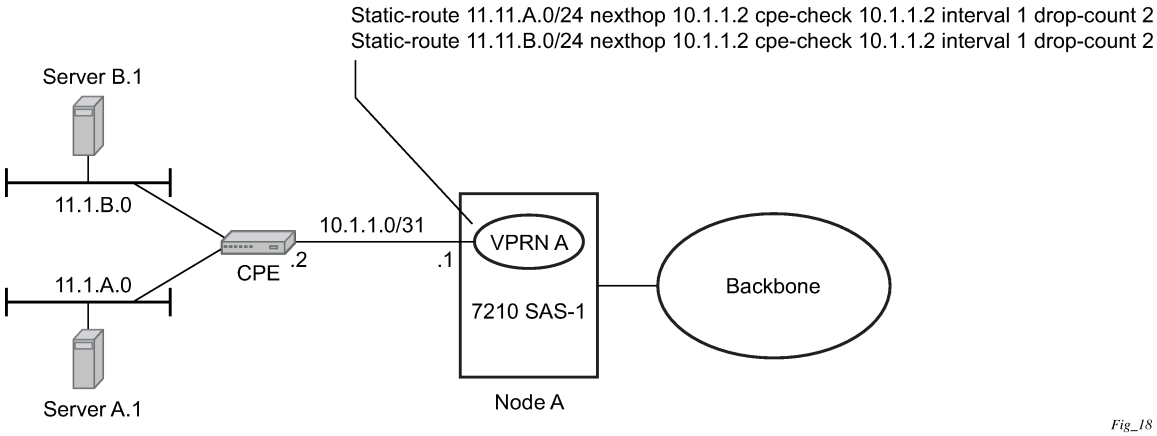
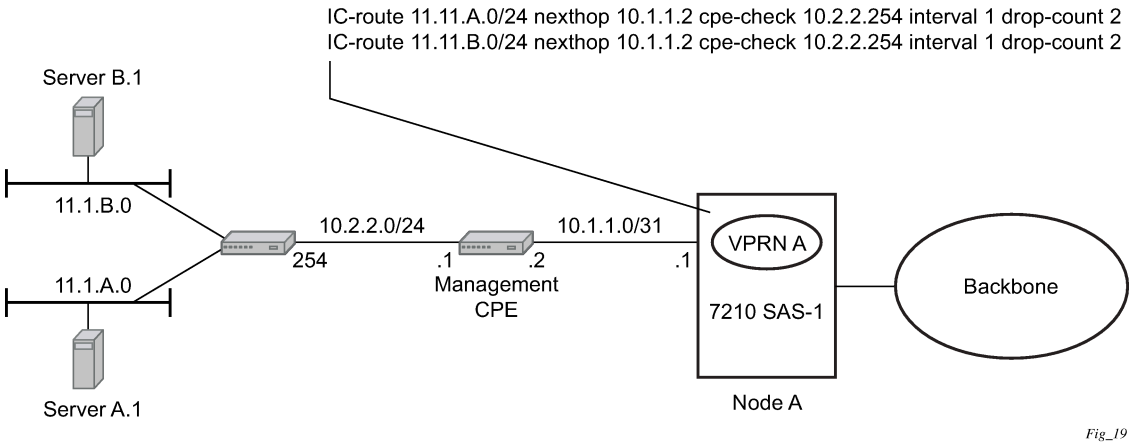


Figure 70: Multiple hops to IP target



The availability of the far-end static route is monitored through periodic polling. The polling period is configured. If the poll fails a specified number of sequential polls, the static route is marked as inactive.

Either ICMP ping or unicast ARP mechanism can be used to test the connectivity. ICMP ping is preferred.

If the connectivity check fails and the static route is de-activated, the 7210 SAS router continues to send polls and reactivate any routes that are restored.

7.1.4 Constrained route distribution

This section describes constrained route distribution or RT constraint (RTC).

7.1.4.1 Constrained VPN route distribution based on route targets

The RTC is a mechanism allows a router to advertise route target membership information to its BGP peers to indicate interest in receiving only VPN routes tagged with specific route target extended communities. After receiving this information, peers restrict the advertised VPN routes to only those requested, which minimizes the control plane load in terms of protocol traffic and possibly routing information base (RIB) memory.

MP-BGP carries the route target membership information, using an address family identifier (AFI) value of 1 and subsequent address family identifier (SAFI) value of 132. For two routers to exchange RT membership network layer reachability information (NLRI), they must advertise the corresponding AFI/SAFI to each other during capability negotiation. MP-BGP allows RT membership NLRI to be propagated, loop-free, within an AS and between ASs using well-known BGP route selection and advertisement rules.

Outbound route filtering (ORF) can also be used for RT-based route filtering, but ORF messages have a limited scope of distribution (to direct peers or neighbors), and, therefore, do not automatically create pruned inter-cluster and inter-AS route distribution trees.

7.1.4.2 Configuring the route target address family

RTC is supported only by the base router BGP instance. When the **family** command at the **bgp**, **group** or **neighbor** CLI context includes the **route-target** keyword, the RTC capability is negotiated with the associated set of eBGP and iBGP peers.

ORF and RT C are mutually exclusive on a specific BGP session. The CLI does not attempt to block this configuration, but if both capabilities are enabled on a session, the ORF capability is not included in the OPEN message sent to the peer.

7.1.4.3 Originating RT constraint routes

When the base router has one or more RTC peers (BGP peers with which the RTC capability has been successfully negotiated), one RTC route is created for each RT extended community imported into a locally-configured Layer-2 VPN or Layer-3 VPN service. These imported route targets are configured in the following contexts:

- **config>service>vpls>bgp**
- **config>service>vprn**
- **config>service>vprn>mvpn**

Note:
See the *7210 SAS-Mxp, R6, R12, S, Sx, T Routing Protocols Guide* for more information about BGP address families that support RTC.

By default, these RTC routes are automatically advertised to all RTC peers, without the need for an export policy to explicitly accept them. Each RTC route has a prefix, prefix length, and path attributes. The

prefix value is the concatenation of the origin AS (a 4-byte value representing the 2- or 4-octet AS of the originating router, as configured using the **configure router autonomous-system** command) and 0 or 16 to 64 bits of a route target extended community encoded in one of the following formats: 2-octet AS specific extended community, IPv4 address specific extended community, or 4-octet AS specific extended community.

A router may be configured to send the default RTC route to any RTC peer using the new **default-route-target group** or **neighbor** CLI command. The default RTC route is a special type of RTC route that has zero prefix length. Sending the default RTC route to a peer conveys a request to receive all VPN routes (regardless of route target extended community) from that peer. The default RTC route is typically advertised by a route reflector to its clients. The advertisement of the default RTC route to a peer does not suppress other, more specific, RTC routes from being sent to that peer.

7.1.4.4 Receiving and re-advertising RT constraint routes

All received RTC routes that are deemed valid are stored in the RIB-IN. An RTC route is considered invalid and treated as withdrawn if any of the following conditions apply:

- The prefix length is 1 to 31.
- The prefix length is 33 to 47.
- The prefix length is 48 to 96 and the 16 most-significant bits are not 0x0002, 0x0102, or 0x0202.

If multiple RTC routes are received for the same prefix value, standard BGP best path selection procedures are used to determine the best of these routes.

The best RTC route per prefix is re-advertised to RTC peers based on the following rules:

- The best path for a default RTC route (prefix length 0, origin AS only with prefix length 32, or origin AS plus 16 bits of an RT type with prefix length 48) is never propagated to another peer.
- A PE with only iBGP RTC peers that is neither a route reflector nor an AS boundary router (ASBR) does not re-advertise the best RTC route to any RTC peer because of standard iBGP split horizon rules.
- A route reflector that receives its best RTC route for a prefix from a client peer re-advertises that route (subject to export policies) to all of its client and non-client iBGP peers (including the originator), per standard RR operation. When the route is re-advertised to client peers, the RR sets the ORIGINATOR_ID to its own router ID and modifies the NEXT_HOP to be its local address for the sessions (for example, system IP).
- A route reflector that receives its best RTC route for a prefix from a non-client peer re-advertises that route (subject to export policies) to all of its client peers, per standard RR operation. If the RR has a non-best path for the prefix from any of its clients, it advertises the best of the client-advertised paths to all non-client peers.
- An ASBR that is neither a PE nor a route reflector that receives its best RTC route for a prefix from an iBGP peer re-advertises that route (subject to export policies) to its eBGP peers. It modifies the NEXT_HOP and AS_PATH of the re-advertised route per standard BGP rules. The aggregation of RTC routes is not supported.
- An ASBR that is neither a PE nor a route reflector that receives its best RTC route for a prefix from an eBGP peer re-advertises that route (subject to export policies) to its eBGP and iBGP peers. When re-advertised routes are sent to eBGP peers, the ASBR modifies the NEXT_HOP and AS_PATH per standard BGP rules. The aggregation of RTC routes is not supported.

Note: These advertisement rules do not handle hierarchical RR topologies properly. This is a limitation of the current RT constraint standard.

7.1.4.5 Using RT constraint routes

In general (ignoring iBGP-to-iBGP rules, add-path, best-external, and so on), the best VPN route for every prefix/NLRI in the RIB is sent to every peer supporting the VPN address family, but export policies may be used to prevent the advertisement of some prefix/NLRIs to specific peers. These export policies may be configured statically or created dynamically based on use of ORF or RTC with a peer. ORF and RTC are mutually exclusive on a session.

When RTC is configured on a session that also supports VPN address families using route targets (vpn-ipv4, vpn-ipv6, and so on), the advertisement of the VPN routes is affected as follows:

- When the session comes up, the advertisement of the VPN routes is delayed briefly to allow RTC routes to be received from the peer.
- After the initial delay, the received RTC routes are analyzed and acted upon. If S1 is the set of routes previously advertised to the peer and S2 is the set of routes that should be advertised based on the most recent received RTC routes, the following applies:
  - The set of routes in S1 but not in S2 should be withdrawn immediately (subject to the minimum route advertisement interval (MRAI)).
  - The set of routes in S2 but not in S1 should be advertised immediately (subject to MRAI).
- If a default RTC route is received from a peer P1, the VPN routes that are advertised to P1 are the set that:
  - are eligible for advertisement to P1 per BGP route advertisement rules
  - have not been rejected by manually configured export policies
  - have not been advertised to the peer

  Note: This applies regardless of whether P1 advertised the best route for the default RTC prefix.

In this context, a default RTC route is any of the following:

- a route with NLRI length = zero
- a route with NLRI value = origin AS and NLRI length = 32
- a route with NLRI value = {origin AS+0x0002 | origin AS+0x0102 | origin AS+0x0202} and NLRI length = 48
  - If an RTC route for prefix A (origin-AS = A1, RT = A2/n, n > 48) is received from an iBGP peer I1 in autonomous system A1, the VPN routes that are advertised to I1 is the set that:
    - are eligible for advertisement to I1 per BGP route advertisement rules
    - have not been rejected by manually configured export policies
    - carry at least one route target extended community with value A2 in the n most significant bits
    - have not been advertised to the peer

    Note: This applies regardless of whether I1 advertised the best route for A.

– If the best RTC route for a prefix A (origin-AS = A1, RT = A2/n, n > 48) is received from an IBGP peer I1 in autonomous system B, the VPN routes that are advertised to I1 is the set that:
  - are eligible for advertisement to I1 per BGP route advertisement rules
  - have not been rejected by manually configured export policies
  - carry at least one route target extended community with value A2 in the n most significant bits
  - have not been advertised to the peer

  Note: This applies only if I1 advertised the best route for A.

– If the best RTC route for a prefix A (origin-AS = A1, RT = A2/n, n > 48) is received from an eBGP peer E1, the VPN routes that are advertised to E1 is the set that:
  - are eligible for advertisement to E1 per BGP route advertisement rules
  - have not been rejected by manually configured export policies
  - carry at least one route target extended community with value A2 in the n most significant bits
  - have not been advertised to the peer

  Note: This applies only if E1 advertised the best route for A.

7.1.5 BGP fast reroute in a VPRN

BGP fast reroute is a feature that brings together indirection techniques in the forwarding plane and precomputation of BGP backup paths in the control plane to support fast reroute of BGP traffic around unreachable/failed next-hops. In a VPRN context BGP fast reroute is supported using VPN-IPv4 and VPN-IPv6 VPN routes. The supported VPRN scenarios are described in the following table.

Table 92: BGP fast reroute scenarios (VPRN Context)

Ingress packet	Primary route	Backup route	Prefix independent convergence
IPv4 (ingress PE)	VPN-IPv4 route with next-hop A resolved by a LDP, RSVP or BGP tunnel	VPN-IPv4 route with next-hop A resolved by a LDP, RSVP or BGP tunnel	Yes
IPv6 (ingress PE)	VPN-IPv6 route with next-hop A resolved by a LDP, RSVP or BGP tunnel	VPN-IPv6 route with next-hop B resolved by a LDP, RSVP or BGP tunnel	Yes

7.1.5.1 BGP fast reroute in a VPRN configuration

Configuring the **enable-bgp-vpn-backup** command under **config>service>vprn** causes only imported BGP-VPN routes to be considered when selecting the primary and backup paths.

This command is required to support fast failover of ingress traffic from one remote PE to another remote PE.

Note: 7210 SAS devices do not support BGP backup path command that is used to enable consideration of multiple paths learned from CE BGP peers when selecting primary and backup path to reach the CE.

7.2 VPRN features

This section describes various VPRN features and any special capabilities or considerations as they relate to VPRN services.

7.2.1 IP interfaces

VPRN customer IP interfaces can be configured with most of the same options found on the core IP interfaces.

The advanced configuration options supported are:

- DHCPv4 relay
- VRRP for IPv4 interface
- Secondary IP addresses
- ICMP options

NTP broadcast receipt configuration options found on core IP interfaces are not supported on VPRN IP interfaces.

7.2.2 SAPs

This section provides information about SAPs.

7.2.2.1 IPv6 support for VPRN IP interfaces (in network mode)

VPRN IPv6 access interfaces are allowed to be configured to provide IPv6 VPN connectivity to customers.

IPv4 and IPv6 route table lookup entries are shared. Before adding routes for IPv6 destinations, route entries in the routed lookup table needs to be allocated for IPv6 addresses. This can be done using the **config>system>resource-profile>router>max-ipv6-routes** command. This command allocates route entries for /64 IPv6 prefix route lookups. The system does not allocate any IPv6 route entries by default and user needs to allocate some resources before using IPv6. For the command to take effect the node must be rebooted after making the change. For more information, see the following example and the *7210 SAS-Mxp, R6, R12, S, Sx, T Basic System Configuration Guide*.

A separate route table (or a block in the route table) is used for IPv6 /128-bit prefix route lookup. A limited amount of IPv6 /128 prefixes route lookup entries is supported. The software enables lookups in this table by default (that is, no user configuration is required to enable IPv6 /128-bit route lookup).

In addition, the number IP subnets can be configured by the user using the **configure> system>resource-profile>router>max-ip-subnets command**. Suitable default are assigned to this parameter. Users can increase the number of subnets if they plan to more IPv6 addresses per IPv6 interface.

Following features and restrictions are applicable for IPv6 VPRN IP interfaces:

- PE-CE routing - static routing and EBGP is supported
- A limited amount of IPv6 /128 prefixes route lookup entries is supported on 7210 SAS platforms.
- VRRP for VPRN IPv6 interfaces is not supported.

7.2.2.2 Encapsulations

The following SAP encapsulations are supported on the 7210 SAS VPRN service:

- Ethernet null
- Ethernet dot1q
- QinQ
- LAG

7.2.3 QoS policies

When applied to a VPRN SAP, service ingress QoS policies only create the unicast queues defined in the policy (as multicast is not supported in VPRN service).

Multicast is not supported in VPRN service.

Both Layer 2 (dot1p only) or Layer 3 criteria can be used in the QoS policies for traffic classification in an VPRN.

7.2.4 Filter policies

Ingress and egress IPv4 and IPv6 filter policies can be applied to VPRN SAPs.

7.2.4.1 CPU QoS for VPRN interfaces

Traffic bound to CPU received on VPRN access interfaces are policed/rate-limited and queued into CPU queues. The software allocates a policer per IP application or a set of IP applications, for rate-limiting CPU bound IP traffic from all VPRN access SAPs. The policers CIR/PIR values are set to appropriate values based on feature scaling and these values are not user configurable. The software allocates a set of queues for CPU bound IP traffic from all VPRN access SAPs. The queues are either shared by a set of IP applications or in some cases allocated to an IP application. The queues are shaped to appropriate rate based on feature scaling. The shaper rate is not user-configurable.

Note:

- The instance of queues and policers used for traffic received on network port IP interfaces is different for traffic received from access port IP interfaces. Additionally, the network CPU queues receive higher priority than the access CPU queues, which provides better security and mitigates the risk of access traffic affecting the network side.

- On the 7210 SAS-R6, the user can configure the IP DSCP value for self-generated traffic.

7.2.5 CE to PE routing protocols

The 7210 SAS VPRN supports the following PE to CE routing protocols:

- eBGP (for both IPv4 and IPv6)
- Static with both IPv4 and IPv6)
- OSPF v2 (IPv4)

7.2.5.1 PE to PE tunneling mechanisms

The 7210 SAS supports multiple mechanisms to provide transport tunnels for the forwarding of traffic between PE routers within the 2547bis network.

The 7210 SAS VPRN implementation supports the use of:

- RSVP-TE protocol to create tunnel LSP's between PE routers
- LDP protocol to create tunnel LSP's between PE routers

These transport tunnel mechanisms provide the flexibility of using dynamically created LSPs where the service tunnels are automatically bound (the "autobind" feature) and the ability to provide specific VPN services with their own transport tunnels by explicitly binding SDPs if needed. When the autobind is used, all services traverse the same LSPs and do not allow alternate tunneling mechanisms or the ability to craft sets of LSP's with bandwidth reservations for specific customers as is available with explicit SDPs for the service.

7.2.5.2 Per VRF route limiting

The 7210 SAS allows setting the maximum number of routes that can be accepted in the VRF for a VPRN service. There are options to specify a percentage threshold at which to generate an event that the VRF table is near full and an option to disable additional route learning when full or only generate an event.

7.2.6 Exporting MP-BGP VPN routes

To reduce the number of MP-BGP VPN tunnels in a group of IP/MPLS PE routers that are part of the same L3 VPN instance, a hierarchy can be established by reexporting the VPN IP routes on a PE aggregation router (which can be an ABR node). In the case of VPRN service labels, reexporting VPN IP routes reduces the required MPLS FIB resources to the scale available on smaller access routers.

Use the **config>service>vprn>allow-export-bgp-vpn** command to configure the feature. This command enables the **vrf-export** and **vrf-target** export functions to include BGP-VPN routes that are installed in the VPRN route table.

When a route is installed in the VPRN route table, the route is exported as a new VPN-IP route to an MP-IBGP peer only; that is, the route is accepted by the VRF export policy but may be rejected by a BGP export policy. Assuming that the export policies have simple accept and reject actions, the new VPN-IP route is the same as the original VPN-IP route, except in the following cases.

- The RD is changed to the value of the advertising VPRN.

- The BGP next-hop is changed to a local address of the PE.
- The label value is changed to the per-VRF label value of the advertising VPRN.

7.2.6.1 Configuration guidelines

The following configuration guidelines apply to this feature:

- You must shut down and restart the VPRN context for any changes to the **allow-export-bgp-vpn** command to take effect.
- You must configure the VPRN service with a loopback IP interface for the command to take effect.
- SAPs cannot be configured in a VPRN service in which the **allow-export-bgp-vpn** command is enabled.

7.2.7 Spoke SDPs

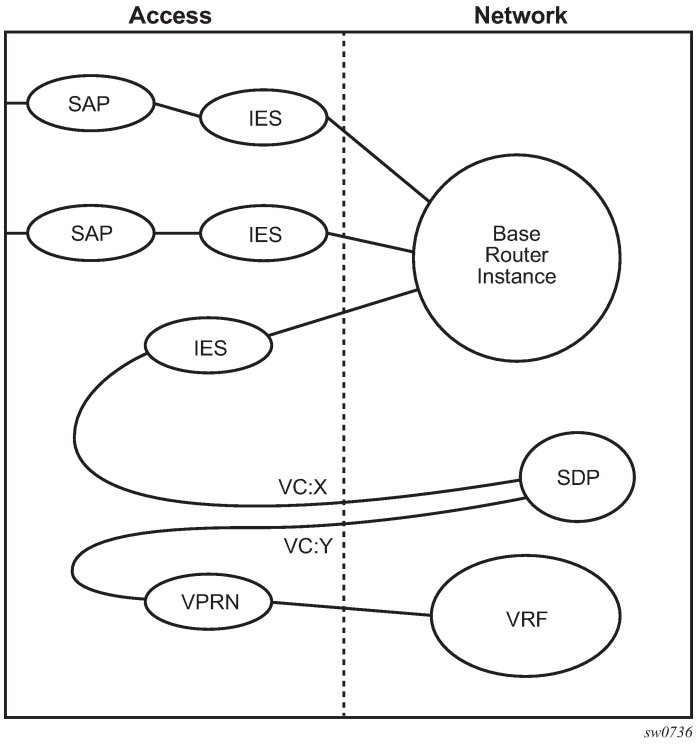
Spoke-SDP termination into a Layer 3 service is not supported on 7210 SAS platforms.

Distributed services use service distribution points (SDPs) to direct traffic to another SR-Series router via service tunnels. SDPs are created on each participating SR-Series and then bound to a specific service. SDP can be created as either GRE or MPLS. See SDPs for information about configuring SDPs.

This feature provides the ability to cross-connect traffic entering on a spoke-SDP, used for Layer 2 services (VLLs or VPLS), on to an IES or VPRN service. From a logical point of view, the spoke-SDP entering on a network port is cross-connected to the Layer 3 service as if it entered by a service SAP. The main exception to this is traffic entering the Layer 3 service by a spoke-SDP is handled with network QoS policies not access QoS policies.

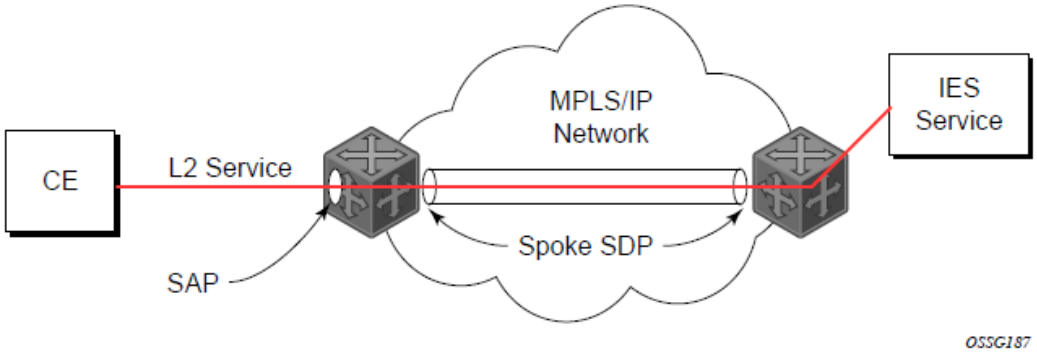
The following figure shows traffic terminating on a specific IES or VPRN service that is identified by the sdp-id and VC label present in the service packet.

Figure 71: SDP-ID and VC label service identifiers



The following figure shows a spoke-SDP terminating directly into an IES. In this case, a spoke-SDP could be tied to an Epipe or H-VPLS service. There is no configuration required on the PE connected to the CE.

Figure 72: Spoke-SDP termination



All the routing protocols, including multicast, that are supported by VPRN are supported for spoke-sdp termination.

7.2.7.1 T-LDP status signaling for spoke SDPs terminating on IES/VPRN

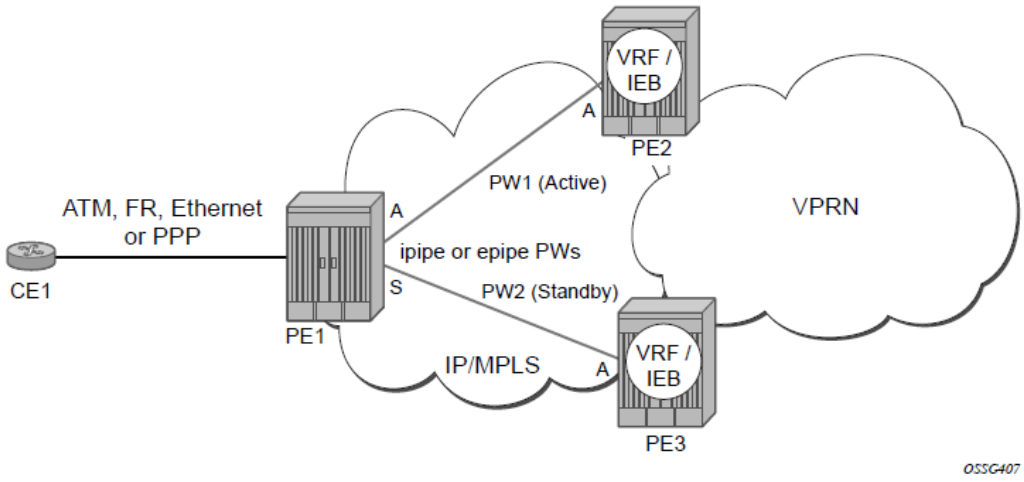
T-LDP status signaling and PW active/standby signaling capabilities are supported on Epipe spoke SDPs.

Spoke-SDP termination on an IES or VPRN provides the ability to cross-connect traffic entering on a spoke-SDP, used for Layer 2 services (VLLs or VPLS), on to an IES or VPRN service. From a logical point of view the spoke-SDP entering on a network port is cross-connected to the Layer 3 service as if it had entered using a service SAP. The main exception to this is traffic entering the Layer 3 service using a spoke-SDP is handled with network QoS policies instead of access QoS policies.

When a SAP Down or SDP binding down status message is received by the PE in which the Ethernet spoke-SDP is terminated on an IES or VPRN interface, the interface is brought down and all associated routes are withdrawn in a similar way when the spoke-SDP goes down locally. The same actions are taken when the standby T-LDP status message is received by the IES/VPRN PE.

This feature can be used to provide redundant connectivity to a VPRN or IES from a PE providing a VLL service, as shown in the following figure.

Figure 73: Active/standby VRF using resilient L2 circuits



7.2.7.2 GR Helper for CE-PE Routing Protocols

The GR helper function for BGP and OSPF between CE and PE is supported for routing protocols that are running in the default routing context.

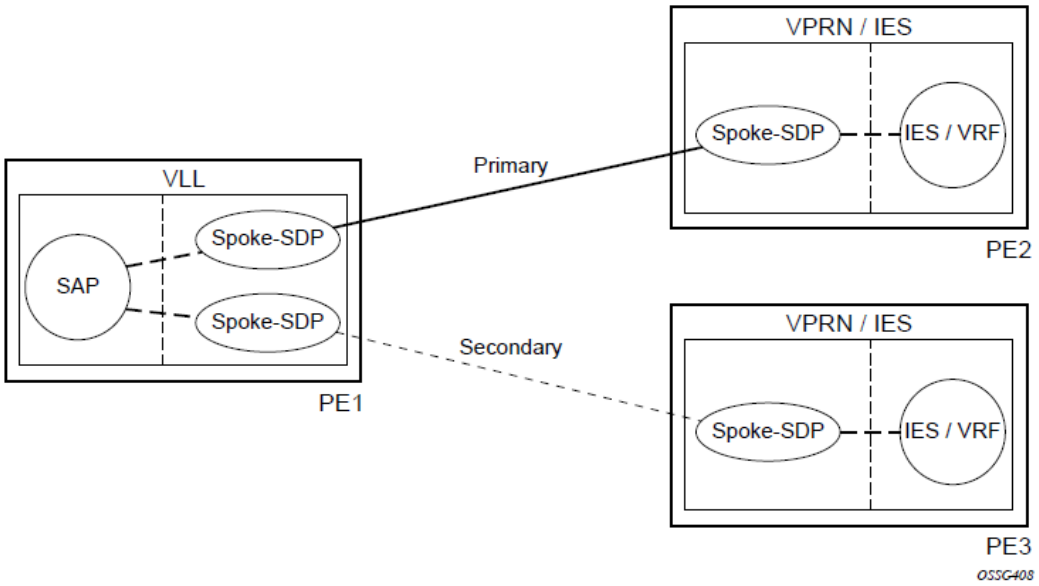
7.2.7.3 Spoke-SDP Redundancy into IES/VPRN

This feature can be used to provide redundant connectivity to a VPRN or IES from a PE providing a VLL service, as shown in Figure 73: Active/standby VRF using resilient L2 circuits, using Epipe spoke-SDPs.

In Figure 73: Active/standby VRF using resilient L2 circuits, PE1 terminates two spoke-SDPs that are bound to one SAP connected to CE1. PE1 chooses to forward traffic on one of the spoke SDPs (the active spoke-SDP), while blocking traffic on the other spoke-SDP (the standby spoke-SDP) in the transmit direction. PE2 and PE3 take any spoke-SDPs for which PW forwarding standby has been signaled by PE1 to an operationally down state.

7210 routers are expected to fulfill both functions (VLL and VPRN/IES PE). The following figure shows the model for spoke-SDP redundancy into a VPRN or IES.

Figure 74: Spoke-SDP redundancy model



7.2.8 Using OSPF in IP-VPNs

Note: OSPF as a PE-CE routing protocol is only supported for IPv4 VPNs.

Using OSPF as a CE to PE routing protocol allows OSPF that is currently running as the IGP routing protocol to migrate to an IP-VPN backbone without changing the IGP routing protocol, introducing BGP as the CE-PE or relying on static routes for the distribution of routes into the service providers IP-VPN. The following features are supported:

- Advertisement/redistribution of BGP-VPN routes as summary (type 3) LSAs flooded to CE neighbors of the VPRN OSPF instance. This occurs if the OSPF route type (in the OSPF route type BGP extended community attribute carried with the VPN route) is not external (or NSSA) and the locally configured domain-id matches the domain-id carried in the OSPF domain ID BGP extended community attribute carried with the VPN route.
- OSPF sham links. A sham link is a logical PE-to-PE unnumbered point-to-point interface that essentially rides over the PE-to-PE transport tunnel. A sham link can be associated with any area and can therefore appear as an intra-area link to CE routers attached to different PEs in the VPN.

7.2.9 Service label mode of a VPRN

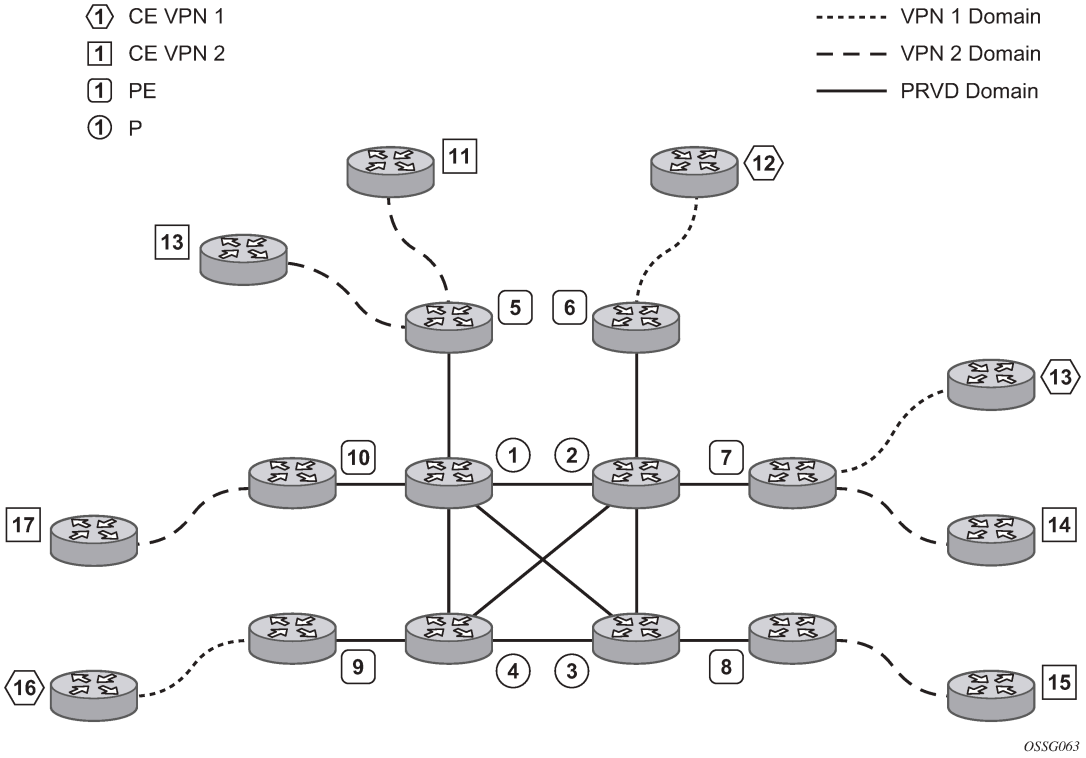
The 7210 SAS allocates one unique (platform-wide) service label per VRF. All VPN-IP routes exported by the PE from a particular VPRN service with that configuration have the same service label. When the PE receives a terminating MPLS packet, the service label value determines the VRF to which the packet belongs. A lookup of the IP packet DA in the forwarding table of the selected VRF determines the next-hop interface.

7.2.10 Multicast in IP-VPN applications

Applications for this feature include enterprise customer implementing a VPRN solution for their WAN networking needs, customer applications including stock-ticker information, financial institutions for stock and other types of trading data and video delivery systems.

The following figure depicts an example of multicast in an IP-VPN application. The provider domain encompasses the core routers (1 through 4) and the edge routers (5 through 10). The various IP-VPN customers each have their own multicast domain, VPN-1 (CE routers 12, 13 and 16) and VPN-2 (CE Routers 11, 14, 15, 17 and 18). In this VPRN example, the VPN-1 data generated by the customer behind router 16 is multicast only by PE router 9 to PE routers 6 and 7 for delivery to CE routers 12 and 13 respectively. Data for VPN-2 generated by the customer behind router 15 is forwarded by PE router 8 to PE routers 5, 7 and 10 for delivery to CE routers 18, 11, 14 and 17 respectively.

Figure 75: Multicast in IP-VPN applications



The demarcation of these domains is in the PE router (routers 5 through 10). The PE router participates in both the customer multicast domain and the provider multicast domain. The customer CE routers are limited to a multicast adjacency with the multicast instance on the PE created to support that specific customer IP-VPN. This way, customers are isolated from the provider core multicast domain and other customer multicast domains while the provider core routers only participate in the provider multicast domain and are isolated from all customer multicast domains.

The PE for a specific customer multicast domain becomes adjacent to the CE routers attached to that PE and to all other PE that participate in the IP-VPN (or customer) multicast domain. This is achieved by the PE, which encapsulates the customer multicast control data and multicast streams inside the provider multicast packets. These encapsulated packets are forwarded only to the PE nodes that are participating

in the same MVPN domain and are part of the same customer VPRN. This prunes the distribution of the multicast control and data traffic to the PEs that do not participate in the customer multicast domain.

Note: To enable ingress FC classification for packets received on a P2MP LSP on a network port IP interface and that needs to be replicated to IP receivers, use the **loopback-no-svc-port>p2mpbud>p2mpbud-port-id>p2mp-bud-classification** command. This command is required only on the 7210 SAS-R6 and 7210 SAS-R12 for ingress FC classification; for other platforms, this is not required.This command allows users to prioritize multicast traffic to IP receivers in the service. In addition, this command marks the packet with IP DSCP values while sending the multicast stream out of the IP interface. Before using the command, users must ensure that sufficient resources are available in the network ingress CAM resource pool and MPLS EXP ingress profile map resource pool. Use the **tools>dump>system-resources** command to check resource availability.

7.2.10.1 Multicast protocols supported in the provider network

An MVPN is defined by two sets of sites: the sender sites set and receiver sites set, with the following properties:

- Hosts within the sender sites set could originate multicast traffic for receivers in the receiver sites set.
- Receivers not in the receiver sites set should not be able to receive this traffic.
- Hosts within the receiver sites set could receive multicast traffic originated by any host in the sender sites set.
- Hosts within the receiver sites set should not be able to receive multicast traffic originated by any host that is not in the sender sites set.

A site could be both in the sender sites set and receiver sites set, which implies that hosts within such a site could both originate and receive multicast traffic. An extreme case is when the sender sites set is the same as the receiver sites set, in which case all sites could originate and receive multicast traffic from each other.

Sites within a specific MVPN can only be within the same organizations, which implies that an MVPN can be an intranet. A site may be in more than one MVPN, which implies that MVPNs may overlap. Not all sites of a specific MVPN have to be connected to the same service provider, which implies that an MVPN can span multiple service providers.

Another way to look at MVPN is to say that an MVPN is defined by a set of administrative policies. These policies determine the sender sites set and receiver site set. These policies are established by MVPN customers, but implemented by MVPN service providers using the existing BGP/MPLS VPN mechanisms, such as route targets, with extensions, as necessary.

7.2.10.1.1 MVPN using BGP control plane

The 7210 SAS supports next generation MVPN with MLDP and RSVP P2MP provider tunnels.

The Nokia implementation supports the following features:

- MVPN is supported all 7210 SAS platforms as described in this document.
- MVPN membership auto-discovery using BGP is supported.
- PE-PE transmission of C-multicast routing using BGP is supported.
- IPv4 is supported.

- Inter-AS MVPN with option A is supported. This does not require any additional control or data plane implementations.

7.2.10.1.2 MVPN membership auto-discovery using BGP

BGP-based auto-discovery (AD) is performed by using a multicast VPN address family. Any PE router that attaches to an MVPN must issue a BGP update message containing an NLRI in this address family, along with a specific set of attributes.

The PE router uses route targets to specify MVPN route import and export. The route target may be the same as the one used for the corresponding unicast VPN, or it may be different. The PE router can specify separate import route targets for sender sites and receiver sites for a specific MVPN.

The route distinguisher (RD) that is used for the corresponding unicast VPN can also be used for the MVPN.

When BGP AD is enabled, PIM peering on the I-PMSI is disabled, so no PIM hellos are sent on the I-PMSI. C-tree to P-tunnel bindings are also discovered using BGP S-PMSI AD routes, instead of PIM join TLVs.

For example, if AD is disabled, the **c-mcast-signaling bgp** command fails and the following error message displays:

```
C-multicast signaling in BGP requires auto-discovery to be enabled
```

AD is enabled by default on the 7210 SAS-R6 and 7210 SAS-R12.

If **c-mcast-signaling** is set to **bgp**, the **no auto-discovery** command fails and the following error message displays:

```
C-multicast signaling in BGP requires auto-discovery to be enabled
```

When **c-mcast-signaling** is set to **bgp**, S-PMSI AD is always enabled (configuration is ignored).

7.2.10.2 Provider tunnel support

The following provider tunnels are supported:

- mLDP inclusive provider tunnel
- mLDP selective provider tunnel
- RSVP P2MP LSPs inclusive provider tunnel
- RSVP P2MP LSPs selective provider tunnel

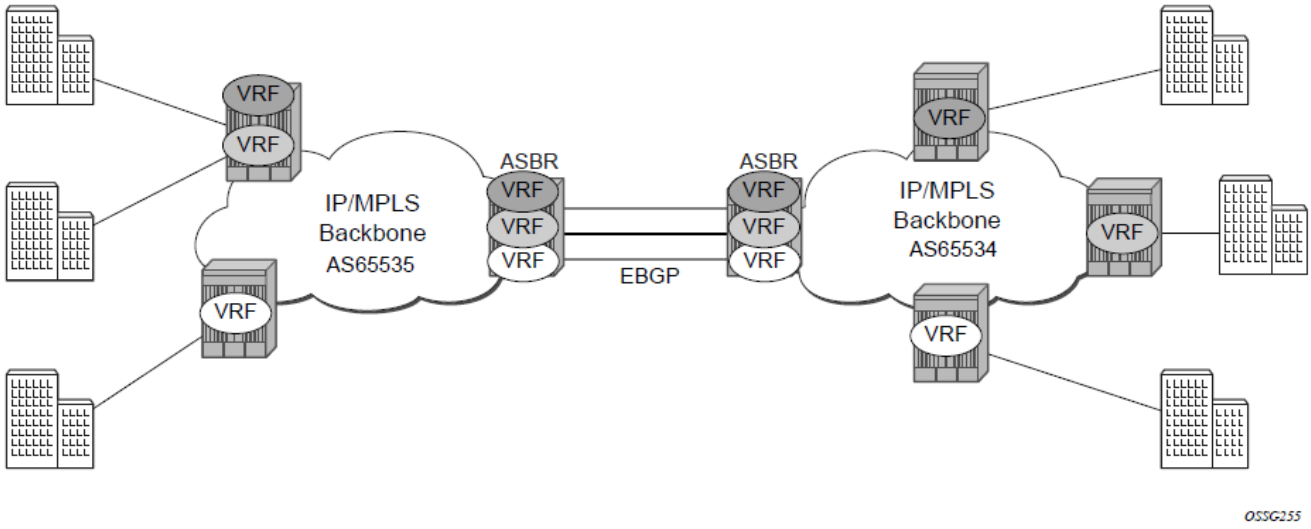
7.2.11 Inter-AS VPRNs

Inter-AS IP-VPN services have been driven by the popularity of IP services and service provider expansion beyond the borders of a single Autonomous System (AS) or the requirement for IP VPN services to cross the AS boundaries of multiple providers. Three options for supporting inter-AS IP-VPNs are described in RFC 4364, *BGP/MPLS IP Virtual Private Networks (VPNs)*.

Note: 7210 SAS platforms support only option-A and option-C. It does not support option-B. It described as follows only for the sake of completeness.

The first option, referred to as Option-A (shown in the following figure), is considered inherent in any implementation. This method uses a back-to-back connection between separate VPRN instances in each AS. As a result, each VPRN instance views the inter-AS connection as an external interface to a remote VPRN customer site. The back-to-back VRF connections between the ASBR nodes require individual sub-interfaces, one per VRF.

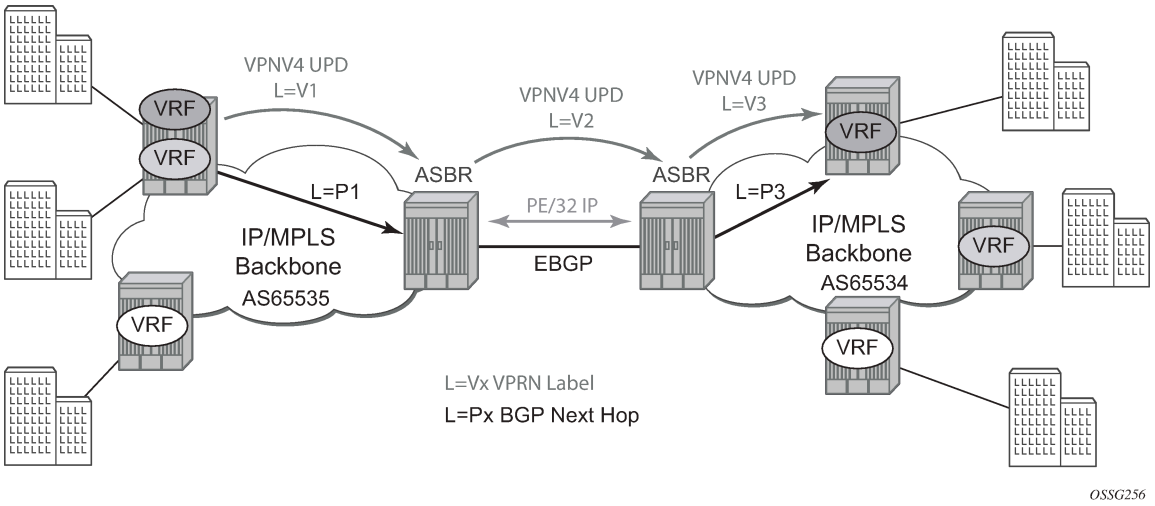
Figure 76: Inter-AS Option-A: VRF-to-VRF model



The second option, referred to as Option-B (Figure 77: Inter-AS Option-B), relies heavily on the AS Boundary Routers (ASBRs) as the interface between the autonomous systems. This approach enhances the scalability of the eBGP VRF-to-VRF solution by eliminating the need for per-VPRN configuration on the ASBRs. However it requires that the ASBRs provide a control plan and forwarding plane connection between the autonomous systems. The ASBRs are connected to the PE nodes in its local autonomous system using iBGP either directly or through route reflectors.

This means the ASBRs receive all the VPRN information and forwards these VPRN updates, VPN-IPV4, to all its EBGP peers, ASBRs, using itself as the next-hop. It also changes the label associated with the route. This means the ASBRs must maintain an associate mapping of labels received and labels issued for those routes. The peer ASBRs, in turn, forward those updates to all local IBGP peers.

Figure 77: Inter-AS Option-B

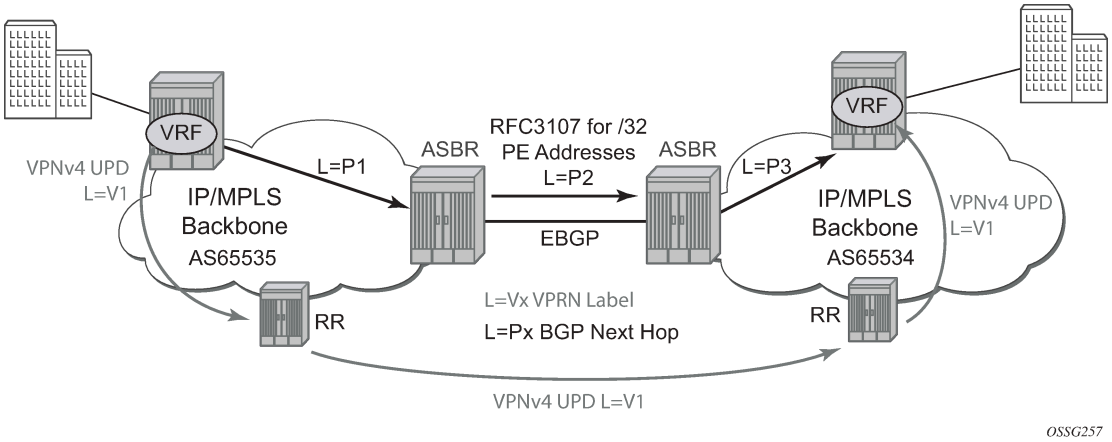


This form of inter-AS VPRNs does not require instances of the VPRN to be created on the ASBR, as in option-A, as a result there is less management overhead. This is also the most common form of Inter-AS VPRNs used between different service providers as all routes advertised between autonomous systems can be controlled by route policies on the ASBRs.

The third option, referred to as Option-C (shown in the following figure), allows for a higher scale of VPRNs across AS boundaries but also expands the trust model between ASNs. As a result this model is typically used within a single company that may have multiple ASNs for various reasons.

This model differs from Option-B, in that in Option-B all direct knowledge of the remote AS is contained and limited to the ASBR. As a result, in option-B the ASBR performs all necessary mapping functions and the PE routers do not need perform any additional functions then in a non-Inter-AS VPRN.

Figure 78: Option-C example



With Option-C, knowledge from the remote AS is distributed throughout the local AS. This distribution allows for higher scalability but also requires all PEs and ASBRs involved in the Inter-AS VPRNs to participate in the exchange of inter-AS routing information.

In Option-C, the ASBRs distribute reachability information for remote PE system IP addresses only. This is done between the ASBRs by exchanging MP-eBGP labeled routes, using RFC 3107, *Carrying Label Information in BGP-4*.

Distribution of VPRN routing information is handled by either direct MP-BGP peering between PEs in the different ASNs or more likely by one or more route reflectors in ASN.

7.3 Configuring a VPRN service with CLI

This section provides information to configure Virtual Private Routed Network (VPRN) services using the command line interface.

7.3.1 Basic configuration

The following fields require specific input (there are no defaults) to configure a basic VPRN service:

- customer ID (see Configuring customer accounts)
- specify interface parameters

Example: VPRN service configuration

```
*A:ALA-1>config>service>vprn# info
----------------------------------------------
            vrf-import "vrfImpPolCust1"
            vrf-export "vrfExpPolCust1"
            autonomous-system 10000
            route-distinguisher 10001:1
            auto-bind ldp
            vrf-target target:10001:1
            interface "to-ce1" create
                address 10.1.0.1/24
                exit
                sap 1/1/10:1 create
                    ingress
                        qos 100
                    exit
                        filter ip 10
                    exit
                exit
                exit
            exit
            static-route 10.5.0.0/24 next-hop 10.1.1.2
            bgp
                router-id 10.0.0.1
                group "to-cel"
                    export "vprnBgpExpPolCust1"
                    peer-as 65101
                    neighbor 10.1.1.2
                    exit
                exit
            exit
            no shutdown
----------------------------------------------
*A:ALA-1>config>service>vprn#
```

7.3.2 Common configuration tasks

About this task

This section provides a brief overview of the tasks that must be performed to configure a VPRN service and provides the syntax commands.

Procedure

Step 1. Associate a VPRN service with a customer ID.

Step 2. Define an autonomous system (optional).

Step 3. Define a route distinguisher (mandatory).

Step 4. Define VRF route-target associations or VRF import/export policies.

Step 5. Create an interface.

Step 6. Define SAP parameters on the interface:

- Select nodes and ports.
- Optional - select QoS policies other than the default (configured in **config>qos** context).
- Optional - select filter policies (configured in **config>filter** context).
- Optional - select accounting policy (configured in **config>log** context).

Step 7. Define BGP parameters (optional).

BGP must be enabled in the **config>router>bgp** context.

Step 8. Enable the service.

7.3.3 Configuring VPRN components

7.3.3.1 Creating a VPRN service

Use the following syntax to create a VRPN service. A route distinguisher must be defined in order for VPRN to be operationally active.

```
config>service# vprn service-id [customer customer-id]
    route-distinguisher [ip-address:number1 | asn:number2]
    description description-string
    no shutdown
```

Example: VPRN service configuration

```
*A:ALA-1>config>service# info
----------------------------------------------
...
        vprn 1 customer 1 create
            route-distinguisher 10001:0
            no shutdown
        exit
```

```
...
-----------------------------------------------
*A:ALA-1>config>service>vprn#
```

7.3.3.2 Configuring global VPRN parameters

See VPRN services command reference for CLI syntax to configure VPRN parameters.

Example: VPRN service with configured parameters

```
*A:ALA-1>config>service# info
-----------------------------------------------
...
        vprn 1 customer 1 create
            vrf-import "vrfImpPolCust1"
            vrf-export "vrfExpPolCust1"
            autonomous-system 10000
            route-distinguisher 10001:1
            exit
            no shutdown
        exit
...
-----------------------------------------------
*A:ALA-1>config>service#
```

7.3.3.2.1 Configuring router interfaces

See the *7210 SAS-Mxp, R6, R12, S, Sx, T Router Configuration Guide* for command descriptions and syntax information to configure router interfaces.

Example: Router interface configuration

```
ALA48>config>router# info
#------------------------------------------
echo "IP Configuration"
#------------------------------------------
...
        interface "if1"
            address 10.2.2.1/24
        exit
        interface "if2"
            address 10.49.1.46/24
            port 1/1/34
        exit
        interface "if3"
            address 10.11.11.1/24
        exit
...
#------------------------------------------
ALA48>config>router#
```

7.3.3.2.2 Configuring VPRN protocols - BGP

The autonomous system number and router ID configured in the VPRN context only applies to that particular service.

The minimal parameters that should be configured for a VPRN BGP instance are:

- Specify an autonomous system number for the router. See Configuring global VPRN parameters.
- Specify a router ID - Note that if a new or different router ID value is entered in the BGP context, then the new values takes precedence and overwrites the VPRN-level router ID. See Configuring global VPRN parameters.
- Specify a VPRN BGP peer group.
- Specify a VPRN BGP neighbor with which to peer.
- Specify a VPRN BGP peer-AS that is associated with the above peer.

VPRN BGP is administratively enabled upon creation. Minimally, to enable VPRN BGP in a VPRN instance, you must associate an autonomous system number and router ID for the VPRN service, create a peer group, neighbor, and associate a peer ASN. There are no default VPRN BGP groups or neighbors. Each VPRN BGP group and neighbor must be explicitly configured.

All parameters configured for VPRN BGP are applied to the group and are inherited by each peer, but a group parameter can be overridden on a specific basis. VPRN BGP command hierarchy consists of three levels:

- the global level
- the group level
- the neighbor level

Use the following commands to configure VPRN BGP groups and neighbors.

```
config>service>vprn>bgp#  (global level)
        group  (group level)
            neighbor      (neighbor level)
```

Note: The local-address must be explicitly configured if two systems have multiple BGP peer sessions between them for the session to be established.

For more information about the BGP protocol, see the *7210 SAS-Mxp, R6, R12, S, Sx, T Router Configuration Guide*.

7.3.3.2.2.1 Configuring VPRN BGP group and neighbor parameters

A group is a collection of related VPRN BGP peers. The group name should be a descriptive name for the group. Follow your group, name, and ID naming conventions for consistency and to help when troubleshooting faults.

All parameters configured for a peer group are applied to the group and are inherited by each peer (neighbor), but a group parameter can be overridden on a specific neighbor-level basis.

After a group name is created and options are configured, neighbors can be added within the same autonomous system to create IBGP connections or neighbors in different autonomous systems to create EBGP peers. All parameters configured for the peer group level are applied to each neighbor, but a group parameter can be overridden on a specific neighbor basis.

7.3.3.2.2.2 VPRN BGP CLI syntax

Use the syntax to configure VPRN BGP parameters (BGP configuration commands).

Example: VPRN BGP configuration

```
*A:ALA-1>config>service# info
----------------------------------------------
...
        vprn 1 customer 1 create
            vrf-import "vrfImpPolCust1"
            vrf-export "vrfExpPolCust1"
            autonomous-system 10000
            route-distinguisher 10001:1
            auto-bind ldp
            vrf-target target:10001:1
            interface "to-ce1" create
                address 10.1.0.1/24
                sap 1/1/10:1 create
                    ingress

                        qos 100
                    exit

                        filter ip 6
                    exit
                exit
            exit
            static-route 10.5.0.0/24 next-hop 10.1.1.2
            bgp
                router-id 10.0.0.1
                group "to-ce1"
                    export "vprnBgpExpPolCust1"
                    peer-as 65101
                    neighbor 10.1.1.2
                    exit
                exit
            exit
            spoke-sdp 2 create
            exit
            no shutdown
        exit
...
----------------------------------------------
*A:ALA-1>config>service#
```

7.3.3.2.3 Configuring a VPRN interface

Interface names associate an IP address to the interface, and then associate the IP interface with a physical port. The logical interface can associate attributes like an IP address, port, Link Aggregation Group (LAG) or the system.

There are no default interfaces.

Note that you can configure a VPRN interface as a loopback interface by issuing the loopback command instead of the **sap** *sap-id* command. The loopback flag cannot be set on an interface where a SAP is already defined and a SAP cannot be defined on a loopback interface.

When using mtrace/mstat in a Layer 3 VPN context then the configuration for the VPRN should have a loopback address configured which has the same address as the core instance's system address (BGP next-hop).

See OSPF configuration commands (IPv4 only) for CLI commands and syntax.

Example: VPRN interface configuration output

```
*A:7210 SAS>config>service>vprn>if# info detail
----------------------------------------------
                no description
                no address
                no mac
                arp-timeout 14400
                no allow-directed-broadcasts
                icmp
                    mask-reply
                    redirects 100 10
                    unreachables 100 10
                    ttl-expired 100 10
                exit
                no arp-populate
                dhcp
                    shutdown
                    no description
                    proxy-server
                        shutdown
                        no emulated-server
                        no lease-time
                    exit
                    no option
                    no server
                    no trusted
                    no lease-populate
                    no gi-address
                    no relay-plain-bootp
                    no use-arp
                exit
                no authentication-policy
                no ip-mtu
                no host-connectivity-verify
                no delayed-enable
                no bfd
                ipcp
                    no peer-ip-address
                    no dns
                exit
                no proxy-arp-policy
                no local-proxy-arp
                no remote-proxy-arp
                no shutdown
----------------------------------------------
*A:7210 SAS>config>service>vprn>if#
```

7.3.3.2.4 Configuring a VPRN interface SAP

A SAP is a combination of a port and encapsulation parameters which identifies the service access point on the interface and within the 7210 SAS. Each SAP must be unique within a router. A SAP cannot be defined if the interface **loopback** command is enabled.

When configuring VPRN interface SAP parameters, a default QoS policy is applied to each ingress and egress SAP. Additional QoS policies and scheduler policies must be configured in the **config>qos** context. Filter policies are configured in the **config>filter** context and must be explicitly applied to a SAP. There are no default filter policies.

Example: VPRN interface SAP configuration

```
*A:ALA-1>config>service# info
----------------------------------------------
...
        vprn 1 customer 1 create
            vrf-import "vrfImpPolCust1"
            vrf-export "vrfExpPolCust1"
            autonomous-system 10000
            route-distinguisher 10001:1
            auto-bind ldp
            vrf-target target:10001:1
            interface "to-ce1" create
                address 10.1.0.1/24
                sap 1/1/10:1 create
                    ingress

                        qos 100
                    exit

                        filter ip 6
                    exit
                exit
            exit
            static-route 6.5.0.0/24 next-hop 10.1.1.2
            spoke-sdp 2 create
            exit
            no shutdown
        exit
...
----------------------------------------------
*A:ALA-1>config>service#
```

7.3.4 Configuring VPRN protocols - OSPF

In a VPRN interface, each VPN routing instance is isolated from any other VPN routing instance, and from the routing used across the backbone. OSPF can be run with any VPRN, independently of the routing protocols used in other VPRNs, or in the backbone itself. For more information about the OSPF protocol, see the *7210 SAS-Mxp, R6, R12, S, Sx, T Routing Protocols Guide*.

Use the **configure>service>vprn>ospf** context to configure the OSPF protocol within VPRN.

7.3.4.1 VPRN OSPF CLI syntax

See Configuring VPRN protocols - OSPF for CLI syntax to configure VPRN parameters.

For more information about the OSPF protocol, see the *7210 SAS-Mxp, R6, R12, S, Sx, T Routing Protocols Guide*.

Example: VPRN OSPF configuration

```
A:duta>config>service>vprn# info
----------------------------------------------
            router-id 10.10.10.1
            autonomous-system 100
            route-distinguisher 65510:1
            auto-bind ldp
            vrf-target target:65520:1
```

```
            interface "to-ixia-1" create
                address 10.1.1.1/24
                sap 1/1/9:1 create
                exit
            exit
            interface "to-ixia-2" create
                address 10.1.2.1/24
                sap 1/1/9:12 create
                exit
            exit
            ospf
                super-backbone
                vpn-domain 0005 0000.0000.0001
                export "from_mbgp_to_ospf"
                area 0.0.0.0
                    interface "to-ixia-2"
                        mtu 1500
                        no shutdown
                    exit
                    sham-link "to-ixia-1" 10.1.1.1
                    exit
                    sham-link "to-ixia-1" 111.11.1.1
                    exit
                exit
            exit
            no shutdown
-------------------------------------------
A:duta>config>service>vprn#
```

7.3.5 Service management tasks

This section describes the service management tasks.

7.3.5.1 Modifying VPRN service parameters

Use the syntax to modify VPRN parameters (VPRN services command reference).

Example: VPRN service creation and modification

```
*A:ALA-1>config>service# info
-------------------------------------------
...
vprn 1 customer 1 create
            shutdown
            vrf-import "vrfImpPolCust1"
            vrf-export "vrfExpPolCust1"
            maximum-routes 2000
            autonomous-system 10000
            route-distinguisher 10001:1
            interface "to-ce1" create
                address 10.1.1.1/24
                sap 1/1/10:1 create
                exit
            exit
            static-route 10.5.0.0/24 next-hop 10.1.1.2
            bgp
                router-id 10.0.0.1
                group "to-ce1"
                    export "vprnBgpExpPolCust1"
```

```
                    peer-as 65101
                    neighbor 10.1.1.2
                    exit
                exit
            exit
            spoke-sdp 2 create
            exit
        exit
...
-------------------------------------------
*A:ALA-1>config>service>vprn#
```

7.3.5.2 Deleting a VPRN service

An VPRN service cannot be deleted until SAPs and interfaces are shut down and deleted. If protocols or a spoke-SDP are defined, they must be shut down and removed from the configuration as well.

Use the following syntax to delete a VPRN service.

```
config>service#
    [no] vprn service-id [customer customer-id]
        shutdown
        [no] interface ip-int-name
            shutdown
        [no] sap sap-id]
            [no] bgp
            shutdown
        [no] spoke-sdp sdp-id
            [no] shutdown
```

7.3.5.3 Disabling a VPRN service

Use the following syntax to shutdown a VPN service without deleting any service parameters.

```
config>service#
        vprn service-id [customer customer-id]
            shutdown
```

Example: Disabling a VPRN service

```
config>service# vprn 1
config>service>vprn# shutdown
config>service>vprn# exit
```

```
*A:ALA-1>config>service# info
-------------------------------------------
...
        vprn 1 customer 1 create
            shutdown
            vrf-import "vrfImpPolCust1"
            vrf-export "vrfExpPolCust1"
            autonomous-system 10000
            route-distinguisher 10001:1
            auto-bind ldp
            vrf-target target:10001:1
            interface "to-ce1" create
```

```
                address 11.1.0.1/24
                sap 1/1/10:1 create
                    ingress

                        qos 100
                    exit
filter ip 6
                    exit
                exit
            exit
            static-route 10.5.0.0/24 next-hop 10.1.1.2
            bgp
                router-id 10.0.0.1
                group "to-cel"
                    export "vprnBgpExpPolCust1"
                    peer-as 65101
                    neighbor 10.1.1.2
                    exit
                exit
            exit
            spoke-sdp 2 create
            exit
        exit
...
-------------------------------------------
*A:ALA-1>config>service#
```

7.3.5.4 Re-enabling a VPRN service

Use the following syntax to re-enable a VPRN service that was shut down.

```
config>service#
        vprn service-id [customer customer-id]
            no shutdown
```

7.4 VPRN services command reference

7.4.1 Command hierarchies

- VPRN service configuration commands
- Multicast VPN commands
- Interface commands
- Interface VRRP commands (IPv4 only - applicable for network mode only)
- Interface SAP commands
- Interface SAP filter and QoS commands
- Routed VPLS commands
- BGP configuration commands
- Router advertisement commands

- OSPF configuration commands (IPv4 only)
- Show commands
- Clear commands
- Debug commands

7.4.1.1 VPRN service configuration commands

```
config
    - service
        - vprn service-id [customer customer-id]
        - no vprn service-id
            - [no] allow-export-bgp-vpn
            - auto-bind-tunnel
                - resolution {any | filter | disabled}
                - resolution-filter
                    - [no] ldp
                    - [no] rsvp
            - autonomous-system as-number
            - no autonomous-system
            - description description-string
            - no description
            - enable-bgp-vpn-backup [ipv4] [ipv6]
            - no enable-bgp-vpn-backup
            - maximum-ipv6-routes number [log-only] [threshold percent]
            - no maximum-ipv6-routes
            - maximum-routes number [log-only] [threshold percent]
            - no maximum-routes
            - route-distinguisher [ip-address:number1 | asn:number2]
            - no route-distinguisher
            - router-id ip-address
            - no router-id
            - [no] shutdown
            - sgt-qos
                - application dscp-app-name dscp {dscp-value | dscp-name}
                - application dot1p-app-name dot1p dot1p-priority
                - no application {dscp-app-name | dot1p-app-name}
                - dscp dscp-name fc fc-name
                - no dscp dscp-name fc fc-name
            - snmp-community community-name [version SNMP-version]
            - no snmp-community community-name
            - source-address
                - application app [ip-int-name | ip-address]
                - no application app
            - [no] spoke-sdp sdp-id
                - description description-string
                - no description
                - [no] shutdown
            - [no] static-route {ip-prefix/prefix-length | ip-prefix netmask}
 [preference preference] [metric metric] [tag tag] [enable | disable] {next-hop ip-int-
name | ip-address | ipsec-tunnel ipsec-tunnel-name} [bfd-enable | {cpe-check cpe-ip-address
 [interval seconds] [drop-count count] [log]}] {prefix-list prefix-list-name [all|none]}]
            - [no] static-route {ip-prefix/prefix-length | ip-prefix netmask}
 [preference preference] [metric metric] [tag tag] [enable | disable] indirect ip-address [cpe-
check cpe-ip-address [interval seconds][drop-count count] [log]] {prefix-list prefix-list-name
 [all|none]}]
            - [no] static-route {ip-prefix/prefix-length | ip-prefix netmask}
 [preference preference] [metric metric] [tag tag] [enable | disable] black-hole {prefix-
list prefix-list-name [all | none]}]
            - vrf-export  policy-name [policy-name...(upto 5 max)]
```

```
            - no vrf-export
            - vrf-import policy-name [policy-name...(upto 5 max)]
            - no vrf-import
            - vrf-target {ext-comm|{[export ext-comm] [import ext-comm]}}
            - no vrf-target
            - [no] shutdown
```

7.4.1.2 Multicast VPN commands

```
config
    - service
        - vprn service-id [customer customer-id]
        - no vprn service-id
            - mvpn
                - [no] auto-discovery [default]
                - c-mcast-signaling {bgp}
                - no c-mcast-signaling
                - [no] intersite-shared
                - mdt-type {sender-receiver | sender-only | receiver-only}
                - no mdt-type
                - provider-tunnel
                    - inclusive
                        - bsr {unicast | spmsi}
                        - no bsr
                        - [no] mldp
                            - [no] shutdown
                        - [no] rsvp
                            - lsp-template lsp-template
                            -  no lsp-template
                            - [no] shutdown
                        - [no] wildcard-spmsi
                    - selective
                        - data-delay-interval value
                        - no data-delay-interval
                        - data-threshold {c-grp-ip-addr/mask | c-grp-ip-addr netmask}
                        - no data-threshold {c-grp-ip-addr/mask | c-grp-ip-addr netmask}
                        - maximum-p2mp-spmsi range
                        - no maximum-p2mp-spmsi
                        - [no] mldp
                            - [no] shutdown
                        - [no] rsvp
                            - lsp-template lsp-template
                            - no lsp-template
                            - [no] shutdown
                - umh-selection {highest-ip}
                - no umh-selection
                - vrf-export {unicast | policy-name [policy-name...(up to 15 max)]}
                - no vrf-export
                - vrf-import {unicast | policy-name [policy-name...(up to 15 max)]}
                - no vrf-import
                - vrf-target {unicast | ext-community | export unicast | ext-community | import
 unicast | ext-community}
                - no vrf-target
                    - export {unicast | ext-community}
                    - import {unicast | ext-community}
```

7.4.1.3 Interface commands

```
config
    - service
        - vprn service-id [customer customer-id]
        - no vprn service-id
            - [no] interface ip-int-name
                - address ip-address[/mask] [netmask] [broadcast {all-ones | host-ones}]
                - no address
                - [no] allow-directed-broadcasts
                - arp-timeout [seconds]
                - no arp-timeout
                - bfd transmit-interval [receive receive-interval] [multiplier multiplier]
[echo-receive echo-interval] [type iom-hw]
                - no bfd
                - delayed-enable seconds [init-only]
                - no delayed-enable
                - description description-string
                - no description [description-string]
                - no description [description-string]
                - dhcp
                    - description description-string
                    - no description
                    - gi-address ip-address [src-ip-addr]
                    - no gi-address
                    - [no] option
                        - action {replace | drop | keep}
                        - no action
                        - [no] circuit-id [ascii-tuple | ifindex | sap-id | vlan-ascii-tuple]
                        - [no] remote-id  [mac | string string]
                        - [no] vendor-specific-option
                            - [no] client-mac-address
                            - [no] sap-id
                            - [no] service-id
                            - string text
                            - no string
                            - [no] system-id
                        - no relay-plain-bootp
                        - relay-plain-bootp
                    - no server
                    - server server1 [server2...(up to 8 max)]
                    - [no] shutdown
                    - [no] trusted
                - icmp
                - [no] 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
                - ipv6
                - no ipv6
                    - [no] address ipv6-address/prefix-length [eui-64] [preferred]
                    - icmp6
                        - [no] packet-too-big number seconds
                        - [no] param-problem number seconds
                        - [no] redirects number seconds
                        - [no] time-exceeded number seconds
```

```
                        - [no] unreachables number seconds
                    - [no] link-local-address ipv6-address [preferred]
                    - [no] local-proxy-nd
                    - [no] neighbor ipv6-address mac-address
                    - [no] proxy-nd-policy policy-name [policy-name...(up to 5 max)]
                - [no] local-proxy-arp
                - [no] loopback
                - [no] proxy-arp-policy policy-name [policy-name...(up to 5 max)]
                - proxy-arp-policy 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}
                - static-arp ieee-address
                - [no] static-arp [ieee-address]
                - [no] shutdown
                - static-arp ip-address ieee-address
                - [no] static-arp ip-address [ieee-address]
                - [no] vrrp virtual-router-id
```

7.4.1.4 Interface VRRP commands (IPv4 only - applicable for network mode only)

```
config
    - service
        - vprn service-id [customer customer-id]
        - no vprn service-id
            - interface ip-int-name
                - vrrp virtual-router-id [owner]
                - no vrrp virtual-router-id
                    - authentication-key {authentication-key | hash-key} [hash | hash2]
                    - no authentication-key
                    - [no] backup ip-address
                    - [no] init-delay [service-id] interface interface-name dst-ip ip-address
                    - init-delay seconds
                    - no init-delay
                    - [no] master-int-inherit
                    - message-interval {[seconds] [milliseconds milliseconds]}
                    - no message-interval
                    - [no] ping-reply
                    - policy vrrp-policy-id
                    - no policy
                    - [no] preempt
                    - priority priority
                    - no priority
                    - [no] shutdown
                    - [no] ssh-reply
                    - [no] standby-forwarding
                    - [no] telnet-reply
                    - [no] traceroute-reply
```

7.4.1.5 Interface SAP commands

```
config
    - service
        - vprn service-id [customer customer-id] [create]
        - no vprn service-id
            - [no] interface ip-int-name [create] [tunnel]
```

```
                - [no] sap sap-id
                    - accounting-policy acct-policy-id
                    - no accounting-policy [acct-policy-id]
                    - [no] collect-stats
                    - description description-string
                    - no description [description-string]
                    - dist-cpu-protection policy-name
                    - no dist-cpu-protection
                    - ingress
                        - meter-override
                            - meter meter-id [create]
                            - no meter meter-id
                                - adaptation-rule  [pir adaptation-rule] [cir adaptation-rule]
                                -  cbs size [kbits | bytes | kbytes]
                                - no cbs
                                - mbs size [kbits | bytes | kbytes]
                                - no mbs
                                - no mode
                                - no mode
                                - rate cir cir-rate [pir pir-rate]
                        - queue-override
                            - queue queue-id [create]
                                - adaptation-rule  [pir adaptation-rule] [cir adaptation-rule]
                                - no port-parent
                                - port-parent [cir-level cir-level] [pir-weight pir-weight]
                                - queue-mgmt name
                                - no queue-mgmt
                                - no rate
                                - rate [cir cir-rate] [pir pir-rate]
                    - [no] shutdown
                    - statistics
                        - ingress
                            - counter-mode {in-out-profile-count | forward-drop-count}
                    - tod-suite tod-suite-name
                    - no tod-suite
```

7.4.1.6 Interface SAP filter and QoS commands

```
config
    - service
        - vprn service-id [customer customer-id] [create]
        - no vprn service-id
            - [no] interface ip-int-name [create] [tunnel]
                - [no] sap sap-id
                    - egress
                        - agg-rate-limit agg-rate
                        - no agg-rate-limit
                        - aggregate-meter-rate rate-in-kbps [burst burst-in-kbits] [enable-
stats]
                        - no aggregate-meter-rate
                        - filter ip ip-filter-id
                        - filter ipv6 ipv6 -filter-id
                        - filter mac mac-filter-id
                        - no filter [ip ip-filter-id] [ ipv6 ipv6-filter-id] [mac mac-filter-
id]
                    - ingress
                        - aggregate-meter-rate rate-in-kbps [burst burst-in-kbits]
                        - no aggregate-meter-rate
                        - filter ip ip-filter-id
                        - filter [ipv6 ipv6-filter-id]
                        - filter mac mac-filter-id
```

```
                        - no filter [ip ip-filter-id] [ipv6 ipv6-filter-id] [mac mac-filter-
id]
                        - qos policy-id [enable-table-classification]
```

7.4.1.7 Routed VPLS commands

```
config
    - service
        - vprn service-id [customer customer-id]
        - no vprn service-id
            - interface ip-int-name [create]
            - no interface ip-int-name
                - vpls service-name
                - no vpls
                    - ingress
                        - [no] enable-table-classification
                        - routed-override-qos-policy policy-id
                        - no routed-override-qos-policy
                        - v4-routed-override-filter ip-filter-id
                        - no v4-routed-override-filter
```

7.4.1.8 BGP configuration commands

```
config
    - service
        - vprn service-id [customer customer-id]
        - no vprn service-id
            - [no] bgp
                - [no] advertise-inactive
                - [no] aggregator-id-zero
                - always-compare-med {zero | infinity}
                - no always-compare-med
                - [no] as-path-ignore
                - auth-keychain name
                - authentication-key [authentication-key | hash-key] [hash | hash2]
                - no authentication-key
                - [no] connect-retry seconds
                - [no] damping
                - description description-string
                - no description
                - [no] disable-4byte-asn
                - disable-capability-negotiation
                - no disable-capability-negotiation
                - disable-communities [standard] [extended]
                - no disable-communities
                - [no] disable-fast-external-failover
                - [no] enable-peer-tracking
                - export policy-name [policy-name...(up to 5 max)]
                - no export
                - family [ipv4] [ipv6]
                - no family
                - hold-time seconds [strict]
                - no hold-time
                - import policy-name [policy-name...(up to 5 max)]
                - no import
                - keepalive seconds
                - no keepalive
                - local-preference ip-address
```

```
                - no local-preference
                - local-as
                - local-as as-number [private]
                - no local-as
                - local-preference local-preference
                - no local-preference
                - loop-detect {drop-peer | discard-route | ignore-loop| off}
                - no loop-detect
                - med-out {number | igp-cost}
                - no med-out
                - min-as-origination seconds
                - no min-as-origination
                - min-route-advertisement seconds
                - no min-route-advertisement
                - multihop ttl-value
                - no multihop
                - next-hop-self
                - no next-hop-self
                - preference preference
                - no preference
                - peer-as as number
                - no peer-as
                - [no] path-mtu-discovery
                - [no] rapid-withdrawal
                - [no] remove-private
                - router-id ip-address
                - no router-id
                - [no] shutdown
                - [no] group name [dynamic-peer]
                    - [no] advertise-inactive
                    - [no] aggregator-id-zero
                    - [no] as-override
                    - auth-keychain name
                    - authentication-key [authentication-key | hash-key] [hash | hash2]
                    - no authentication-key
                    - connect-retry seconds
                    - no connect-retry
                    - [no] damping
                    - description description-string
                    - no description
                    - [no] disable-4byte-asn
                    - disable-communities [standard] [extended]
                    - no disable-communities
                    - [no] disable-fast-external-failover
                    - [no] enable-peer-tracking
                    - export policy-name [policy-name...(up to 5 max)]
                    - no export
                    - family [ipv4] [ipv6]
                    - no family
                    - hold-time seconds [strict]
                    - no hold-time
                    - import policy-name [policy-name...(up to 5 max)]
                    - no import
                    - keepalive seconds
                    - no keepalive
                    - local-address ip-address
                    - no local-address
                    - local-as as-number [private]
                    - no local-as
                    - local-preference local-preference
                    - no local-preference
                    - loop-detect {drop-peer | discard-route | ignore-loop | off}
                    - no loop-detect
                    - med-out {number | igp-cost}
```

```
                    - no med-out
                    - min-as-origination seconds
                    - no min-as-origination
                    - min-route-advertisement seconds
                    - no min-route-advertisement
                    - multihop ttl-value
                    - no multihop
                    - [no] next-hop-self
                    - peer-as as-number
                    - no peer-as
                    - preference preference
                    - no preference
                    - path-mtu-discoveryprefix-limit limit [log-only] [threshold percent]
                    - no prefix-limit
                    - [no] remove-private
                    - [no] shutdown
                    - ttl-security min-ttl-value
                    - no ttl-security
                    - type {internal | external}
                    - no type
                    - [no] neighbor ip-address
                        - [no] advertise-inactive
                        - [no] aggregator-id-zero
                        - [no] as-override
                        - auth-keychain name
                        - authentication-key [authentication-key | hash-key] [hash | hash2]
                        - no authentication-key
                        - connect-retry seconds
                        - no connect-retry
                        - [no] damping
                        - description description-string
                        - no description
                        - [no] disable-4byte-asn
                        - disable-communities [standard] [extended]
                        - no disable-communities
                        - [no] disable-fast-external-failover
                        - [no] enable-peer-tracking
                        - export policy-name [policy-name...(up to 5 max)]
                        - no export
                        - family [ipv4] [ipv6]
                        - no family
                        - hold-time seconds [strict]
                        - no hold-time
                        - import policy-name [policy-name...(up to 5 max)]
                        - no import
                        - keepalive seconds
                        - no keepalive
                        - local-address ip-address
                        - no local-address
                        - local-as as-number [private]
                        - no local-as
                        - local-preference local-preference
                        - no local-preference
                        - loop-detect {drop-peer | discard-route | ignore-loop | off}
                        - no loop-detect
                        - med-out {number | igp-cost}
                        - no med-out
                        - min-as-origination seconds
                        - no min-as-origination
                        - min-route-advertisement seconds
                        - no min-route-advertisement
                        - multihop ttl-value
                        - no multihop
                        - [no] next-hop-self
```

```
                        - peer-as as-number
                        - no peer-as
                        - preference preference
                        - no preference
                        - [no] path-mtu-discovery
                        - prefix-limit limit [log-only] [threshold percent]
                        - no prefix-limit
                        - [no] remove-private
                        - [no] shutdown
                        - ttl-security min-ttl-value
                        - no ttl-security
                        - type {internal | external}
                        - no type
```

7.4.1.9 Router advertisement commands

```
config
    - service
        - vprn service-id [customer customer-id]
        - no vprn service-id
            - [no]router-advertisement
                - [no] interface ip-int-name
                    - current-hop-limit number
                    - no current-hop-limit
                    - [no] managed-configuration
                    - max-advertisement-interval seconds
                    - no max-advertisement-interval
                    - min-advertisement-interval seconds
                    - no min-advertisement-interval
                    - mtu mtu-bytes
                    - no mtu
                    - [no] other-stateful-configuration
                    - prefix
                        - [no] autonomous
                        - [no] on-link
                        - preferred-lifetime {seconds | infinite}
                        - no preferred-lifetime
                        - valid-lifetime{seconds | infinite}
                        - no valid-lifetime
                    - reachable-time milli-seconds
                    - no reachable-time
                    - retransmit-time milli-seconds
                    - no retransmit-time
                    - router-lifetime seconds
                    - no router-lifetime
                    - [no] shutdown
```

7.4.1.10 OSPF configuration commands (IPv4 only)

```
config
    - service
        - vprn service-id [customer customer-id]
        - no vprn service-id
            - [no] ospf
                - [no] area area-id
                    - area-range  ip-prefix/mask [advertise | not-advertise]
                    - no area-range  ip-prefix/mask
                    - [no] blackhole-aggregate
```

```
                - [no] interface ip-int-name [secondary]
                    - [no] advertise-subnet
                    - authentication-key [authentication-key | hash-key] [hash | hash2]
                    - no authentication-key
                    - authentication-type {password | message-digest}
                    - no authentication-type
                    - bfd-enable [remain-down-on-failure]
                    - no bfd-enable
                    - dead-interval seconds
                    - no dead-interval
                    - hello-interval seconds
                    - no hello-interval
                    - interface-type {broadcast | point-to-point}
                    - no interface-type
                    - message-digest-key key-id md5 [key | hash-key] [hash | hash2]
                    - no message-digest-key key-id
                    - metric metric
                    - no metric
                    - mtu bytes
                    - no mtu
                    - [no] passive
                    - priority number
                    - no priority
                    - retransmit-interval seconds
                    - no retransmit-interval
                    - [no] shutdown
                    - transit-delay seconds
                    - no transit-delay
                - [no] nssa
                    - area-range  ip-prefix/mask [advertise | not-advertise]
                    - no area-range  ip-prefix/mask
                    - originate-default-route [type-7]
                    - no originate-default-route
                    - [no] redistribute-external
                    - [no] summaries
                - [no] sham-link ip-int-name ip-address
                    - authentication-key [authentication-key | hash-key] [hash | hash2]
                    - no authentication-key
                    - authentication-type {password | message-digest}
                    - no authentication-type
                    - dead-interval seconds
                    - no dead-interval
                    - hello-interval seconds
                    - no hello-interval
                    - message-digest-key key-id md5 [key | hash-key] [hash | hash2]
                    - no message-digest-key key-id
                    - metric metric
                    - no metric
                    - retransmit-interval seconds
                    - no retransmit-interval
                    - [no] shutdown
                    - transit-delay seconds
                    - no transit-delay
                - [no] stub
                    - default-metric metric
                    - no default-metric
                    - [no] summaries
                - [no] virtual-link router-id transit-area area-id
                    - authentication-key [authentication-key | hash-key] [hash | hash2]
                    - no authentication-key
                    - authentication-type {password | message-digest}
                    - no authentication-type
                    - dead-interval seconds
                    - no dead-interval
```

```
                        - hello-interval seconds
                        - no hello-interval
                        - message-digest-key key-id md5 [key | hash-key] [hash | hash2]
                        - no message-digest-key key-id
                        - retransmit-interval seconds
                        - no retransmit-interval
                        - [no] shutdown
                        - transit-delay seconds
                        - no transit-delay
                    - [no] compatible-rfc1583
                    - export policy-name [ policy-name...(up to 5 max)]
                    - no export
                    - external-db-overflow limit seconds
                    - no external-db-overflow
                    - external-preference preference
                    - no external-preference
                    - [no] ignore-dn-bit
                    - import policy-name [policy-name...(up to 5 max)]
                    - no import policy-name [policy-name...(up to 5 max)]
                    - overload [timeout seconds]
                    - no overload
                    - [no] overload-include-stub
                    - overload-on-boot [timeout seconds]
                    - no overload-on-boot
                    - preference preference
                    - no preference
                    - reference-bandwidth  bandwidth-in-kbps
                    - no reference-bandwidth
                    - router-id ip-address
                    - no router-id
                    - [no] shutdown
                    - [no] super-backbone
                    - [no] suppress-dn-bit
                    - timers
                        - [no] lsa-arrival lsa-arrival-time
                        - [no] lsa-generate max-lsa-wait [lsa-initial-wait [lsa-second-wait]]
                        - [no] spf-wait max-spf-wait [spf-initial-wait [spf-second-wait]]
                    - vpn-domain id {0005 | 0105 | 0205 | 8005}
                    - no vpn-domain
                    - vpn-tag vpn-tag
                    - no vpn-tag
```

7.4.1.11 Show commands

```
show
    - service
        - egress-label start-label [end-label]
        - ingress-label start-label [[end-label]
        - id service-id
            - all
            - base
            - dhcp
                - statistics [sap sap-id] [interface interface-name]
                - summary [interface interface-name | saps]
            - sap [sap-id [detail]]
            - sdp [sdp-id | far-end ip-address] [detail]
        - labels
        - sap-using [sap sap-id]
        - sap-using interface [ip-address | ip-int-name]
        - sap-using [ingress | egress] filter filter-id
        - sap-using [ingress| qos-policy qos-policy-id
```

```
        - sdp-using [sdp-id | far-end ip-address] [detail | keep-alive-history]
        - sdp-using [sdp-id[:vc-id]
        - service-using [vprn] [sdp sdp-id] [customer customer-id]
```

```
show
    - router [vprn-service-id]
        - aggregate [family] [active]
        - arp [ip-int-name | ip-address[/mask]|mac ieee-mac address |summary] [local | dynamic
 | static | managed]
        - bgp
            - auth-keychain [keychain]
            - damping [ip-prefix[/prefix-length]] [decayed | history | suppressed] [detail]
 [ipv4]
            - damping [ip-prefix[/prefix-length]] [decayed | history | suppressed] [detail]
 vpn-ipv4
            - group [name] [detail] inter-as-label
            - neighbor [ip-address [detail]
            - neighbor [as-number [detail]
            - neighbor [ip-address [[family family] filter1][filter3]]
            - neighbor [as-number [[family family] filter2]]
            - next-hop [family] [ip-address [detail]]
            - paths
            - routes [family family] [prefix [detail | longer]]
            - routes [family family] [prefix [hunt | brief]]
            - routes [family family] [community comm-id]
            - routes [family family] [aspath-regex reg-ex1]
            - routes [family] [ipv6-prefix[/prefix-length] [detail | longer]|[hunt [brief]]]
            - summary [all]
        - interface [{[ip-address | ip-int-name] [detail]} | summary [family family]
 [neighbor ip-address]
        - mvpn
        - mvpn-list [type type] [auto-discovery auto-discovery] [signalling signalling]
 [group group]
        - route-table [family] [ip-address[/prefix-length] [longer | exact]] | [protocol
 protocol-name] | [summary]
        - sgt-qos               (See following Note)
            - application
            - dscp-map
        - static-arp [ip-address | ip-int-name | mac ieee-mac-address]
        - static-route [ip-prefix /mask] | [preference preference] | [next-hop ip-address| tag
 tag] [detail]
        - tunnel-table [ip-address[/mask] [protocol protocol | sdp sdp-id]
        - tunnel-table [summary]
```

Note:
For descriptions of the **show>router>sgt-qos** commands, see the *7210 SAS-Mxp, R6, R12, S, Sx, T Quality of Service Guide*, "Network QoS Policy Command Reference, Show Commands (for 7210 SAS-R6 and 7210 SAS-R12)".

7.4.1.12 Clear commands

```
clear
    - router
        - bgp
            - damping [{prefix/mask [neighbor ip-address]} | {group name}]
            - flap-statistics [[ip-prefix/mask] [neighbor ip-address]] | [group group-name] |
 [regex reg-exp] | [policy policy-name]
            - neighbor {ip-address | as as-number | external | all} [soft | soft-inbound |
 statistics]
```

```
            - protocol
        - interface [ip-int-name | ip-address] [icmp] [statistics]
clear
    - service
        - id service-id
            - spoke-sdp sdp-id:vc-id ingress-vc-label
        - statistics
            - sap sap-id {all | counters | stp}
            - sdp sdp-id keep-alive
            - id service-id
                - counters
                - spoke-sdp sdp-id:vc-id {all | counters | stp}
                - spoke-sdp
```

7.4.1.13 Debug commands

```
debug
    - service
        - id service-id
            - [no] event-type {config-change | svc-oper-status-change | sap-oper-status-change
 | sdpbind-oper-status-change}
            - [no] sap sap-id
                - event-type {config-change | oper-status-change}
            - [no] sdp sdp-id:vc-id
                - event-type {config-change | oper-status-change}
            - stp
                - [no] all-events
                - [no] bpdu
                - [no] core-connectivity
                - [no] exception
                - [no] fsm-state-changes
                - [no] fsm-timers
                - [no] port-role
                - [no] port-state
                - [no] sap sap-id
                - [no] sdp sdp-id:vc-id
```

7.4.2 Command descriptions

7.4.2.1 Configuration commands

7.4.2.1.1 Generic commands

shutdown

Syntax

[**no**] **shutdown**

Context

config>service>vprn

config>service>vprn>if

config>service>vprn>if>sap

config>service>vprn>bgp

config>service>vprn>bgp>group

config>service>vprn>bgp>group>neighbor

config>service>vprn>spoke-sdp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

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

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

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

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

If the ASN was previously changed, the BGP ASN inherits the new value.

Special Cases

Service Admin State

Bindings to an SDP within the service are put into the out-of-service state when the service is shut down. While the service is shut down, all customer packets are dropped and counted as discards for billing and debugging purposes.

A service is regarded as operational providing that one IP Interface SAP and one SDP is operational.

VPRN BGP

This command disables the BGP instance on the specified IP interface. Routes learned from a neighbor that is shut down are immediately removed from the BGP database and RTM. If BGP is globally shut down, all group and neighbor interfaces are shut down operationally. If a BGP group is shut down, all member neighbor interfaces are shut down operationally. If a BGP neighbor is shut down, just that neighbor interface is operationally shut down.

description

Syntax

description *description-string*

no description

Context

config>service>vprn>bgp

config>service>vprn

config>service>vprn>if

config>service>vprn>if>sap

config>service>vprn>bgp

config>service>vprn>bgp>group

config>service>vprn>bgp>group>neighbor

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

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

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

Parameters

description-string

Specifies the description character string. Allowed values are any string up to 80 characters composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

7.4.2.1.2 Global commands

vprn

Syntax

vprn *service-id* [**customer** *customer-id*] [**create**]

no vprn *service-id*

Context

config>service

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command creates or edits a Virtual Private Routed Network (VPRN) service instance.

If the *service-id* does not exist, a context for the service is created. If the *service-id* exists, the context for editing the service is entered.

VPRN services allow the creation of customer-facing IP interfaces in the same routing instance used for service network core routing connectivity. VPRN services require that the IP addressing scheme used by the subscriber must be unique between it and other addressing schemes used by the provider and potentially the entire Internet.

IP interfaces defined within the context of an VPRN service ID must have a SAP created as the access point to the subscriber network.

When a service is created, the **customer** keyword and *customer-id* must be specified and associate 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 recreated 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 this 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.

Parameters

service-id

Specifies the service ID 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 7210 SAS on which this service is defined.

Values *service-id*: 1 to 2147483648 *svc-name*: 64 characters maximum

customer customer-id

Specifies an existing customer ID number to be associated with the service. This parameter is required on service creation and optional for service editing or deleting.

Values 1 to 2147483647

create

Mandatory keyword for creating a VPRN service.

allow-export-bgp-vpn

Syntax

[**no**] **allow-export-bgp-vpn**

Context

config>service>vprn

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command causes the **vrf-export** and **vrf-target** commands to include BGP-VPN routes installed in the VPRN route table. These routes are usually not readvertisable as VPN-IP routes because of split-horizon.

When a BGP-VPN route is reexported, the route distinguisher and label values are rewritten according to the configuration of the reexporting VPRN.

Note:

- This command requires the **vrpn** context to be shut down and restarted for changes to take effect.
- This command can only be configured with VPRN loopback interfaces.

Caution: Before enabling the **allow-export-bgp-vpn** command, ensure that the routing updates do not loop back to the source. Failure to do so may cause the routes to become unstable.

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

Default

no allow-export-bgp-vpn

auto-bind-tunnel

Syntax

auto-bind-tunnel

Context

config>service>vprn

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

Commands in this context configure automatic binding of a VPRN service using tunnels to MP-BGP peers.

Users must configure the **resolution** option to enable auto-bind resolution to tunnels in TTM. If the **resolution** option is explicitly set to **disabled**, the auto-binding to tunnel is removed.

If the **resolution** is set to **any**, any supported tunnel type within the VPRN context is selected following the TTM preference. If one or more explicit tunnel types are specified using the **resolution-filter** option, only these tunnel types are selected again following the TTM preference.

The following tunnel types are supported in a VPRN context in order of preference: RSVP and LDP. The BGP tunnel type is not explicitly configured and is therefore implicit. It is always preferred over any other tunnel type enabled in the **auto-bind-tunnel** context.

The **ldp** value instructs BGP to search for an LDP LSP with a FEC prefix corresponding to the address of the BGP next hop.

The **rsvp** value instructs BGP to search for the best metric RSVP LSP to the address of the BGP next hop. This address can correspond to the system interface or to another loopback used by the BGP instance on the remote node. The LSP metric is provided by MPLS in the tunnel table. In the case of multiple RSVP LSPs with the same lowest metric, BGP selects the LSP with the lowest tunnel ID.

Users must set the **resolution** to **filter** to activate the list of tunnel-types configured under the **resolution-filter**.

When an explicit SDP to a BGP next-hop is configured in a VPRN service (using the **configure>service>vprn>spoke-sdp** command), it overrides the **auto-bind-tunnel** selection for that BGP next hop only. There is no support for reverting automatically to the **auto-bind-tunnel** selection if the explicit SDP goes down. The user must delete the explicit spoke-SDP in the VPRN service context to resume using the**auto-bind-tunnel** selection for the BGP next hop.

resolution

Syntax

resolution {**any** | **filter** | **disabled**}

Context

config>service>vprn>auto-bind-tunnel

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the resolution mode in the automatic binding of a VPRN service to tunnels to MP-BGP peers.

Parameters

any

Keyword that enables the binding to any supported tunnel type within the VPRN context following TTM preference.

filter

Keyword that enables the binding to the subset of tunnel types configured under resolution-filter.

disabled

Keyword that disables the automatic binding of a VPRN service to tunnels to MP-BGP peers.

resolution-filter

Syntax

resolution-filter

Context

config>service>vprn>auto-bind-tunnel

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the subset of tunnel types that can be used in the resolution of VPRN prefixes within the automatic binding of VPRN service to tunnels to MP-BGP peers.

The following tunnel types are supported in a VPRN context in order of preference: RSVP and LDP. The BGP tunnel type is not explicitly configured and is therefore implicit. It is always preferred over any other tunnel type enabled in the **auto-bind-tunne**l context.

Parameters

ldp

Keyword that selects the LDP tunnel type.

rsvp

Keyword that selects the RSVP-TE tunnel type.

autonomous-system

Syntax

autonomous-system *as-number*

no autonomous-system

Context

config>service>vprn

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command defines the autonomous system (AS) to be used by this VPN routing or forwarding (VRF).

The **no** form of this command removes the defined AS from this VPRN context.

Default

no autonomous-system

Parameters

as-number

Specifies the ASN for the VPRN service.

Values 1 to 4294967295

enable-bgp-vpn-backup

Syntax

enable-bgp-vpn-backup [**ipv4**] [**ipv6**]

no enable-bgp-vpn-backup

Context

config>service>vprn

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables only imported BGP-VPN routes from the remote PE to be considered when selecting the primary and backup paths. This command is required to support fast failover of ingress traffic from one remote PE to another remote PE.

Note: 7210 SAS devices do not consider multiple paths learned from CE BGP peers when selecting primary and backup path to reach the CE.

Default

no enable-bgp-vpn-backup

Parameters

ipv4

Keyword that allows BGP-VPN routes to be used as backup paths for IPv4 prefixes.

ipv6

Keyword that allows BGP-VPN routes to be used as backup paths for IPv6 prefixes.

grt-lookup

Syntax

grt-lookup

Context

config>service>vprn

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

Commands in this context configure GRT leaking commands. If all the supporting commands in the context are removed, this command is also removed.

source

Syntax

[**no**] **source** *ip-address*

Context

config>service>vprn>igmp>ssm-translate

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command specifies the source IP address for the group range. Whenever a (*,G) report is received in the range specified by **grp-range** *start* and *end* parameters, it is translated to an (S,G) report with the value of this object as the source address.

Parameters

ip-address

Specifies the IP address for sending data.

maximum-ipv6-routes

Syntax

maximum-ipv6-routes *number* [**log-only**] [**threshold** *percent*]

no maximum-ipv6-routes

Context

config>service>vprn

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command specifies the maximum number of remote IPv6 routes that can be held within a VPN routing/forwarding (VRF) context. Local, host, static, and aggregate routes are not counted.

The VPRN service ID must be in a shutdown state before **maximum-ipv6-routes** command parameters can be modified.

If the **log-only** parameter is not specified and the maximum-routes value is set below the existing number of routes in a VRF, the offending RIP peer (if applicable) is brought down (but the VPRN instance remains up). BGP peering remains up, but the exceeding BGP routes are not added to the VRF.

The maximum route threshold can dynamically change to increase the number of supported routes even when the maximum has already been reached. Protocols resubmit the routes that were initially rejected.

The **no** form of this command disables any limit on the number of routes within a VRF context. Issue the **no** form of this command only when the VPRN instance is shut down.

Default

0 or disabled

Parameters

number

Specifies the maximum number of routes to be held in a VRF context.

Values 1 to 2147483647

log-only

Keyword to specify that if the maximum limit is reached, only log the event. This keyword does not disable the learning of new routes.

threshold *percent*

Specifies the percentage at which a warning log message and SNMP trap should be set. There are two warnings, the first is a mid-level warning at the threshold value set, and the second is a high-level warning at a level between the maximum number of routes and the mid-level rate ([mid+max] / 2).

Values 0 to 100

maximum-routes

Syntax

maximum-routes *number* [**log-only**] [**threshold** *percent*]

no maximum-routes

Context

config>service>vprn

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command specifies the maximum number of remote routes that can be held within a VPN routing/forwarding (VRF) context. Local, host, static, and aggregate routes are not counted.

The VPRN service ID must be in a shutdown state before **maximum-routes** command parameters can be modified.

If the **log-only** parameter is not specified and the maximum-routes value is set below the existing number of routes in a VRF, the offending RIP peer (if applicable) is brought down (but the VPRN instance remains up). BGP peering will remain up but the exceeding BGP routes will not be added to the VRF.

The maximum route threshold can dynamically change to increase the number of supported routes even when the maximum has already been reached. Protocols resubmit the routes that were initially rejected.

The **no** form of this command disables any limit on the number of routes within a VRF context. Issue the **no** form of this command only when the VPRN instance is shut down.

Default

0 or disabled

Parameters

number

Specifies the maximum number of routes to be held in a VRF context.

Values 1 to 2147483647

log-only

Keyword to specify that if the maximum limit is reached, only log the event. This keyword does not disable the learning of new routes.

threshold *percent*

Specifies the percentage at which a warning log message and SNMP trap should be set. There are two warnings, the first is a mid-level warning at the threshold value set and the second is a high-level warning at level between the maximum number of routes and the mid-level rate ([mid+max] / 2).

Values 0 to 100

route-distinguisher

Syntax

route-distinguisher [**rd**]

no route-distinguisher

Context

config>service>vprn

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command sets the identifier attached to routes to which the VPN belongs. Each routing instance must have a unique (within the carrier domain) route distinguisher associated with it. A route distinguisher must be defined for a VPRN to be operationally active.

Default

no route-distinguisher

Parameters

ip-address:number

Specifies the IP address in dotted-decimal notation. The assigned number must not be greater than 65535.

asn:number

Specifies the ASN as a 2-byte value less than or equal to 65535. The assigned number can be any 32-bit unsigned integer value.

rd

Specifies the route distinguisher value.

Values *ip-addr:comm-val* | *2byte-asnumber:ext-comm-val* | *4byte-asnumber:comm-val*

where:

ip-addr — IP address in the form a.b.c.d.

comm-val — 0 to 65535

2byte-asnumber — 1 to 65535

ext-comm-val — 0 to 4294967295

4byte-asnumber — 0 to 4294967295

router-id

Syntax

router-id *ip-address*

no router-id

Context

config>service>vprn

config>service>vprn>ospf

config>service>vprn>bgp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command sets the router ID for a specific VPRN context.

If neither the router ID nor system interface are defined, the router ID from the base router context is inherited.

The **no** form of this command removes the router ID definition from the specified VPRN context.

Default

no router-id

Parameters

ip-address

Specifies the IP address in dotted-decimal notation.

service-name

Syntax

service-name *service-name*

no service-name

Context

config>service>vprn

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures an optional service name, up to 64 characters, which adds a name identifier to a specified service. The service name can be used for reference in configuration and show commands. This helps the service provider or administrator to identify and manage services within the 7210 SAS platforms.

All services are required to assign a service ID to initially create a service. However, either the service ID or the service name can be used to identify and reference a specified service when it is initially created.

Parameters

service-name

Specifies a unique service name to identify the service. Service names may not begin with an integer (0 to 9).

sgt-qos

Syntax

sgt-qos

Context

config>service>vprn

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

Commands in this context configure DSCP or dot1p re-marking for select self-generated traffic.

application

Syntax

application *dscp-app-name* **dscp** {*dscp-value* | *dscp-name*}

application *dot1p-app-name* **dot1p** *dot1p-priority*

no application {*dscp-app-name* | *dot1p-app-name*}

Context

config>service>vprn>sgt-qos

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures DSCP or dot1p re-marking for self-generated application traffic. When an application is configured using this command, the specified DSCP name/value is used for all packets generated by this application within the router instance in which it is configured. The instances can be base router, VPRN service, or management.

The values configured in this command do the following:

- set the DSCP bits in the IP packet
- map to the FC
- based on this FC, the egress QoS policy sets the Ethernet 802.1p and MPLS EXP bits. This includes ARP and IS-IS packets that, because of their nature, do not carry DSCP bits.
- DSCP value in the egress IP header is as configured in this command

Only one DSCP name/value can be configured per application. If multiple entries are configured, the subsequent entry overrides the previously configured entry.

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

Parameters

dscp-app-name

Specifies the DSCP application name.

Values bgp, icmp, igmp, ndis, ospf, pim, ssh, telnet, traceroute, vrrp, arp

dscp-value

Specifies a value when this packet egresses. The respective egress policy should provide the mapping for the DSCP value to either LSP-EXP bits or IEEE 802.1p (dot1p) bits, otherwise the default mapping applies.

Values 0 to 63

dscp-name

Specifies the DSCP name.

Values none, be, ef, cp1, cp2, cp3, cp4, cp5, cp6, cp7, cp9, cs1, cs2, cs3, cs4, cs5, nc1, nc2, af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, cp11, cp13, cp15, cp17, cp19, cp21, cp23, cp25, cp27, cp29, cp31, cp33, cp35, cp37, cp39, cp41, cp42, cp43, cp44, cp45, cp47, cp49, cp50, cp51, cp52, cp53, cp54, cp55, cp57, cp58, cp59, cp60, cp61, cp62, cp63

dot1p-priority

Specifies the dot1p priority.

Values none, or 0 to 7

dot1p-app-name

Specifies the dot1p application name.

Values The following values apply to the 7210 SAS-R6 and 7210 SAS-R12:

arp, isis

dscp

Syntax

dscp *dscp-name* **fc** *fc-name*

no dscp *dscp-name*

Context

config>service>vprn>sgt-qos

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command creates a mapping between the DSCP of the self-generated traffic and the forwarding class.

Self-generated traffic for configured applications that matches the specified DSCP are assigned to the corresponding forwarding class. Multiple commands can be entered to define the association of some or all 64 DSCPs to a forwarding class.

All DSCP names that define a DSCP value must be explicitly defined.

The **no** form of this command removes the DSCP-to-forwarding class association.

Parameters

dscp-name

Specifies the name of the DSCP to be associated with the forwarding class. A DSCP can only be specified by its name and only an existing DSCP can be specified. The software provides names for the well known code points.

Values be, ef, cp1, cp2, cp3, cp4, cp5, cp6, cp7, cp9, cs1, cs2, cs3, cs4, cs5, nc1, nc2, af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, cp11, cp13, cp15, cp17, cp19, cp21, cp23, cp25, cp27, cp29, cp31, cp33, cp35, cp37, cp39, cp41, cp42, cp43, cp44, cp45, cp47, cp49, cp50, cp51, cp52, cp53, cp54, cp55, cp57, cp58, cp59, cp60, cp61, cp62, cp63

fc *fc-name*

Specifies the forwarding class name. Applications and protocols that are configured using the **dscp** command use the configured IP DSCP value.

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

snmp-community

Syntax

snmp-community *community-name* [**version** *SNMP-version*]

no snmp-community [*community-name*]

Context

config>service>vprn

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command sets the SNMP community name to be used with the associated VPRN instance.

If an SNMP community name is not specified, SNMP access is not allowed.

The **no** form of this command removes the SNMP community name from the specified VPRN context.

Parameters

community-name

Specifies one or more SNMP community names.

version *SNMP-version*

Specifies the SNMP version.

Values v1, v2c, both

source-address

Syntax

source-address

Context

config>service>vprn

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

Commands in this context specify the source address and application that should be used in all unsolicited packets.

application

Syntax

application *app* [*ip-int-name* | *ip-address*]

no application *app*

Context

config>service>vprn>source-address

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command specifies the source address and application.

Parameters

app

Specifies the application name.

Values telnet, ssh, traceroute, ping

ip-int-name* | *ip-address

Specifies the name of the IP interface or IP address. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

static-route

Syntax

[**no**] **static-route** {*ip-prefix/prefix-length* | *ip-prefix netmask*} [**preference** *preference*] [**metric** *metric*] [**tag** *tag*] [**enable** | **disable**] {**next-hop** *ip-int-name* | *ip-address* | **ipsec-tunnel** *ipsec-tunnel-name*} [**bfd-enable** | {**cpe-check** *cpe-ip-address* [**interval** *seconds*] [**drop-count** *count*] [**log**]}]

[**no**] **static-route** {*ip-prefix/prefix-length* | *ip-prefix netmask*} [**preference** *preference*] [**metric** *metric*] [**tag** *tag*] [**enable** | **disable**] **indirect** *ip-address* [**cpe-check** *cpe-ip-address* [**interval** *seconds*] [**drop-count** *count*] [**log**]]

[**no**] **static-route** {*ip-prefix/prefix-length* | *ip-prefix netmask*} [**preference** *preference*] [**metric** *metric*] [**tag** *tag*] [**enable** | **disable**] **black-hole**

Context

config>service>vprn

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command creates static route entries within the associated router instance. When configuring a static route, the **next-hop**, **indirect**, or **black-hole** parameters must be configured.

The **no** form of this command deletes the static route entry. If a static route needs to be removed when multiple static routes exist to the same destination, as many parameters as are required to uniquely identify the static route must be entered.

If a CPE connectivity check target address is already being used as the target address in a different static route, the **cpe-check** parameters must match. If they do not, the new configuration command are rejected.

If a **static-route** command is issued with no **cpe-check** target but the destination *prefix/netmask* and **next-hop** matches a static route that did have an associated **cpe-check**, the **cpe-check** test is removed from the associated static route.

Parameters

ip-prefix

Specifies the destination address of the aggregate route in dotted-decimal notation.

Values

ipv4-prefix:	a.b.c.d (host bits must be 0)
ipv4-prefix-length:	0 to 32
ipv6-prefix:	x:x:x:x:x:x:x:x (eight 16-bit pieces)
	x:x:x:x:x:x:d.d.d.d
	x: [0 to FFFF]H
	d: [0 to 255]D

ipv6-prefix-length: 0 to 128

netmask

Specifies the subnet mask in dotted-decimal notation.

Values a.b.c.d (network bits all 1 and host bits all 0)

ip-int-name

Specifies the name of the IP interface. Interface names must be unique within the group of defined IP interfaces for **config router interface** and **config service ies interface** commands. An interface name cannot be in the form of an IP address. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

ip-address

Specifies the IP address of the IP interface. The *ip-addr* portion of the **address** command specifies the IP host address that is used by the IP interface within the subnet. This address must be unique within the subnet and specified in dotted-decimal notation.

Values ipv4-address a.b.c.d (host bits must be 0)

enable

Keyword to re-enable a disabled static route. Static routes can be administratively enabled or disabled. To enable a static route, it must be uniquely identified by the IP address, mask, and any other parameter that is required to identify the exact static route.

The administrative state is maintained in the configuration file.

Default enable

disable

Keyword to disable a static route while maintaining the static route in the configuration. Static routes can be administratively enabled or disabled. To enable a static route, it must be uniquely identified by the IP address, mask, and any other parameter that is required to identify the exact static route.

The administrative state is maintained in the configuration file.

Default enable

interval *seconds*

Optionally specifies the interval between ICMP pings to the target IP address.

Values 1 to 255 seconds

Default 1 seconds

drop-count *count*

Optionally specifies the number of consecutive ping-replies that must be missed to declare the CPE down and to de-active the associated static route.

Values Value range: 1 to 255

Default 3

log

Optional keyword to enable the ability to log transitions between active and in-active based on the CPE connectivity check. Events should be sent to the system log, syslog, and SNMP traps.

next-hop [*ip-address* | *ip-int-name*]

Specifies the directly connected next-hop IP address used to reach the destination. If the next hop is over an unnumbered interface, the *ip-int-name* of the unnumbered interface (on this node) can be configured.

The **next-hop** keyword and the **indirect** or **black-hole** keywords are mutually exclusive. If an identical command is entered (with the exception of either the **indirect** or **black-hole** parameters), this static route is replaced with the newly entered command, and unless specified, the respective defaults for **preference** and **metric** are applied.

The *ip-addr* configured here can be either on the network side or the access side on this node. This address must be associated with a network directly connected to a network configured on this node.

ipsec-tunnel *ipsec-tunnel-name*

Specifies an IPSec tunnel name, up to 32 characters.

indirect *ip-address*

Specifies that the route is indirect and specifies the next-hop IP address used to reach the destination.

The configured *ip-addr* is not directly connected to a network configured on this node. The destination can be reachable via multiple paths. The static route remains valid as long as the address configured as the indirect address remains a valid entry in the routing table. Indirect static routes cannot use an ip-prefix/mask to another indirect static route.

The **indirect** keyword and the **next-hop** or **black-hole** keywords are mutually exclusive. If an identical command is entered (with the exception of either the **next-hop** or **black-hole** parameters), this static route is replaced with the newly entered command and unless specified the respective defaults for **preference** and **metric** are be applied.

The *ip-addr* can be either on the network or the access side and is at least one hop away from this node.

black-hole

Keyword to specify a blackhole route, meaning that if the destination address on a packet matches this static route it is silently discarded.

The **black-hole** keyword is mutually exclusive with either the **next-hop** or **indirect** keywords. If an identical command is entered, with exception of either the **next-hop** or **indirect** parameters, the static route is replaced with the new command, and unless specified, the respective defaults for **preference** and **metric** are applied.

preference *preference*

Specifies the preference of this static route (as opposed to the routes from different sources such as BGP or OSPF), expressed as a decimal integer. When modifying the **preference** value of an existing static route, the metric does not change unless specified.

If multiple routes are learned with an identical preference using the same protocol, the lowest cost route is used. If multiple routes are learned with an identical preference using

the same protocol and the costs (metrics) are equal, the decision of which route to use is determined by the configuration of the **ecmp** command.

Default 5

Values 1 to 255

metric ***metric***

Specifies the cost metric for the static route, expressed as a decimal integer. This value is used when importing this static route into other protocols, such as OSPF. This value is also used to determine the static route to install in the forwarding table. When modifying the **metric** values of an existing static route, the preference does not change unless specified.

If there are multiple static routes with the same preference but unequal metrics, the lower cost (metric) route is installed. If there are multiple static routes with equal preference and metrics, ECMP rules apply. If there are multiple routes with unequal preferences, the lower preference route is installed.

Default 1

Values 0 to 65535

tag

Keyword to add a 32-bit integer tag to the static route. The tag is used in route policies to control distribution of the route into other protocols.

Values 1 to 4294967295

bfd-enable

Keyword to associate the state of the static route to a BFD session between the local system and the configured next hop. This keyword cannot be configured if the next hop is **indirect** or a **black-hole** keyword is specified. See the *7210 SAS-Mxp, R6, R12, S, Sx, T Router Configuration Guide* for more information about the protocols and platforms that support BFD.

cpe-check ***target-ip-address***

Specifies the IP address of the target CPE device. ICMP pings are sent to this target IP address. This parameter must be configured to enable the CPE connectivity feature for the associated static route. The *target-ip-address* cannot be in the same subnet as the static route subnet to avoid possible circular references. This option and BFD support on a specified static route are mutually exclusive.

Default no cpe-check enabled

vrf-export

Syntax

vrf-export *policy-name* [*policy-name*...(up to 15 max)]

no vrf-export

Context

config>service>vprn

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command specifies the export policies to control routes exported from the local VPN routing/forwarding (VRF) to other VRFs on the same or remote PE routers (via MP-BGP).

The **no** form of this command removes all route policy names from the export list.

Parameters

policy-name

Specifies the route policy statement name, up to 32 characters.

vrf-import

Syntax

vrf-import *policy-name* [*policy-name*...(up to 15 max)]

no vrf-import

Context

config>service>vprn

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the import policies to control routes imported to the local VPN routing/forwarding (VRF) from other VRFs on the same or remote PE routers (via MP-BGP). BGP-VPN routes imported using a **vrf-import** policy use the BGP preference value of 170 when imported from remote PE routers, or retain the protocol preference value of the exported route when imported from other VRFs on the same router, unless the preference is changed by the policy.

The **no** form of this command removes all route policy names from the import list.

Parameters

policy-name

Specifies the route policy statement name.

vrf-target

Syntax

vrf-target {**ext-community** | **export** *ext-community* | **import** *ext-community*}

no vrf-target

Context

config>service>vprn

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command facilitates a simplified method to configure the route target to be added to advertised routes or compared against received routes from other VRFs on the same or remote PE routers (via MP-BGP).

BGP-VPN routes imported with a **vrf-target** statement use the BGP preference value of 170 when imported from remote PE routers, or retain the protocol preference value of the exported route when imported from other VRFs in the same router.

Specified **vrf-import** or **vrf-export** policies override the **vrf-target** policy.

The **no** form of this command removes the vrf-target

Default

no vrf-target

Parameters

ext-community

Specifies an extended BGP community in the *type*:*x*:*y* format. The value **x** can be an integer or IP address. The **type** can be the target or origin. **x** and **y** are 16-bit integers.

Values *ip-addr:comm-val* | *2byte-asnumber:ext-comm-val* | *4byte-asnumber:comm-val*

where:

ip-addr — IP address in the form a.b.c.d.

comm-val — 0 to 65535

2byte-asnumber — 0 to 65535

ext-comm-val — 0 to 4294967295

4byte-asnumber — 0 to 4294967295

import *ext-community*

Specifies communities allowed to be accepted from remote PE neighbors.

export *ext-community*

Specifies communities allowed to be sent to remote PE neighbors.

7.4.2.1.3 Multicast VPN commands

mvpn

Syntax

mvpn

Context

config>service>vprn

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

Commands in this context configure MVPN-related parameters for the IP VPN.

auto-discovery

Syntax

[**no**] **auto-discovery** [**default**]

Context

config>service>vprn>mvpn

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables MVPN membership auto-discovery through BGP. When auto-discovery is enabled, PIM peering on the inclusive provider tunnel is disabled.

The **no** form of this command disables MVPN membership auto-discovery through BGP.

Default

enabled

c-mcast-signaling

Syntax

c-mcast-signaling {**bgp**}

no c-mcast-signaling

Context

config>service>vprn>mvpn

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command specifies BGP or PIM, for PE-to-PE signaling of CE multicast states. When this command is set to PIM and neighbor discovery by BGP is disabled, PIM peering is enabled on the inclusive tree.

Changes may be made to this command only when the MVPN node is shutdown.

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

Default

mcast-signaling bgp

Parameters

bgp

Specifies to use BGP for PE-to-PE signaling of CEmulticast states. Auto-discovery must be enabled.

intersite-shared

Syntax

intersite-shared

no intersite-shared

Context

config>service>vprn>mvpn

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command specifies whether to use inter-site shared C-trees.

Default

intersite-shared

mdt-type

Syntax

mdt-type {**sender-receiver** | **sender-only** | **receiver-only**}

no mdt-type

Context

config>service>vprn>mvpn

Platforms

Supported on all 7210 SAS as described in this document

Description

This command restricts MVPN instances per PE node to a specific role. By default, the MVPN instance on a specific PE node assumes the role of sender and receiver. This creates a mesh of MDT/PMSI across all PE nodes from this PE.

This command provides an option to configure either a **sender-only** or **receiver-only** mode per PE node. Restricting the PE node to a specific role prevents the creation of full mesh of MDT/PMSI across all participating PE nodes in the MVPN instance.

The **auto-rp-discovery** command cannot be enabled together with the **mdt-type sender-only**, **mdt-type receiver-only**, or **wildcard-spmsi** configurations.

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

Default

mdt-type sender-receiver

Parameters

sender-receiver

Keyword to connect both senders and receivers to the PE node for MVPN.

sender-only

Keyword to connect only senders to the PE node for MVPN.

receiver-only

Keyword to connect only receivers to the PE node for MVPN.

provider-tunnel

Syntax

provider-tunnel

Context

config>service>vprn>mvpn

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables context to configure tunnel parameters for the MVPN.

inclusive

Syntax

inclusive

Context

config>service>vprn>mvpn>pt

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables the context for specifying inclusive provider tunnels.

bsr

Syntax

bsr {**unicast** | **spmsi**}

no bsr

Context

config>service>vprn>mvpn>pt>inclusive

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the type of bootstrap router (BSR) signaling used.

The **no** form of this command restores the default.

Default

no bsr

Parameters

unicast

Keyword to send or forward BSR PDUs using unicast PDUs (default).

spmsi

Keyword to send or forward BSR PDUs using S-PMSI full mesh.

mldp

Syntax

mldp

no mldp

Context

config>service>vprn>mvpn>provider-tunnel>inclusive

config>service>vprn>mvpn>provider-tunnel>selective

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables use of mLDP LSP for the provider tunnel.

Default

no mldp

shutdown

Syntax

shutdown

no shutdown

Context

config>service>vprn>mvpn>provider-tunnel>inclusive>mldp

config>service>vprn>mvpn>provider-tunnel>selective

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command administratively disables and enables use of mLDP LSP for the provider tunnel.

Default

no shutdown

rsvp

Syntax

rsvp

no rsvp

Context

config>service>vprn>mvpn>pt>inclusive

config>service>vprn>mvpn>pt>selective

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables use of P2MP RSVP as the inclusive or selective provider tunnel

The **no** form of this command removes the **rsvp** context, including all the statements in the context.

Default

no rsvp

lsp-template

Syntax

lsp-template *lsp-template*

no lsp-template

Context

config>service>vprn>mvpn>pt>inclusive>rsvp

config>service>vprn>mvpn>pt>exclusive>rsvp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the use of an automatically created P2MP LSP as the inclusive or selective provider tunnel. The P2MP LSP is signaled using the parameters specified in the template, such as bandwidth constraints.

The **no** form of the command removes the configuration.

Default

no lsp-template

Parameters

lsp-template

Specifies the LSP template name, up to 32 characters.

shutdown

Syntax

shutdown

no shutdown

Context

config>service>vprn>mvpn>pt>inclusive>rsvp

config>service>vprn>mvpn>pt>selective>rsvp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command administratively disables the use of RSVP P2MP LSP for the inclusive or selective provider tunnel.

The **no** form of this command administratively enables the use of RSVP P2MP LSP for the provider tunnel.

Default

no shutdown

wildcard-spmsi

Syntax

wildcard-spmsi

no wildcard-spmsi

Context

config>service>vprn>mvpn>pt>inclusive

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables RFC 6625 (C-*, C-*) S-PMSI functionality for NG-MVPN. When enabled, (C-*, C-*) S-PMSI is used instead of I-PMSI for this MVPN. Wildcard S-PMSI uses the I-PMSI LSP template.

The **auto-rp-discovery** command cannot be enabled together with **mdt-type sender-only** or **mdt-type receiver-only**, or **wildcard-spmsi** configurations.

The **no** form of this command disables the (C-*, C-*) S-PMSI functionality.

Default

no wildcard-spmsi

selective

Syntax

selective

Context

config>service>vprn>mvpn>provider-tunnel

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

Commands in this context specify selective provider tunnel parameters.

data-delay-interval

Syntax

data-delay-interval *value*

no data-delay-interval

Context

config>service>vprn>mvpn>provider-tunnel>selective

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command specifies the interval, in seconds, before a PE router connected to the source switches traffic from the inclusive provider tunnel to the selective provider tunnel.

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

Default

data-delay-interval 3

Parameters

value

Specifies the data delay interval, in seconds.

Values 3 to 180

data-threshold

Syntax

data-threshold {*c-grp-ip-addr/mask* | *c-grp-ip-addr netmask*}

no data-threshold {*c-grp-ip-addr/mask* | *c-grp-ip-addr netmask*}

Context

config>service>vprn>mvpn>provider-tunnel>selective

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command specifies the group range for which a switch from the inclusive provider tunnel to the selective provider tunnel for C-(S,G) must be triggered. On 7210 SAS this command provides an option to use selective provide tunnel, independent of the multicast data rate (that is, there is no rate-threshold configuration required). For C-(S,G) groups specified with this command, the selective provider tunnel is used.

For C-(S,G) groups not configured with this command, the inclusive provider tunnel is used.

Multiple statements are allowed in the configuration to specify multiple group ranges.

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

Parameters

group-address/mask

Specifies a multicast group address and netmask length.

maximum-p2mp-spmsi

Syntax

[**no**] **maximum-p2mp-spmsi**

Context

config>service>vprn>mvpn>provider-tunnel>selective

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command specifies the maximum number of RSVP P2MP or LDP P2MP S-PMSI tunnels for the mVPN. When the limit is reached, no more RSVP P2MP S-PMSI or LDP P2MP S-PMSI are created and the traffic over the data-threshold stayd on I-PMSI.

Default

maximum-p2mp-spmsi 10

Parameters

number

Specifies the maximum number of RSVP P2MP or LDP P2MP S-PMSI tunnel for the mVPN.

Values 1 to 510

umh-selection

Syntax

umh-selection {**highest-ip**}

no umh-selection

Context

config>service>vprn>mvpn

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command specifies the Upstream Multicast Hop (UMH) selection mechanism to use (highest IP address).

The **no** form of this command reverts to default value.

Default

umh-selection highest-ip

Parameters

highest-ip

Keyword to specify that the highest IP address is selected as the UMH.

vrf-export

Syntax

vrf-export {**unicast** | *policy-name* [*policy-name*...(up to 15 max)]}

no vrf-export

Context

config>service>vprn>mvpn

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command specifies the export policy (up to 15) to control MVPN routes exported from the local VRF to other VRFs on the same or remote PE routers.

Default

vrf-export unicast

Parameters

unicast

Keyword that specifies to use unicast VRF export policy for the MVPN.

policy-name

Specifies a route policy name.

vrf-import

Syntax

vrf-import {**unicast** | *policy-name* [*policy-name*...(up to 15 max)]}

no vrf-import

Context

config>service>vprn>mvpn

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command specifies the import policy (up to 15) to control MVPN routes imported to the local VRF from other VRFs on the same or remote PE routers.

Default

vrf-import unicast

Parameters

unicast

Keyword to specify to use a unicast VRF import policy for the MVPN.

policy-name

Specifies a route policy name.

vrf-target

Syntax

vrf-target {**unicast** | *ext-community* | **export unicast** | *ext-community* | **import unicast** | *ext-community*}

no vrf-target

Context

config>service>vprn>mvpn

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command specifies the route target to be added to the advertised routes or compared against the received routes from other VRFs on the same or remote PE routers. The VRF import or VRF export policies override the VRF target policy.

The **no** form of this command removes the VRF target.

Default

no vrf-target

Parameters

unicast

Keyword that specifies to use unicast **vrf-target** *ext-community* for the multicast VPN.

ext-comm

Specifies an extended BGP community in the **type**:**x**:**y** format. The value **x** can be an integer or IP address. The **type** can be the target or origin. **x** and **y** are 16-bit integers.

Values *ip-addr:comm-val* | *2byte-asnumber:ext-comm-val* | *4byte-asnumber:comm-val*

where:

ip-addr — IP address in the form a.b.c.d.

comm-val — 0 to 65535

2byte-asnumber — 0 to 65535

4byte-asnumber — 0 to 4294967295

import *ext-community*

Specifies communities allowed to be accepted from remote PE neighbors.

export *ext-community*

Specifies communities allowed to be sent to remote PE neighbors.

export

Syntax

export {**unicast** | *ext-community*}

Context

config>service>vprn>mvpn>vrf-target

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command specifies communitities to be sent to peers.

Parameters

unicast

Keyword that specifies to use unicast **vrf-target** *ext-community* for the multicast VPN.

ext-comm

Specifies an extended BGP community in the **type**:**x**:**y** format. The value **x** can be an integer or IP address. The **type** can be the target or origin. **x** and **y** are 16-bit integers.

Values *ip-addr:comm-val* | *2byte-asnumber:ext-comm-val* | *4byte-asnumber:comm-val*

where:

ip-addr — IP address in the form a.b.c.d.

comm-val — 0 to 65535

2byte-asnumber — 0 to 65535

4byte-asnumber — 0 to 4294967295

import

Syntax

import {**unicast** | *ext-community*}

Context

config>service>vprn>mvpn>vrf-target

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command specifies communitities to be accepted from peers.

Parameters

unicast

Keyword to specify to use unicast **vrf-target** *ext-community* for the multicast VPN.

ext-comm

Specifies an extended BGP community in the **type**:**x**:**y** format. The value **x** can be an integer or IP address. The **type** can be the target or origin. **x** and **y** are 16-bit integers.

Values *ip-addr:comm-val* | *2byte-asnumber:ext-comm-val* | *4byte-asnumber:comm-val*

where:

ip-addr — IP address in the form a.b.c.d.

comm-val — 0 to 65535

2byte-asnumber — 0 to 65535

4byte-asnumber — 0 to 4294967295

7.4.2.1.4 SDP commands

spoke-sdp

Syntax

[**no**] **spoke-sdp** *sdp-id*

Context

config>service>vprn

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command binds a service to an existing SDP. The SDP defines the transport tunnel to which this VPRN service is bound.

The SDP has an operational state that determines the operational state of the SDP within the service; for example, if the SDP is administratively or operationally down, the SDP for the service is down.

The SDP must already exist in the **config>service>sdp** context before it can be associated with a VPRN service. If the **sdp** *sdp-id* is not already configured, an error message is generated. If the *sdp-id* exists, a binding between the specific *sdp-id* and service is created.

SDPs must be explicitly associated and bound to a service to allow far-end 7210 SAS devices to participate in the service.

The **no** form of this command removes the SDP binding from the service; the SDP configuration is not affected. When the SDP binding is removed, no packets are forwarded to the far-end router.

Special Cases

VPRN

Several SDPs can be bound to a VPRN service. Each SDP must be destined for a different 7210 SAS router. If two *sdp-id* bindings terminate on the same 7210 SAS, an error occurs and the second SDP binding is rejected.

Parameters

sdp-id

Specifies the SDP identifier. Allowed values are integers for existing SDPs.

Values 1 to 17407

vc-id

Specifies the virtual circuit identifier.

Values 1 to 4294967295

spoke-sdp

Syntax

spoke-sdp *sdp-id* [**:***vc-id*] *vc-type* {**ether** } [**create**]

no spoke-sdp *sdp-id* [**:***vc-id*] *vc-type* {**ether** } [**create**]

Context

config>service>vprn>if

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command binds a service to an existing SDP.

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

The SDP has an operational state that determines the operational state of the SDP within the service; for example, if the SDP is administratively or operationally down, the SDP for the service is down.

The SDP must already be defined in the **config>service>sdp** context to associate an SDP with a service. If the **sdp** *sdp-id* is not already configured, an error message is generated. If the *sdp-id* does exist, a binding between that *sdp-id* and the service is created.

SDPs must be explicitly associated and bound to a service. If an SDP is not bound to a service, no far-end devices can participate in the service.

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

The **no** form of this command removes the SDP binding from the service. The SDP configuration is not affected; only the binding of the SDP to a service. When removed, no packets are forwarded to the far-end router.

Special Cases

VPRN

Several SDPs can be bound to a VPRN service. Each SDP must be destined for a different router. If two SDP ID bindings terminate on the same 7210 SAS, an error occurs and the second SDP is binding is rejected.

Parameters

sdp-id

Specifies the SDP identifier.

Values 1 to 17407

vc-id

Specifies the virtual circuit identifier.

Values 1 to 4294967295

vc-type

Specifies the encapsulation and pseudowire type for the spoke-SDP.

Values **ether** — Keyword to specify an Ethernet pseudowire

Default ether

egress

Syntax

egress

Context

cconfig>service>vprn>if>spoke-sdp

config>service>vprn>red-if>spoke-sdp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures an SDP context.

ingress

Syntax

ingress

Context

config>service>vprn>if>spoke-sdp

config>service>vprn>red-if>spoke-sdp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the SDP context.

vc-label

Syntax

vc-label *egress-vc-label*

no vc-label [*egress-vc-label*]

Context

config>service>vprn>if>spoke-sdp>egress

config>service>vprn>red-if>spoke-sdp>egress

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the egress VC label.

Parameters

egress-vc-label

Specifies a VC egress value that indicates a specific connection.

Values 16 to 1048575

vc-label

Syntax

vc-label *ingress-vc-label*

no vc-label [*ingress-vc-label*]

Context

config>service>vprn>>if>spoke-sdp>ingress

config>service>vprn>red-if>spoke-sdp>ingress

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the ingress VC label.

Parameters

ingress-vc-label

Specifies a VC ingress value that indicates a specific connection.

Values 2048 to 18431

filter

Syntax

filter ip *ip-filter-id*

no filter

Context

config>service>vprn>if>spoke-sdp>egress

config>service>vprn>if>spoke-sdp>ingress

config>service>vprn>red-if>spoke-sdp>ingress

config>service>vprn>red-if>spoke-sdp>egress

config>service>vprn>nw-if>egress

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command associates an IP filter policy with an ingress or egress SAP or IP interface. An IP filter policy can be associated with spoke SDPs. Filter policies control the forwarding and dropping of packets based on IP or MAC matching criteria.

The filter command is used to associate a filter policy that has 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 fails and an error message is 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 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 the **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 an IP filter policy. The filter ID must already exist within the created IP filters.

Values 1 to 65535

7.4.2.1.5 Interface commands

interface

Syntax

interface *ip-int-name*

no interface *ip-int-name*

Context

config>service>vprn

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command creates a logical IP routing interface for a VPRN. When created, attributes like an IP address and SAP can be associated with the IP interface.

This command creates and maintains IP routing interfaces within VPRN service IDs. The **interface** command can be executed in the context of a 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 IP interfaces defined by the **config router interface** and **config service vprn interface** commands. 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 using 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, no IP interface names are 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 the interface and all the associated configuration. The interface must be administratively shut down before issuing the **no interface** command.

For VPRN services, the IP interface must be shut down before the SAP on that interface may be removed. VPRN services do not have the **shutdown** command in the SAP CLI context. VPRN service SAPs rely on the interface status to enable and disable them.

Parameters

ip-int-name

Specifies the name of the IP interface. Interface names must be unique within the group of defined IP interfaces for **config router interface** and **config service vprn interface** commands. An interface name cannot be in the form of an IP address. Interface names can be from 1 to 32 alphanumeric characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

If *ip-int-name* already exists within the service ID, the context is changed to maintain that IP interface. If *ip-int-name*already exists within another service ID or is an IP interface defined within the **config router** commands, an error occurs and the context is not changed to that IP interface. If *ip-int-name* does not exist, the interface is created and the context is changed to that interface for further command processing.

address

Syntax

address {*ip-address/mask* | *ip-address netmask*} [**broadcast** [**all-ones** | **host-ones**]

no address

Context

config>service>vprn>if

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command 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 7210 SAS.

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. When 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** 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 are stored in configuration files.

By default, no IP address or subnet association exists on an IP interface until it is explicitly created.

Use the **no** form of this command to remove the IP address assignment from the IP interface. When the **no address** command is entered, the interface becomes operationally down.

Table 93: Administrative and operational state values

Address	Administrative state	Operational state
No address	up	down
No address	down	down
1.1.1.1	up	up
1.1.1.1	down	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 adminstratively up state and an address is assigned, it becomes operationally up and the protocol interfaces and the MPLS LSPs associated with that IP interface are reinitialized.

Parameters

ip-address

Specifies the IP address of the IP interface. The *ip-address* portion of the **address** command specifies the IP host address that is used by the IP interface within the subnet. This address must be unique within the subnet and specified in dotted-decimal notation.

Values a.b.c.d (no multicast/broadcast address)

1.0.0.0 to 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

Specifies 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. A mask length of 32 is reserved for system IP addresses.

Values 0 to 30

netmask

Specifies 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 is used in a logical "AND" function to derive the local subnet of the IP address. A mask of 255.255.255.255 is reserved for system IP addresses.

Values 128.0.0.0 to 255.255.255.254

broadcast

Specifies to 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 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**) is received by the IP interface.

Default host-ones

all-ones

Keyword following the **broadcast** parameter that specifies the broadcast address used by the IP interface for this IP address is 255.255.255.255, also known as the local broadcast.

host-ones

Keyword following the **broadcast** parameter that specifies that the broadcast address used by the IP interface for this IP address is 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 negation feature, which is usually used to revert a parameter to the default value. To change the **broadcast**

type to **host-ones** after being changed to **all-ones**, the **address** command must be executed with the **broadcast** parameter defined.

allow-directed-broadcasts

Syntax

[**no**] **allow-directed-broadcasts**

Context

config>service>vprn>if

Platforms

Supported on all 7210 SAS platforms as described in this document

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 for the subnet broadcast address of the egress IP interface.

When enabled, a frame destined for the local subnet on this IP interface is sent as a subnet broadcast out this interface. Care should be exercised when allowing directed broadcasts, because it is a well-known mechanism used for denial-of-service attacks.

When disabled, directed broadcast packets discarded at this egress IP interface are counted in the normal discard counters for the egress SAP.

By default, directed broadcasts are not allowed and are 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

bfd

Syntax

bfd *transmit-interval* [**receive** *receive-interval*] [**multiplier** *multiplier*] [**echo-receive** *echo-interval*] [**type** *iom-hw*]

no bfd

Context

config>service>vprn>if

config>service>ies>if

Platforms

Supported on all 7210 SAS platforms as described in this document

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) are notified of the fault.

See the *7210 SAS-Mxp, R6, R12, S, Sx, T Router Configuration Guide* for information about the routing and MPLS protocols and features that can use BFD for protection on 7210 SAS platforms.

The **no** form of this command removes BFD from the associated IGP protocol adjacency.

Default

no bfd

Parameters

transmit-interval

Sets the transmit interval for the BFD session.

Values 10 to 100000

Default 100

receive *receive-interval*

Sets the receive interval for the BFD session.

Values 10 to 100000

Default 100

multiplier *multiplier*

Sets the multiplier for the BFD session.

Values 3 to 20

Default 3

echo-receive *echo-interval*

Sets the minimum echo receive interval, in milliseconds, for the BFD session.

Values 100 to 100000

Default 100

type *iom-hw*

Specifies the IOM hardware type.

local-proxy-arp

Syntax

[**no**] **local-proxy-arp**

Context

config>service>vprn>if

Platforms

Supported on all 7210 SAS platforms as described in this document

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 therefore becomes the forwarding point for all traffic between hosts in that subnet. When the **local-proxy-arp** command is enabled, ICMP redirects on the ports associated with the service are automatically blocked.

Default

no local-proxy-arp

loopback

Syntax

[**no**] **loopback**

Context

config>service>vprn>if

Platforms

Supported on all 7210 SAS platforms as described in this document

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, the configuration for the VPRN should have a loopback address configured that has the same address as the core instance system address (BGP next hop).

proxy-arp-policy

Syntax

[**no**] **proxy-arp-policy** *policy-name* [*policy-name*...(up to 5 max)]

Context

config>service>vprn>if

Platforms

Supported on all 7210 SAS platforms as described in this document

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

Specifies the export route policy name. Allowed values are any string up to 32 characters composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

remote-proxy-arp

Syntax

[**no**] **remote-proxy-arp**

Context

config>service>vprn>if

Platforms

Supported on all 7210 SAS platforms as described in this document

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

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command assigns up to 64 secondary IP addresses to the interface, including the primary IP address. Each address can be configured in an IP address, IP subnet, or broadcast address format.

Parameters

ip-address

Specifies the IP address of the IP interface. The ip-address portion of the address command specifies the IP host address that is used by the IP interface within the subnet. This address must be unique within the subnet and specified in dotted-decimal notation.

Values a.b.c.d

/

The forward slash is a parameter delimiter that 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* parameter. If a forward slash does not immediately follow the *ip-address*, a dotted decimal *netmask* must follow the prefix.

mask

Specifies 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* parameter. The *mask* 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. A mask length of 32 is reserved for system IP addresses.

Values 1 to 32

netmask

Specifies 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 *netmask* parameter indicates the complete mask that is used in a logical "AND"

function to derive the local subnet of the IP address. A netmask of 255.255.255.255 is reserved for system IP addresses.

Values a.b.c.d (network bits all 1 and host bits all 0)

broadcast {all-ones | host-ones}

Optional keyword to override 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 to a broadcast address of **host-ones**.

The **broadcast** parameter within the **address** command does not have a negation feature, which is usually used to revert a parameter to the default value. To change the broadcast type to **host-ones** after being configured as **all-ones**, the **address** command must be executed with the **broadcast** parameter defined. 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**) is received by the IP interface

Values **all-ones** — Keyword to specify that the broadcast address used by the IP interface for this IP address is 255.255.255.255, also known as the local broadcast. **host-ones** — Keyword to specify that the broadcast address used by the IP interface for this IP address is the subnet broadcast address. This is an IP address that corresponds to the local subnet described by the *ip-address* and *mask* or *netmask* with all of the host bits set to binary 1. This is the default broadcast address used by an IP interface.

Default host-ones

igp-inhibit

Keyword to specify that the secondary IP address should not be recognized as a local interface by the running IGP.

static-arp

Syntax

[**no**] **static-arp** *ip-address ieee-mac-address*

Context

config>service>vprn>if

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures a static ARP entry associating a subscriber IP address with a MAC address for the core router instance. This static ARP appears in the core routing ARP table. A static ARP can be configured only 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 is replaced with the new MAC address.

The **no** form of this command removes a static ARP entry.

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.

7.4.2.1.6 Router advertisement commands

router-advertisement

Syntax

[**no**] **router-advertisement**

Context

config>service>vprn

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures router advertisement properties. By default, it is disabled for all IPv6 enabled interfaces.

The **no** form of this command disables all IPv6 interface. However, the **no interface** *interface-name* command disables a specific interface.

Default

disabled

interface

Syntax

[**no**] **interface** *ip-int-name*

Context

config>service>vprn>router-advertisement

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures router advertisement properties on a specific interface. The interface must already exist in the **config>router>interface** context.

Parameters

ip-int-name

Specifies the interface name. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

current-hop-limit

Syntax

current-hop-limit *number*

no current-hop-limit

Context

config>service>vprn>router-advert>if

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the current hop limit in the router advertisement messages. It informs the nodes on the subnet about the hop limit when originating IPv6 packets.

Default

64

Parameters

number

Specifies the hop limit. A value of zero means there is an unspecified number of hops.

Values 0 to 255

managed-configuration

Syntax

[**no**] **managed-configuration**

Context

config>service>vprn>router-advert>if

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command sets the managed address configuration flag. This flag indicates that DHCPv6 is available for address configuration in addition to any address autoconfigured using stateless address autoconfiguration.

Default

no managed-configuration

max-advertisement-interval

Syntax

[**no**] **max-advertisement-interval** *seconds*

Context

config>service>vprn>router-advert>if

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the maximum interval between sending router advertisement messages.

Default

600

Parameters

seconds

Specifies the maximum interval in seconds between sending router advertisement messages.

Values 4 to 1800

min-advertisement-interval

Syntax

[**no**] **min-advertisement-interval** *seconds*

Context

config>service>vprn>router-advert>if

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the minimum interval between sending ICMPv6 neighbor discovery router advertisement messages.

Default

200

Parameters

seconds

Specifies the minimum interval in seconds between sending ICMPv6 neighbor discovery router advertisement messages.

Values 3 to 1350

mtu

Syntax

[**no**] **mtu** *mtu-bytes*

Context

config>service>vprn>router-advert>if

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the MTU for the nodes to use to send packets on the link.

Default

no mtu

Parameters

mtu-bytes

Specifies the MTU for the nodes to use to send packets on the link.

Values 1280 to 9212

other-stateful-configuration

Syntax

[**no**] **other-stateful-configuration**

Context

config>service>vprn>router-advert>if

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command sets the "Other configuration" flag. This flag indicates that DHCPv6lite is available for autoconfiguration of other (non-address) information, such as DNS-related information or information about other servers in the network.

Default

no other-stateful-configuration

prefix

Syntax

[**no**] **prefix** [*ipv6-prefixIprefix-length*]

Context

config>service>vprn>router-advert>if

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures an IPv6 prefix in the router advertisement messages. To support multiple IPv6 prefixes, use multiple prefix statements. No prefix is advertised until explicitly configured using prefix statements.

Parameters

ip-prefix

Specifies the IP prefix for the prefix list entry in dotted-decimal notation.

Values

ipv4-prefix:	a.b.c.d (host bits must be 0)
ipv4-prefix-length:	0 to 32
ipv6-prefix:	x:x:x:x:x:x:x:x (eight 16-bit pieces)
	x:x:x:x:x:x:d.d.d.d
	x: [0 to FFFF]H
	d: [0 to 255]D
ipv6-prefix-length:	0 to 128

prefix-length

Keyword that specifies a route must match the most significant bits and have a prefix length.

Values 1 to 128

autonomous

Syntax

[**no**] **autonomous**

Context

config>service>vprn>router-advert>if>prefix

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command specifies whether the prefix can be used for stateless address autoconfiguration.

Default

enabled

on-link

Syntax

[**no**] **on-link**

Context

config>service>vprn>router-advert>if>prefix

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command specifies whether the prefix can be used for on-link determination.

Default

enabled

preferred-lifetime

Syntax

[**no**] **preferred-lifetime** {*seconds* | **infinite**}

Context

config>service>vprn>router-advert>if

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the remaining length of time in seconds that this prefix continues to be preferred, such as, time until deprecation.

The address generated from a deprecated prefix should not be used as a source address in new communications, but packets received on such an interface are processed as expected.

Default

604800

Parameters

seconds

Specifies the remaining length of time in seconds that this prefix continues to be preferred.

infinite

Keyword that specifies the prefix is always preferred. A value of 4,294,967,295 represents infinity.

valid-lifetime

Syntax

valid-lifetime {*seconds* | **infinite**}

Context

config>service>vprn>router-advert>if

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command specifies the length of time in seconds that the prefix is valid for the purpose of on-link determination. A value of all one bits (0xffffffff) represents infinity.

The address generated from an invalidated prefix should not appear as the destination or source address of a packet.

Default

2592000

Parameters

seconds

Specifies the remaining length of time in seconds that this prefix continues to be valid.

infinite

Keyword that specifies the prefix is always valid. A value of 4,294,967,295 represents infinity.

reachable-time

Syntax

reachable-time *milli-seconds*

no reachable-time

Context

config>service>vprn>router-advert>if

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures how long this router should be considered reachable by other nodes on the link after receiving a reachability confirmation.

Default

no reachable-time

Parameters

milli-seconds

Specifies the length of time the router should be considered reachable.

Values 0 to 3600000

retransmit-time

Syntax

retransmit-timer *milli-seconds*

no retransmit-timer

Context

config>service>vprn>router-advert>if

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the retransmission frequency of neighbor solicitation messages.

Default

no retransmit-time

Parameters

milli-seconds

Specifies how often the retransmission should occur.

Values 0 to 1800000

router-lifetime

Syntax

router-lifetime *seconds*

no router-lifetime

Context

config>service>vprn>router-advert>if

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command sets the router lifetime.

Default

1800

Parameters

seconds

Specifies the length of time, in seconds (relative to the time the packet is sent), that the prefix is valid for route determination.

Values 0, 4 to 9000

0 means that the router is not a default router on this link.

7.4.2.1.7 Interface Internet Control Message Protocol commands

icmp

Syntax

icmp

Context

config>service>vprn>if

config>service>vprn>sub-if>grp-if

config>service>vprn>nw-if

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures Internet Control Message Protocol (ICMP) parameters on a VPRN service.

mask-reply

Syntax

[**no**] **mask-reply**

Context

config>service>vprn>if>icmp

config>service>vprn>sub-if>grp-if>icmp

config>service>vprn>nw-if>icmp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables responses to 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 replies to mask requests.

The **no** form of this command disables replies to ICMP mask requests on the router interface.

Default

mask-reply

redirects

Syntax

redirects [*number seconds*]

no redirects

Context

config>service>vprn>if>icmp

config>service>vprn>sub-if>grp-if>icmp

config>service>vprn>nw-if>icmp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This commad configures the rate for 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 are 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 specified time interval.

By default, the 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

Parameters

number

Specifies the maximum number of ICMP redirect messages to send. This parameter must be specified with the *seconds* parameter.

Values 10 to 1000

seconds

Specifies the time frame, in seconds, used to limit the *number* of ICMP redirect messages that can be issued.

Values 1 to 60

ttl-expired

Syntax

ttl-expired *number seconds*

no ttl-expired

Context

config>service>vprn>if>icmp

config>service>vprn>sub-if>grp-if>icmp

config>service>vprn>nw-if>icmp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the rate ICMP TTL expired messages are issued by the IP interface.

By default, the 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

Specifies 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 to 1000

seconds

Specifies 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 to 60

unreachables

Syntax

unreachables [*number seconds*]

no unreachables

Context

config>service>vprn>if>icmp

config>service>vprn>sub-if>grp-if>icmp

config>service>vprn>nw-if>icmp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the rate for ICMP host and network destination unreachable messages issued 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 that can be issued on the interface for a specified time interval.

By default, the generation of ICMP destination unreachable 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 destination unreachable messages on the router interface.

Default

unreachables 100 10

Parameters

number

Specifies the maximum number of ICMP unreachable messages to send. This parameter must be specified with the *seconds* parameter.

Values 10 to 1000

seconds

Specifies the time frame in seconds used to limit the *number* of ICMP unreachable messages that can be issued.

Values 1 to 60

ip-mtu

Syntax

ip-mtu *octets*

no ip-mtu

Context

config>service>vprn>if

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the maximum IP transmit unit (packet) for the interface.

The MTU that is advertised from the VPRN size is:

MINIMUM((SdpOperPathMtu - EtherHeaderSize), (Configured ip-mtu))

By default (for Ethernet network interface) if **no ip-mtu** is configured, the packet size is (1568 - 14) = 1554.

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

Default

no ip-mtu

Parameters

octets

Specifies the number of octets in the IP-MTU.

Values 512 to 9000

7.4.2.1.8 Interface Service Access Point commands

sap

Syntax

sap *sap-id* [**create**]

no sap *sap-id*

Context

config>service>vprn>if

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command creates a Service Access Point (SAP) within a service. A SAP is a combination of port and encapsulation parameters that identify the service access point on the interface and within the 7210 SAS. 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 does 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 be associated with only a single service. A SAP can be defined only on a port that has been configured as an access port using the **config interface** *port-type port-id* **mode access** command.

If a port is shut down, all SAPs on that port become operationally down. When a service is shut down, SAPs for the service are not displayed as operationally down, although all traffic traversing the service is 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 are also deleted.

Special Cases

VPRN

A VPRN SAP must be defined on an Ethernet interface.

Parameters

sap-id

Specifies the physical port identifier portion of the SAP definition. See Common CLI command descriptions 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.

The *port-id* must reference a valid port type. The port must be configured as an access port.

create

Mandatory keyword to create an SAP instance.

split-horizon-group ***group-name***

Specifies the name of the split horizon group to which the SAP belongs.

tod-suite

Syntax

tod-suite *tod-suite-name*

no tod-suite

Context

config>service>vprn>if>sap

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

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

Default

no tod-suite

Parameters

tod-suite-name

Specifies a collection of policies (ACLs, QoS), including time-ranges, that define the full or partial behavior of a SAP or a subscriber. The suite can be applied to more than one SAP.

accounting-policy

Syntax

accounting-policy *acct-policy-id*

no accounting-policy

Context

config>service>vprn>if>sap

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command creates the accounting policy context that can be applied to an interface SAP or interface SAP spoke-SDP.

An accounting policy must be defined before it can be associated with a SAP. If the *policy-id* does not exist, an error message is generated.

A maximum of one accounting policy can be associated with a SAP at one time. Accounting policies are configured in the **config>log** context.

The **no** form of this command removes the accounting policy association from the SAP, and the accounting policy reverts to the default value.

Parameters

acct-policy-id

Specifies the accounting *policy-id* as configured in the **config>log>accounting-policy** context.

Values 1 to 99

collect-stats

Syntax

[**no**] **collect-stats**

Context

config>service>vprn>if>sap

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables accounting and statistical data collection for an interface SAP or interface SAP spoke-SDP, or network port. When applying accounting policies, by default the data is collected in the appropriate records and written to the designated billing file.

When the **no collect-stats** command is issued, the statistics are still accumulated by the IOM cards. However, the CPU does not obtain the results and write them to the billing file. If a subsequent **collect-stats** command is issued, the counters written to the billing file include all the traffic while the **no collect-stats** command was in effect.

Default

no collect-stats

dist-cpu-protection

Syntax

dist-cpu-protection *policy-name*

no dist-cpu-protection

Context

config>service>vprn>if>sap

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command assigns a valid existing Distributed CPU Protection (DCP) policy to a SAP. By default, no DCP policy is associated with the SAP.

The **no** form of this command disables the use of DCP policies for the SAP.

Default

no dist-cpu-protection

Parameters

policy-name

Specifies the name of the DCP policy, up to 32 characters.

7.4.2.1.9 Interface anti-spoofing commands

anti-spoof

Syntax

anti-spoof {**ip** | **mac** | **ip-mac** | **nh-mac**}

no anti-spoof-type

Context

config>service>vprn>if>sap

config>service>vprn>sub-if>grp-if>sap

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables anti-spoof filtering and optionally changes the anti-spoof matching type for the interface.

The type of anti-spoof filtering defines what information in the incoming packet is used to generate the criteria to look up an entry in the anti-spoof filter table. The parameter type defines the anti-spoof filter type enforced by the SAP when anti-spoof filtering is enabled.

The following are the default filter types:

- non-Ethernet encapsulation default anti-spoof filter type

  When enabled on a non-Ethernet encapsulated SAP, the anti-spoof filter default type is **ip**.

- Ethernet encapsulated default anti-spoof filter type

  When enabled on an Ethernet encapsulated SAP, the anti-spoof default type is **ip-mac**.

- default anti-spoof filter state

  By default, anti-spoof filtering is disabled on the SAP.

The **no** form of this command disables anti-spoof filtering on the SAP.

Parameters

ip

Keyword to specify that SAP anti-spoof filtering uses only the source IP address in its lookup. If a static host exists on the SAP without an IP address specified, the anti-spoof type **ip** command fails.

mac

Keyword to specify that SAP anti-spoof filtering uses only the source MAC address in its lookup. Setting the anti-spoof filter type to **mac** is not allowed on non-Ethernet encapsulated SAPs. If a static host exists on the SAP without a specified MAC address, the anti-spoof type **mac** command fails. The anti-spoof type **mac** command also fails if the SAP does not support Ethernet encapsulation.

ip-mac

Keyword to specify that SAP anti-spoof filtering uses both the source IP address and the source MAC address in its lookup. If a static host exists on the SAP without both the IP address and MAC address specified, the anti-spoof type **ip-mac** command fails. This is also true if the default anti-spoof filter type of the SAP is **ip-mac** and the default is not overridden. The anti-spoof type **ip-mac** command also fails if the SAP does not support Ethernet encapsulation.

nh-mac

Keyword to specify that the ingress anti-spoof is based on the source MAC address and the egress anti-spoof is based on the nh-ip-address.

arp-populate

Syntax

[**no**] **arp-populate**

Context

config>service>vprn>if

config>service>vprn>sub-if>subscriber-interface

config>service>vprn>sub-if>grp-if

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures populating static and dynamic hosts into the system ARP cache. When enabled, the host 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 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 are repopulated when all static and dynamic host information for the IP address are removed. Because 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 fails if an existing static subscriber host on the SAP does not have both MAC and IP addresses specified.

When the **arp-populate** command is enabled, creating a static subscriber host on the SAP without both an IP address and MAC address fails.

The **arp-populate** command can be enabled on only VPRN interfaces supporting Ethernet encapsulation.

The **no** form of this command disables ARP cache population functions for static and dynamic hosts on the interface. All static and dynamic host information in the system ARP cache are removed. Any existing static ARP entries previously inactive because of static or dynamic hosts are populated in the system ARP cache.

When **arp-populate** is enabled, the system does 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 the **arp-populate** command enabled.

Default

no arp-populate

arp-timeout

Syntax

arp-timeout *seconds*

no arp-timeout

Context

config>service>vprn>if

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the minimum time in seconds an ARP entry learned on the IP interface is 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 reverts to the default value.

Default

14400 seconds

Parameters

seconds

Specifies the minimum number of seconds a learned ARP entry is stored in the ARP table, expressed as a decimal integer. A value of zero specifies that the timer is inoperative and learned ARP entries are not aged.

Values 0 to 65535

delayed-enable

Syntax

delayed-enable *seconds* [**init-only**]

no delayed-enable

Context

config>service>vprn>if

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command delays making the 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 (for example, after a reboot). To ensure that the state has time to be synchronized, the **delayed-enable** timer can be specified. The optional **init-only** parameter specifies to use the **delayed-enable** 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 to 1200

init-only

Keyword that delays the initialization of the subscriber interface to give the system time to complete necessary tasks, such as allowing routing protocols to converge or MCS to synchronize the subscriber information. The delay occurs only immediately after a reboot.

host

Syntax

[**no**] **host** {[**ip** *ip-address* [**mac** *ieee-address*]} [**subscriber** *sub-ident-string*] [**sub-profile** *sub-profile-name*] [**sla-profile** *sla-profile-name*]

no host {[**ip** *ip-address*] [**mac** *ieee-address*]}

Context

config>service>vprn>if>sap

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command creates a static host for the SAP. Applications within the system that make use of static host entries include anti-spoof and source MAC population into the VPLS forwarding database.

Multiple static hosts can be defined on the SAP. Each host is identified by a source IP address, a source MAC address, or both a source IP and source MAC address. When anti-spoof is enabled on the SAP, the host information is populated into the SAP anti-spoof table, allowing ingress packets that match the entry to access the SAP. When the MAC address exists in the host definition, the MAC address is populated into the VPLS forwarding database and associates it with the SAP. The static host definition overrides static MAC entries using the same MAC and prevents dynamic learning of the MAC on another interface.

Defining a static host identical to an existing static host has no effect and does not generate a log or error message.

Every static host definition must have at least one address defined: IP or MAC.

Static hosts may exist on the SAP even with anti-spoof and **arp-populate** (VPRN) features disabled. When enabled, each feature has different requirements for static hosts.

The **no** form of this command removes a static entry from the system. The specified **ip** *address* and **mac** *address* must exactly match the IP and MAC addresses of the host as defined when it was created. When

a static host is removed from the SAP, the affect of its removal on the anti-spoof filter, ARP cache, or the VPLS forwarding database is also evaluated.

Parameters

anti-spoof

Keyword that specifies to use static and dynamic host information to populate entries into an anti-spoof filter table. The anti-spoof filter entries generated are of the same type as specified in the **anti-spoof** type parameter. If the SAP **anti-spoof** filter is defined as **mac**, each static host definition must specify a MAC address. If the SAP **anti-spoof** filter is defined as **ip**, each static host definition must specify an IP address. If the SAP **anti-spoof** filter is defined as **ip-mac**, each static host definition must specify both an IP address and MAC address. If the definition of a static host is attempted without addresses specified for the enabled **anti-spoof** filter, the static host definition fails.

arp-populate

Keyword that specifies to use static and dynamic host information to populate entries into the system ARP cache. This is only available on the VPRN service SAPs. Both a MAC address and IP address are required to populate an ARP entry in the system. If the definition of a static host is attempted without both a MAC and IP address specified when **arp-populate** is enabled, the static host definition fails.

fdb-populate

Keyword that is an implicit feature and uses the static host definition as a static MAC in the VPLS forwarding database. It cannot be enabled or disabled and has no effect on the ability to create static hosts without a MAC address specified. When a MAC address is specified for a static host, it is automatically populated into the VPLS forwarding database associated with the SAP on which the host is created. The static host MAC address overrides static MAC entries that use the same MAC and prevent dynamic learning of the MAC on another interface. Existing static MAC entries with the same MAC address as a static host are marked as inactive but not deleted. If all static hosts are removed from the SAP, the static MAC may be populated. New static MAC definitions for the VPLS instance may be created while a static host exists associated with the static MAC address.

ip *ip-address*

Optional parameter that specifies a static host. The IP address must be specified for **anti-spoof** *ip* and **anti-spoof** *ip-mac* commands. Only one static host can be configured on the SAP with a specified IP address. The following rules apply to configuring static hosts using an IP address.

- Only one static host can be defined using a specific IP address.
- Defining a static host with the same IP address as a previous static host overwrites the previous static host.
- If a static host has an IP address assigned, the MAC address for the host is optional (depending on the features enabled on the SAP).

mac *mac-address*

Optional parameter that specifies a static host. The MAC address must be specified for **anti-spoof** *ip* and **anti-spoof** *ip-mac*. Multiple static hosts may be configured with the same MAC address if each definition is distinguished by a unique IP address. The following rules apply to configuring static hosts using a MAC address:

- Multiple static hosts can share the same MAC address.

- Executing the host command with the same MAC address but a different IP address as an existing static host creates a new static host.
- If a static host has a MAC address assigned, the IP address for the host is optional (depending on the features enabled on the SAP).

Values 8k static and dynamic hosts per 10G forwarding complex per system.

subscriber *sub-ident-string*

Optional parameter that specifies an existing subscriber identification profile to be associated with the static subscriber host. The subscriber identification profile is configured using the **config>subscr-mgmt>sub-ident-policy** context. The subscriber information is used by the VPRN SAP **arp-reply-agent** to determine the correct handling of received ARP requests from subscribers.

- For VPRN SAPs with **arp-reply-agent** enabled with the optional *sub-ident* parameter, the static subscriber host *sub-ident-string* is used to determine whether an ARP request received on the SAP is sourced from a host belonging to the same subscriber as the destination host. When both the destination and source hosts from the ARP request are known on the SAP and the subscriber identifications do not match, the ARP request may be forwarded to the rest of the VPRN destinations.

  If the static subscriber host *sub-ident-string* is not defined, the host is not considered to belong to the same subscriber as another host on the SAP.

  If source or destination host is unknown, the hosts are not considered to belong to the same subscriber. ARP messages from unknown hosts are subject to anti-spoof filtering rules applied at the SAP.

  If *sub-ident* is not enabled on the SAP **arp-reply-agent**, subscriber identification matching is not performed on ARP requests received on the SAP.

  ARP requests are never forwarded back to the same SAP or within the receiving SAP split horizon group.

sub-profile *sub-profile-name*

Optional parameter that specifies an existing subscriber profile name to be associated with the static subscriber host. The subscriber profile is configured in the **config>subscr-mgmt>sub-profile** context.

sla-profile *sla-profile-name*

Optional parameter that specifies an existing SLA profile name to be associated with the static subscriber host. The SLA profile is configured in the **config>subscr-mgmt>sla-profile** context.

frame-relay

Syntax

frame-relay

Context

config>service>vprn>if>sap

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

Commands in this context configure Frame Relay parameters on the SAP.

frf-12

Syntax

[**no**] **frf-12**

Context

config>service>vprn>if>sap

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables the use of FRF12 headers.

The **no** form of this command disables the use of FRF12 headers.

ete-fragment-threshold

Syntax

ete-fragment-threshold *threshold*

no ete-fragment-threshold

Context

config>service>vprn>if>sap>frf-12

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command specifies the maximum length of a fragment to be transmitted.

The **no** form of this command reverts to the default.

Parameters

threshold

Specifies the maximum length of a fragment to be transmitted.

Values 128 to 512

Default 0

interleave

Syntax

interleave

no interleave

Context

config>service>vprn>if>sap>frame-relay>frf.12

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables interleaving of high priority frames and low-priority frame fragments within a FR SAP using FRF.12 end-to-end fragmentation.

When this option is enabled, only frames of the FR SAP non-expedited forwarding class queues are subject to fragmentation. The frames of the FR SAP expedited queues are interleaved, with no fragmentation header among the fragmented frames. This provides behavior similar to MLPPP Link Fragment Interleaving (LFI).

When this option is disabled, frames of all the FR SAP forwarding class queues are subject to fragmentation. However, the fragmentation header is not included when the frame size is smaller than the user-configured fragmentation size. In this mode, the SAP transmits all fragments of a frame before sending the next full or fragmented frame.

The receive direction of the FR SAP supports both modes of operation concurrently, with and without fragment interleaving.

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

Default

no interleave

scheduling-class

Syntax

scheduling-class *class-id*

Context

config>service>vprn>if>sap

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command specifies the scheduling class to use for this SAP.

Parameters

class-id

Specifies the scheduling class to use for this sap.

Values 0 to 3

Default 0

7.4.2.1.10 Interface SAP filter and QoS policy commands

egress

Syntax

egress

Context

config>service>vprn>if>sap

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

Commands in this context 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.

agg-rate-limit

Syntax

agg-rate-limit *agg-rate*

no agg-rate-limit

Context

config>service>vprn>if>sap>egress

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command defines a maximum total rate for all egress queues on a service SAP.

The port scheduler mode should be set to "sap-based" scheduling mode before using this command. The egress port scheduler enforces the aggregate queue rate for the SAP as it distributes its bandwidth to all the SAPs configured on the port. The port scheduler stops distributing bandwidth to member queues when it has detected that the aggregate rate limit has been reached.

A SAP aggregate scheduler is created for each instance of the SAP queues created on each of the member ports of the LAG. For a LAG, the port scheduler mode configured for the primary port is used for all the member ports of the LAG.

The scheduler mode is specified by the **scheduler-mode** command. To implement the **agg-rate-limit**, the scheduler mode must be specified as "sap-based". See the *7210 SAS-Mxp, R6, R12, S, Sx, T Interface Configuration Guide* for more information about the **scheduler-mode** command.

The **no** form of this command removes the aggregate rate limit from the SAP or multi-service site.

Parameters

agg-rate

Specifies the aggregate rate, in kilobits-per-second, that the queues on the SAP or MSS can operate.

Values 1 to 10000000, max

aggregate-meter-rate

Syntax

aggregate-meter-rate *rate-in-kbps* [**burst** *burst-in-kbits*] [**enable-stats**]

no aggregate-meter-rate

Context

config>service>vprn>if>sap>egress

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command associates a set of two counters to count total forwarded packets and octets and total dropped packets and octets. When the counter is enabled, the number of resources required increases by twice the number of resources taken up when counter is not used. If the **enable-stats** keyword is specified during the creation of the meter, the counter is allocated by the software, if available. To free up the counter and relinquish its use, the user can use the **no aggregate-meter-rate** command, and then recreate the meter using the **aggregate-meter-rate** command.

If egress rrame-based accounting is used, the SAP egress aggregate meter rate accounts for the Ethernet frame overhead. The system accounts for 12 bytes of IFG and 8 bytes of start delimiter. Frame-based counting does not affect the count of octets maintained by the counter, if it is in use.

Note:

- Before enabling this command for a SAP, resources must be allocated to this feature from the egress internal TCAM resource pool using the **configure system resource-profile egress-internal-tcam egress-sap-aggregate-meter** command. See the *7210 SAS-Mxp, R6, R12, S, Sx, T Basic System Configuration Guide* for more information.
- The egress aggregate meter is not FC aware. The forward and drop decisions are made based on the order the packets are sent out of the SAP by the egress port scheduler.

The **no** form of this command removes the egress aggregate policer from use.

Default

no aggregate-meter-rate

Parameters

rate-in-kbps

Specifies the rate in kilobits per second.

Values 1 to 100000000, max

Default max

burst-in-kbits

Specifies the burst size for the policer in kilobits. The burst size cannot be configured without configuring the rate.

Values 4 to 2146959, default

Default 512

enable-stats

Keyword to specify whether the counter that counts forwarded and dropped packets must be allocated.

filter

Syntax

filter ip *ip-filter-id ipv6 ipv6-filter-id*

filter [**mac** *mac-filter-id*]

no filter [**ip** *ip-filter-id* | *ipv6 ipv6-filter-id*]

no filter [**mac** *mac-filter-id*]

no filter

Context

config>service>vprn>if>sap>egress

config>service>vprn>if>sap>ingress

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command associates an IP filter policy with an ingress or egress 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 that has 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 fails and an error message is 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 is not removed from the system unless the scope of the created filter is set to **local**.

Parameters

ip *ip-filter-id*

Specifies the IP filter policy. The filter ID must already exist within the created IP filters.

Values 1 to 65535

ipv6 *ipv6-filter-id*

Specifies the IPv6 filter policy. The filter ID must already exist within the created IPv6 filters.

Values 1 to 65535

mac *mac-filter-id*

Specifies the MAC filter policy. The specified filter ID must already exist within the created MAC filters. The filter policy must already exist within the created MAC filters.

Values 1 to 65535

qos

Syntax

qos *policy-id*

qos *policy-id* [**enable-table-classification**]

no qos

Context

config>service>vprn>if>sap>egress

config>service>vprn>if>sap>ingress

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command associates a QoS policy with an ingress or egress SAP or IP interface.

QoS ingress and egress policies are important for the enforcement of SLA agreements. The policy ID must be defined before associating the policy with a SAP or IP interface. If the *policy-id* does not exist, an error is returned.

The **qos** command associates both ingress and egress QoS policies. The **qos** command only allows ingress policies to be associated on SAP or IP interface ingress, and only allows 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 policy of the same or different type replaces the earlier one with the new policy.

On the 7210 SAS-R6 and 7210 SAS-R12 (ingress), using the **enable-table-classification** keyword enables the use of IP DSCP tables to assign FC and profile on a per-SAP ingress basis. The match-criteria configured in the service ingress policy, which require CAM resources, are ignored. Only meters from the service ingress policy are used (and the meters still require CAM resources). The IP DSCP classification policy configured in the SAP ingress policy is used to assign FC and profile. The default FC is assigned from the SAP ingress policy.

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.

Note: On the 7210 SAS-R6 and 7210 SAS-R12, when the interface is associated with RVPLS, the behavior of the **qos** command is affected. See the and commands for information about classification behavior for RVPLS.

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 value.

Parameters

policy-id

Specifies the ingress or egress policy ID to associate with SAP or IP interface on ingress or egress. The policy ID must already exist.

Values 1 to 65535

enable-table-classification

Keyword that enables the use of table-based classification instead of CAM-based classification at SAP ingress. The FC and profile are taken from the IP DSCP classification policy configured in the ingress policy, along with the meters from the SAP ingress policy. Match-criteria entries in the SAP ingress policy are ignored.

ingress

Syntax

ingress

Context

config>service>vprn>if>sap

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

Commands in this context configure ingress SAP 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.

aggregate-meter-rate

Syntax

aggregate-meter-rate *rate-in-kbps* [**burst** *burst-in-kbits*]

no aggregate-meter-rate

Context

config>service>vprn>if>sap>ingress

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the SAP aggregate policer. The rate of the SAP aggregate policer must be specified by the user. The user can optionally specify the burst size for the SAP aggregate policer. The aggregate policer monitors the traffic on different FCs and determines the destination of the packet. The packet is either forwarded to an identified profile or dropped.

Note: The sum of the CIR rates of the individual FCs configured under the SAP cannot exceed the PIR rate configured for the SAP. Though the 7210 SAS does not block this configuration, it is not recommended for use.

The following table lists information about the final disposition of the packet based on the operating rate of the per-FC policer and the per-SAP aggregate policer.

Table 94: Final disposition of the packet based on per-FC and per-SAP policer or meter

Per-FC meter operating rate	Per-FC assigned color	SAP aggregate meter operating rate	SAP aggregate meter color	Final packet color
Within CIR	Green	Within PIR	Green	Green or In-profile
Within CIR[17]	Green	Above PIR	Red	Green or In-profile
Above CIR, Within PIR	Yellow	Within PIR	Green	Yellow or Out-of-Profile
Above CIR, Within PIR	Yellow	Above PIR	Red	Red or Dropped
Above PIR	Red	Within PIR	Green	Red or Dropped
Above PIR	Red	Above PIR	Red	Red or Dropped

When the SAP aggregate policer is configured, the per-FC policer can be configured only in "trtcm2" mode (RFC 4115).

Note: The meter modes "srtcm" and "trtcm1" are used in the absence of an aggregate meter.

The SAP ingress meter counters increment the packet or octet counts based on the final disposition of the packet.

If ingress frame-based accounting is used, the SAP aggregate meter rate accounts for the Ethernet frame overhead. The system accounts for 12 bytes of IFG and 8 bytes of start delimiter.

The **no** form of this command removes the aggregate policer from use.

Default

no aggregate-meter-rate

Parameters

rate-in-kbps

Specifies the rate in kilobits per second.

[17] This configuration is not recommended for use.

Values 01 to 20000000 | max

Default max

burst burst-in-kilobits

Specifies the burst size for the policer in kilobits. The burst size cannot be configured without configuring the rate.

Values 4 to 2146959

Default 512

meter-override

Syntax

[**no**] **meter-override**

Context

config>service>vprn>if>sap>ingress

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command, within the SAP ingress contexts, enables the context for specific overrides to one or more meters created on the SAP through the SAP ingress QoS policies.

The **no** form of this command removes existing meter overrides.

Default

no meter-override

meter

Syntax

meter *meter-id* [**create**]

no meter *meter-id*

Context

config>service>vprn>if>sap>ingress>meter-override

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command, within the SAP ingress contexts, enables the context for specific overrides to a specific meter created on the SAP through a sap-ingress QoS policies.

The **no** form of this command is used to remove any existing overrides for the specified meter-id.

Parameters

meter-id

Specifies the meter ID. The specified *meter-id* must exist within the SAP ingress QoS policy applied to the SAP. If the meter is not currently used by any forwarding class or forwarding type mappings, the meter does noty exist on the SAP. This does not preclude creating an **override** context for the *meter-id*.

create

Keyword that is required when a **meter** *meter-id* override node is being created and the system is configured to expect explicit confirmation that a new object is being created. When the system is not configured to expect explicit confirmation, the **create** keyword is not required.

adaptation-rule

Syntax

adaptation-rule [**pir** *adaptation-rule*] [**cir** *adaptation-rule*]

no adaptation-rule

Context

config>service>vprn>if>sap>ingress>meter-override>meter

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command overrides specific attributes of the specified meter adaptation rule parameters. The adaptation rule controls the method used by the system to derive the operational CIR and PIR settings when the meter is provisioned in hardware. For the CIR and PIR parameters individually, the system attempts to find the best operational rate depending on the defined constraint.

The **no** form of this command removes any explicitly defined constraints used to derive the operational CIR and PIR created by the application of the policy. When a specific **adaptation-rule** is removed, the default constraints for **rate** and **cir** apply.

Default

no adaptation-rule

Parameters

pir

Keyword that defines the constraints enforced when adapting the PIR rate defined within the **meter-override meter** command. The **pir** keyword requires a qualifier that defines the constraint used when deriving the operational PIR for the queue. When the **meter-override** command is not specified, the default applies.

When the meter mode in use is "trtcm2," this parameter is interpreted as EIR value. See the *7210 SAS-Mxp, R6, R12, S, Sx, T Quality of Service Guide* for a description and relevant notes for meter modes.

cir

Keyword that defines the constraints enforced when adapting the CIR rate defined within the **meter-override meter** command. The **cir** parameter requires a qualifier that defines the constraint used when deriving the operational CIR for the queue. When the **cir** parameter is not specified, the default constraint applies.

adaptation-rule

Specifies the criteria to use to compute the operational CIR and PIR values for this meter, while maintaining a minimum offset.

Values **max** — The **max**, **min**, and **closest** parameters are mutually exclusive. When **max** (maximum) is defined, the operational PIR for the meter is equal to or less than the administrative rate specified using the **meter-override** command.

min — The **min**, **max**, and **closest** parameters are mutually exclusive. When **min** (minimum) is defined, the operational PIR for the queue is equal to or greater than the administrative rate specified using the **meter-override** command.

closest — The **closest**, **min**, and **max** parameters are mutually exclusive. When **closest** is defined, the operational PIR for the meter is the rate closest to the rate specified using the **meter-override** command.

cbs

Syntax

cbs *size* [**kbits** | **bytes** | **kbytes**]

no cbs

Context

config>service>vprn>if>sap>ingress>meter-override>meter

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command provides a mechanism to override the default CBS for the meter. The *size* parameter specifies the maximum burst size that can be transmitted by the source while still complying with the CIR. If the transmitted burst is lower than the CBS value, the packets are marked as in-profile by the meter to indicate that the traffic is complying with meter configured parameters.

The **no** form of this command reverts the CBS size to the default value.

Default

32 kbits

Parameters

size

Specifies the value in either kbits, bytes, or kilobytes.

Values kbits: 4 to 2146959 | default

bytes: 512 to 274810752

kbytes: 1 to 268369

mbs

Syntax

mbs *size* [**kbits** | **bytes** | **kbytes**]

no mbs

Context

config>service>vprn>if>sap>ingress>meter-override>meter

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command overrides the default MBS for the meter. The *size* parameter specifies the maximum burst size that can be transmitted by the source while still complying with the CIR. If the transmitted burst is lower than the MBS value, the packets are marked as in-profile by the meter to indicate that the traffic is complying meter configured parameters.

The **no** form of this command reverts the MBS size to the default value.

Default

512kbits

Parameters

size

Specifies the value in either kbits, bytes, or kilobytes.

Values kbits: 4 to 2146959 | default
bytes: 512 to 274810752
kbytes: 1 to 268369

mode

Syntax

mode *mode*

no mode

Context

config>service>vprn>if>sap>ingress>meter-override>meter

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command is used to override the SAP ingress QoS policy configured mode parameters for the specified *meter-id*.

The **no** form of this command restores the policy defined metering and profiling mode to a meter.

Parameters

mode

Specifies the rate mode of the meter-override.

Values trtcm1, trtcm2, srtcm

rate

Syntax

rate cir *cir-rate* [**pir** *pir-rate*]

no rate

Context

config>service>vprn>if>sap>ingress>meter-override>meter

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command is used to override the SAP ingress QoS policy configured rate parameters for the specified *meter-id*.

The **no** form of this command restores the policy defined metering and profiling rate to a meter.

Default

max

The **max** default specifies the amount of bandwidth in kilobits per second (thousand bits per second). The **max** value is mutually exclusive to the *pir-rate* value.

Parameters

pir-rate

Specifies the administrative PIR rate, in kilobits, for the queue. When the **rate** command is executed, a valid PIR setting must be explicitly defined. When the **rate** command has not been executed, the default PIR of **max** is assumed. Fractional values are not allowed and must be entered as a positive integer.

When the meter mode is set to "trtcm2," the PIR value is interpreted as the EIR value. See the *7210 SAS-Mxp, R6, R12, S, Sx, T Quality of Service Guide* for more information.

The actual PIR rate is dependent on the queue **adaptation-rule** parameters and the hardware where the queue is provisioned.

Values 0 to 20000000 | max

Default max

cir-rate

Specifies to override the default administrative CIR used by the queue. When the **rate** command is executed, a CIR setting is optional. When the **rate** command has not been executed or the **cir** parameter is not explicitly specified, the default CIR (0) is assumed. Fractional values are not allowed and must be entered as a positive integer.

Values 0 to 20000000 | max

Default 0

ipsec-gw

Syntax

ipsec-gw *name*

no ipsec-gw

Context

config>service>vprn>if>sap

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the IPSec gateway.

Parameters

name

Specifies the IPSec gateway name, up to 32 characters.

default-secure-service

Syntax

default-secure-service *service-id* **ipsec-interface** *ip-int-name*

no default-secure-service

Context

config>service>vprn>if>sap>ipsec-gw

Platforms

Supported on all 7210 SAS platforms as described in this document

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 1 to 2147483648

default-tunnel-template

Syntax

default-tunnel-template *ipsec template identifier*

no default-tunnel-template

Context

config>service>vprn>if>sap>ipsec-gw

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the default tunnel policy template for the gateway.

Parameters

ipsec template id*

1 to 2048

ike-policy

Syntax

ike-policy *ike-policy-id*

no ike-policy

Context

config>service>vprn>if>sap>ipsec-gw

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the IKE policy for the gateway.

Parameters

ike-policy-id

Specifies the IKE policy ID.

Values 1 to 2048

local-gateway-address

Syntax

local-gateway-address *ip-address*

no local-gateway-address

Context

config>service>vprn>if>sap>ipsec-gw

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the ipsec-gateway local address.

Parameters

ip-address

Specifies the IP unicast address.

pre-shared-key

Syntax

pre-shared-key *key*

no pre-shared-key

Context

config>service>vprn>if>sap>ipsec-gw

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command specifies the shared secret between the two peers forming the tunnel.

Parameters

key

Specifies a pre-shared key for dynamic keying.

multi-service-site

Syntax

multi-service-site *customer-site-name*

no multi-service-site *customer-site-name*

Context

config>service>vprn>if>sap

config>service>vprn>sub-if>grp-if>sap

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command creates a new customer site or edits an existing customer site using the *customer-site-name* parameter. A customer site is an anchor point to create an ingress and egress virtual scheduler hierarchy. When scheduler policies are defined for ingress and egress, the scheduler names contained in each policy are created according to the parameters defined in the policy. Multi-service customer sites exist for the sole purpose of creating a virtual scheduler hierarchy and making it available to queues on multiple SAPs.

The scheduler policy association with the customer site prevents the scheduler policy from being deleted until after the scheduler policy is removed from the customer site. The multi-service-site object generates a log message indicating that the association was deleted because of scheduler policy removal.

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

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

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

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

When the maximum number of customer sites is exceeded, a configuration error occurs; the command does not execute and the CLI context does not change.

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

Parameters

customer-site-name

Specifies a unique customer site name within the context of the customer.

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

queue-override

Syntax

[**no**] **queue-override**

Context

config>service>epipe>sap>ingress

config>service>vpls>sap>ingress

config>service>ies>sap>ingress

config>service>vprn>sap>ingress

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command overrides values for the specified SAP egress or ingress QoS queue. These values override the corresponding ones specified in the associated SAP egress or ingress QoS policy.

queue

Syntax

[**no**] **queue** *queue-id*

Context

config>service>epipe>sap>ingress>queue-override

config>service>vpls>sap>ingress>queue-override

config>service>ies>sap>ingress>queue-override

config>service>vprn>sap>ingress>queue-override

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command specifies the ID of the queue whose parameters are to be overridden.

Parameters

queue-id

Specifies the queue ID whose parameters are to be overridden.

adaptation-rule

Syntax

adaptation-rule [**pir** *adaptation-rule*] [**cir** *adaptation-rule*]

no adaptation-rule

Context

config>service>epipe>sap>ingress>queue-override>queue

config>service>vpls>sap>ingress>queue-override>queue

config>service>ies>sap>ingress>queue-override>queue

config>service>vprn>sap>ingress>queue-override>queue

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command overrides specific attributes of the specified queue adaptation rule parameters. The adaptation rule controls the method used by the system to derive the operational CIR and PIR settings when the queue is provisioned in hardware. For the CIR and PIR parameters individually, the system attempts to find the best operational rate depending on the defined constraint.

The **no** form of this command removes any explicitly defined constraints used to derive the operational CIR and PIR created by the application of the policy. When a specific **adaptation-rule** is removed, the default constraints for **rate** and **cir** apply.

Default

no adaptation-rule

Parameters

pir

Keyword that defines the constraints enforced when adapting the PIR rate defined using the **queue** *queue-id* **rate** command. The **pir** parameter requires a qualifier that defines the constraint used when deriving the operational PIR for the queue. When the **rate** command is not specified, the default applies.

cir

Keyword that defines the constraints enforced when adapting the CIR rate defined using the **queue** *queue-id* **rate** command. The **cir** parameter requires a qualifier that defines the constraint used when deriving the operational CIR for the queue. When the **cir** parameter is not specified, the default constraint applies.

adaptation-rule

Specifies the criteria to use to compute the operational CIR and PIR values for this queue, while maintaining a minimum offset.

Values **max** — The **max**, **min**, and **closest** parameters are mutually exclusive. When **max** (maximum) is defined, the operational PIR for the queue is equal to or less than the administrative rate specified using the **rate** command.

min — The **min**, **max**, and **closest** parameters are mutually exclusive. When **min** (minimum) is defined, the operational PIR for the queue is equal to or greater than the administrative rate specified using the **rate** command.

closest — The **closest**, **min**, and **max** parameters are mutually exclusive. When **closest** is defined, the operational PIR for the queue is the rate closest to the rate specified using the **rate** command.

port-parent

Syntax

port-parent [**cir-level** *cir-level*] [**pir-level** *pir-weight*]

Context

config>service>epipe>sap>ingress>queue-override>queue

config>service>vpls>sap>ingress>queue-override>queue

config>service>ies>sap>ingress>queue-override>queue

config>service>vprn>sap>ingress>queue-override>queue

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the queue parameters *cir-level* and *pir-weight*. The system creates and associates a port-scheduler with every access port on the system. Every queue within a SAP is associated with the port scheduler available on the port on which the SAP is created. The port scheduler uses these parameters to apportion the bandwidth to all the queues competing for the available bandwidth.

Queues with the *cir-level* value set to 8 are treated differently by the software than other queues configured with different *cir-level* values. The PIR rate values configured for the *cir-level* 8 queues are ignored. Only CIR rate value is used and the PIR is set to the CIR value. In addition, when executing the **no** form of the rate command for a queue configured at *cir-level* 8, the default CIR (and PIR) value is set to 1.

The **no** form of this command sets the *cir-level* and *pir-weight* to default values.

Default

port-parent cir-level 1 pir-weight 1

Parameters

cir-level *cir-level*

Specifies the priority of the queue with respect to other queues. The priority of the queue is used only in the CIR loop. Level "8" is the highest priority and level "1" is the lowest priority.

In the PIR loop, the priority of the queues cannot be configured. The system assigns the priority to the queues based on the *cir-level* associated with the queue.

Values 1 to 8 (8 is the highest priority)

pir-weight ***pir-weight***

Specifies the relative weight of the queue with respect to the other queues. The weight parameter is used only in the PIR loop. If a queue level parameter is set to "8," the weight parameter is ignored by the system.

Values 1 to 100

queue-mgmt

Syntax

queue-mgmt *name*

Context

config>service>epipe>sap>ingress>queue-override>queue

config>service>vpls>sap>ingress>queue-override>queue

config>service>ies>sap>ingress>queue-override>queue

config>service>vprn>sap>ingress>queue-override>queue

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command specifies the WRED and buffer parameters associated with the queue.

All the queues in the system allocate buffers from the system pool.

Parameters

name

Specifies the name of the queue-management policy.

rate

Syntax

rate *pir-rate* [**cir** *cir-rate*]

no rate

Context

config>service>epipe>sap>ingress>queue-override>queue

config>service>vpls>sap>ingress>queue-override>queue

config>service>ies>sap>ingress>queue-override>queue

config>service>vprn>sap>ingress>queue-override>queue

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command overrides specific attributes of the specified queue PIR and CIR parameters. The PIR defines the maximum rate that the queue can transmit packets out an egress interface (for SAP egress queues). Defining a PIR does not necessarily guarantee that the queue can transmit at the intended rate. The actual rate sustained by the queue can be limited by oversubscription factors or available egress bandwidth.

The CIR defines the rate at which the system prioritizes the queue over other queues competing for the same bandwidth. In-profile packets are preferentially queued by the system at egress and at subsequent next-hop nodes where the packet can traverse. To be properly handled as in-profile or out-of-profile throughout the network, the packets must be marked accordingly for profiling at each hop.

The CIR can be used by the queue parent command *cir-level* and *cir-weight* parameters to define the amount of bandwidth considered to be committed for the child queue during bandwidth allocation by the parent scheduler.

The **rate** command can be executed at any time, altering the PIR and CIR rates for all queues created through the association of the SAP egress QoS policy with the *queue-id*.

The **no** form of this command reverts all queues created with the *queue-id* by association with the QoS policy to the default PIR and CIR parameters (**max**, 0).

Default

rate max cir 0

The **max** default specifies the amount of bandwidth in kilobits per second (thousand bits per second). The **max** value is mutually exclusive to the *pir-rate* value.

Parameters

pir-rate

Specifies the administrative PIR rate, in kilobits, for the queue. When the **rate** command is executed, a valid PIR setting must be explicitly defined. When the **rate** command has not been executed, the default PIR of **max** is assumed. Fractional values are not allowed and must be entered as a positive integer.

The actual PIR rate is dependent on the queue **adaptation-rule** parameters and the actual hardware where the queue is provisioned.

Values 0 to 20000000 | max

Default max

cir-rate

Specifies to override the default administrative CIR used by the queue. When the **rate** command is executed, a CIR setting is optional. When the **rate** command has not been executed or the **cir** parameter is not explicitly specified, the default CIR (0) is assumed.

Fractional values are not allowed and must be entered as a positive integer. The **sum** keyword specifies that the CIR be used as the summed CIR values of the children schedulers or queues.

Values 0 to 20000000 | max

scheduler-override

Syntax

[**no**] **scheduler-override**

Context

config>service>vprn>if>sap>egress

config>service>vprn>if>sap>ingress

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command specifies the set of attributes whose values have been overridden via management on this virtual scheduler. Clearing a specified flag reverts the corresponding overridden attribute to the value defined by the ingress scheduler policy on the SAP.

scheduler

Syntax

scheduler *scheduler-name*

no scheduler *scheduler-name*

Context

config>service>vprn>if>sap>egress>sched-override

config>service>vprn>if>sap>ingress>sched-override

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command overrides attributes of the specified scheduler name.

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

Each scheduler must have a unique name within the context of the scheduler policy; however the same name can be reused in multiple scheduler policies. If *scheduler-name* already exists within the policy tier

level (regardless of the inclusion of the **create** keyword), the context changes to that scheduler name for the purpose of editing the scheduler parameters. Modifications made to an existing scheduler are executed on all instantiated schedulers created through association with the policy of the edited scheduler. This can cause queues or schedulers to become orphaned (invalid parent association) and adversely affect the ability of the system to enforce service level agreements (SLAs).

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

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

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

When the maximum number of schedulers has been exceeded on the policy, a configuration error occurs and the command does not execute nor does the CLI context change. If the provided *scheduler-name* is invalid, a name syntax error occur, the command does not execute, and the CLI context does not change.

Parameters

scheduler-name

Specifies the name of the scheduler.

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

create

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

rate

Syntax

rate *pir-rate* [**cir** *cir-rate*]

no rate

Context

config>service>vprn>if>sap>egress>sched-override>scheduler

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

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

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

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

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

Parameters

pir-rate

Specifies the multiplier used to determine the PIR rate at which the queue operates. A value of 0 to 100000000 or the keyword **max** or **sum** is accepted. Any other value results in an error without modifying the current PIR rate.

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

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

The PIR parameter for SAP ingress queues does not have a negation (**no**) function. To revert the queue PIR rate to the default value, that value must be specified as the PIR value.

Values 1 to 100000000, **max**

Default max

cir *cir-rate*

Specifies a step-multiplier value that specifies the multiplier used to determine the CIR rate at which the queue operates. A value of 0 to 250 or the **max** keyword is accepted. Any other value results in an error without modifying the current CIR rate.

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

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

Values 0 to 10000000, **max**, **sum**

Default sum

7.4.2.1.11 Routed VPLS commands

ingress

Syntax

ingress

Context

config>service>ies>if>vpls

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

Commands in this context define the routed *ip-filter-id* optional filter overrides.

enable-table-classification

Syntax

[**no**] **enable-table-classification**

Context

config>service>vprn>if>vpls>ingress

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables and disables the use of IP DSCP table-based classification to assign FC and profile on a per-interface ingress basis.

The match-criteria configured in the service ingress policy, which require CAM resources, are ignored. Only meters from the service ingress policy are used (and the meters still require CAM resources). If an

IP DSCP classification policy is configured in the VPLS SAP ingress policy, it is not used to assign FC and profile.

The **no** form of this command disables table-based classification. When disabled, the IP ingress packets within a VPLS service attached to the IP interface use the SAP ingress QoS policy applied to the virtual port used by the packets, when defined.

Default

no enable-table-classification

routed-override-qos-policy

Syntax

routed-override-qos-policy *policy-id*

no routed-override-qos-policy

Context

config>service>vprn>if>vpls>ingress

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command specifies an IP DSCP classification policy that is applied to all ingress packets entering the VPLS service. The DSCP classification policy overrides existing SAP ingress QoS policies applied to SAPs for packets associated with the routing IP interface. The routed override QoS policy is optional and when it is not defined or it is removed, the IP routed packets use the existing SAP ingress QoS policy configured on the VPLS virtual port.

The **no** form of this command removes the IP DSCP classification policy from the ingress IP interface. When removed, the IP ingress routed packets within a VPLS service attached to the IP interface use the SAP ingress QoS policy applied to the virtual port used by the packets, when defined.

Default

no routed-override-qos-policy

Parameters

policy-id

Specifies the ID for the routed override QoS policy. Allowed values are integers that correspond to a previously created IP DSCP classification policy in the **configure>qos>dscp-classification** context.

Values 1 to 65535

v4-routed-override-filter

Syntax

v4-routed-override-filter *ip-filter-id*

no v4-routed-override-filter

Context

config>service>ies>if>vpls>ingress

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command specifies an IP filter ID that is applied to all ingress packets entering the VPLS service. The filter overrides the existing ingress IP filter applied to SAPs or SDP bindings for packets associated with the routing IP interface. The override filter is optional and if not defined or removed, the IP routed packets use the existing ingress IP filter on the VPLS virtual port.

The **no** form of this command is used to remove the IP routed override filter from the ingress IP interface. When removed, the IP ingress routed packets within a VPLS service attached to the IP interface use the IP ingress filter applied to the packets virtual port when defined.

Parameters

ip-filter-id

Specifies the ID for the IP filter policy. Allowed values are integers that correspond to a previously created IP filter policy in the **configure>filter>ip-filter** context.

Values 1 to 65535

7.4.2.1.12 Interface VRRP commands

vrrp

Syntax

vrrp *virtual-router-id* [**owner**]

no vrrp *virtual-router-id*

Context

config>service>vprn>if

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command creates or edits a Virtual Router ID (VRID) on the service IP interface. A VRID is internally represented in conjunction with the IP interface name. This allows the VRID to be used on multiple IP interfaces while representing different virtual router instances.

Two VRRP nodes can be defined on an IP interface. One, both, or none may be defined as owner. The nodal context of **vrrp** *virtual-router-id* is used to define the configuration parameters for the VRID.

The **no** form of this command removes the specified VRID from the IP interface. This terminates VRRP participation for the virtual router and deletes all references to the VRID. The VRID does not need to be shut down to remove the virtual router instance.

Parameters

virtual-router-id

Specifies a new virtual router ID or one that can be modified on the IP interface.

Values 1 to 255

owner

Keyword that defines the virtual router instance as an owner.

authentication-key

Syntax

authentication-key [*authentication-key* | *hash-key*] [**hash** | **hash2**]

no authentication-key

Context

config>service>vprn>if>vrrp

config>service>vprn>if>vrrp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command assigns a simple text password authentication key to generate master VRRP advertisement messages and validate received VRRP advertisement messages.

The **authentication-key** command is one of the few commands not affected by the presence of the **owner** keyword. If simple text password authentication is not required, this command is not required. If the command is re-executed with a different password key defined, the new key will be used immediately. If a no **authentication-key** command is executed, the password authentication key reverts to the default value. The **authentication-key** command may be executed at any time, altering the simple text password used when **authentication-key** password authentication method is used by the virtual router instance. The **authentication-type password** command does not need to be executed before defining the **authentication-key** command.

To change the current in-use password key on multiple virtual router instances:

- identify the current master
- shut down the virtual router instance on all backups
- execute the **authentication-key** command on the master to change the password key
- execute the **authentication-key** command and **no shutdown** command on each backup key

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

Parameters

authentication-key

Specifies the simple text password used when VRRP Authentication Type 1 is enabled on the virtual router instance. Type 1 uses a string eight octets long that is inserted into all transmitted VRRP advertisement messages and compared against all received VRRP advertisement messages. The authentication data fields are used to transmit the key.

The **authentication-key** parameter is expressed as a string consisting of up to eight alpha-numeric characters. Spaces must be contained in quotation marks (" "). The quotation marks are not considered part of the string.

The string is case-sensitive and is left-justified in the VRRP advertisement message authentication data fields. The first field contains the first four characters with the first octet (starting with IETF RFC bit position 0) containing the first character. The second field holds the fifth through eighth characters. Any unspecified portion of the authentication data field is padded with the value 0 in the corresponding octet.

Values Any 7-bit printable ASCII character.

exceptions:	double quote	(")	ASCII 34
	carriage return		ASCII 13
	line feed		ASCII 10
	tab		ASCII 9
	backspace		ASCII 8

hash-key

Specifies the hash key. The key can be any combination of ASCII characters up to 22 characters (encrypted). If spaces are used in the string, enclose the entire string in quotation marks (" ").

This is useful when a user must configure the parameter, but, for security purposes, the actual unencrypted key value is not provided.

hash

Specifies the key is entered in an encrypted form. If the **hash** parameter is not used, the key is assumed to be in a non-encrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** parameter specified.

hash2

Specifies the key is entered in a more complex encrypted form. If the **hash2** parameter is not used, the less encrypted **hash** form is assumed.

backup

Syntax

[**no**] **backup** *ip-address*

Context

config>service>vprn>if>vrrp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures virtual router IP addresses for the interface.

init-delay

Syntax

init-delay *seconds*

no init-delay

Context

config>service>vprn>if>vrrp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures a VRRP initialization delay timer.

Default

no init-delay

Parameters

seconds

Specifies the initialization delay timer for VRRP, in seconds.

Values 1 to 65535

mac

Syntax

[**no**] **mac** *ieee-mac-address*

Context

config>service>vprn>if>vrrp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command assigns a specific MAC address to an IP interface.

By default, the physical MAC address associated with the Ethernet interface that the SAP is configured on is used.

The **no** form of this command reverts the MAC address of the IP interface to the default value.

Parameters

ieee-mac-address

Specifies the 48-bit MAC address for the static ARP in the form *aa*:*bb*:*cc*:*dd*:*ee*:*ff* or *aa*-*bb*-*cc*-*dd*-*ee*-*ff*, where *aa*, *bb*, *cc*, *dd*, *ee* and *ff* are hexadecimal numbers. Allowed values are any non-broadcast, non-multicast MAC and non-IEEE reserved MAC addresses.

master-int-inherit

Syntax

[**no**] **master-int-inherit**

Context

config>service>vprn>if>vrrp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command allows the master instance to dictate the master down timer (non-owner context only).

Default

no master-int-inherit

message-interval

Syntax

message-interval {[*seconds*] [**milliseconds** *milliseconds*]}

no message-interval

Context

config>service>vprn>if

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command sets the advertisement timer and indirectly sets the master down timer on the virtual router instance. The **message-interval** setting must be the same for all virtual routers participating as a virtual router. Any VRRP advertisement message received with an advertisement interval field different from the virtual router instance configured message-interval value is silently discarded.

The **message-interval** command is available in both non-owner and owner **vrrp** *virtual-router-id* nodal contexts. If the **message-interval** command is not executed, the default message interval of 1 second is used.

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

Default

1 s

Parameters

seconds

Specifies the number of seconds that transpires before the advertisement timer expires.

Values 1 to 255

milliseconds ***milliseconds***

Specifies the milliseconds time interval between sending advertisement messages. This parameter is not supported on single-slot chassis.

Values 100 to 900

ping-reply

Syntax

[**no**] **ping-reply**

Context

config>service>vprn>if>vrrp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command allows the non-owner master to reply to ICMP echo requests directed at the virtual router instances IP addresses. The ping request can be received on any routed interface.

Ping must not have been disabled at the management security level (either on the parent IP interface or based on the ping source host address). When ping reply is not enabled, ICMP echo requests to non-owner master virtual IP addresses are silently discarded.

Non-owner backup virtual routers never respond to ICMP echo requests regardless of the setting of ping-reply configuration.

The **ping-reply** command is available only in the non-owner **vrrp** *virtual-router-id* context. If the **ping-reply** command is not executed, ICMP echo requests to the virtual router instance IP addresses are silently discarded.

The **no** form of this command reverts the default operation of discarding all ICMP echo request messages destined for the non-owner virtual router instance IP addresses.

Default

no ping-reply

policy

Syntax

policy *vrrp-policy-id*

no policy

Context

config>service>vprn>if>vrrp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command associates a VRRP priority control policy with the virtual router instance (non-owner context only).

Parameters

vrrp-policy-id

Specifies a VRRP priority control policy.

Values 1 to 9999

preempt

Syntax

preempt

no preempt

Context

config>service>vprn>if

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the ability to override an existing non-owner master with the virtual router instance. Enabling preempt mode is recommended for correct operation of the base-priority and vrrp-policy-id definitions on the virtual router instance. If the virtual router cannot preempt an existing non-owner master, the affect of the dynamic changing of the in-use priority is greatly diminished.

The **preempt** command is available only in the non-owner **vrrp** *virtual-router-id* context. The owner may not be preempted because the priority of non-owners can never be higher than the owner. The owner always preempts all other virtual routers when it is available.

Non-owner virtual router instances only preempt when preempt is set and the current master has an in-use message priority value less than the virtual router instance in-use priority.

A master non-owner virtual router only allows itself to be preempted when the incoming VRRP advertisement message priority field value is one of the following:

- creater than the virtual router in-use priority value
- equal to the in-use priority value, and the source IP address (primary IP address) is greater than the virtual router instance primary IP address

The **no** form of this command prevents a non-owner virtual router instance from preempting another, less desirable, virtual router.

Default

preempt

priority

Syntax

priority *priority*

no priority

Context

config>service>vprn>if>vrrp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures a specific priority value for the virtual router instance. In conjunction with an optional **policy** command, the base priority is used to derive the in-use priority of the virtual router instance.

The **policy** command is available only in the non-owner **vrrp** *virtual-router-id* context. The priority of owner virtual router instances is permanently set to 255 and cannot be changed. For non-owner virtual router instances, if the priority command is not executed, the base priority is set to 100.

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

Parameters

base-priority

Specifies the base priority used by the virtual router instance. If a VRRP priority control policy is not also defined, the base priority is the in-use priority for the virtual router instance.

Values 1 to 254

Default 100

ssh-reply

Syntax

[**no**] **ssh-reply**

Context

config>service>vprn>if>vrrp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command allows the non-owner master to reply to SSH requests directed at the virtual router instance IP addresses. The SSH request can be received on any routed interface. SSH must not have been disabled at the management security level (either on the parental IP interface or based on the SSH source host address). Correct login and CLI command authentication is still enforced.

When the **ssh-reply** command is not enabled, SSH packets to non-owner master virtual IP addresses are silently discarded. Non-owner backup virtual routers never respond to SSH regardless of the ssh-reply configuration.

The **ssh-reply** command is available only in the non-owner **vrrp** *virtual-router-id* context. If the **ssh-reply** command is not executed, SSH packets to the virtual router instance IP addresses are silently discarded.

The **no** form of this command reverts to the default operation of discarding all SSH packets destined to the non-owner virtual router instance IP addresses.

Default

no ssh-reply

standby-forwarding

Syntax

[**no**] **standby-forwarding**

Context

config>service>vprn>if>vrrp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command allows the forwarding of packets by a standby router.

The **no** form of this command specifies that a standby router should not forward traffic sent to the virtual router MAC address. The standby router should forward traffic sent to the real MAC address of the standby router.

Default

no standby-forwarding

telnet-reply

Syntax

[**no**] **telnet-reply**

Context

config>service>vprn>if>vrrp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command allows the non-owner master to reply to TCP port 23 Telnet requests directed at the virtual router instance IP addresses. The Telnet request can be received on any routed interface. Telnet must not

have been disabled at the management security level (either on the parental IP interface or based on the Telnet source host address). Correct login and CLI command authentication is still enforced.

When the **telnet-reply** command is not enabled, TCP port 23 Telnet packets to non-owner master virtual IP addresses are silently discarded.

Non-owner backup virtual routers never respond to Telnet requests regardless of the Telnet reply configuration.

The **telnet-reply** command is available only in the non-owner **vrrp** context. If the **telnet-reply** command is not executed, Telnet packets to the virtual router instance IP addresses are silently discarded.

The **no** form of this command reverts to the default operation of discarding all Telnet packets destined for the non-owner virtual router instance IP addresses.

Default

no telnet-reply

traceroute-reply

Syntax

[**no**] **traceroute-reply**

Context

config>service>vprn>if>vrrp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command allows a non-owner master to reply to traceroute requests directed to the virtual router instance IP addresses.

This command is valid only if the VRRP virtual router instance associated with this entry is a non-owner.

A non-owner backup virtual router never responds to traceroute requests regardless of the traceroute reply status.

Default

no traceroute-reply

7.4.2.1.13 Counter mode commands

statistics

Syntax

statistics

Context

config>service>vprn>if>sap

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

Commands in this context configure the counters associated with SAP ingress.

ingress

Syntax

ingress

Context

config>service>vprn>if>sap>statistics

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

Commands in this context configure the ingress SAP statistics counter.

counter-mode

Syntax

counter-mode {**in-out-profile-count** | **forward-drop-count**}

Context

config>service>vprn>if>sap>statistics>ingress

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command sets the counter mode for the counters associated with SAP ingress meters or policers. A pair of counters is available with each meter. These counters count different events based on the counter mode value.

Note: The counter mode can be changed if an accounting policy is associated with a SAP. If the counter mode is changed, the counters associated with the meter are reset and the counts are

cleared. If an accounting policy is in use when the counter mode is changed, a new record is written into the current accounting file.

Execute the following sequence of commands on the specified SAP to ensure the correct statistics are collected when the counter mode is changed.

1. Execute the **config service vprn interface sap no collect-stats** command to disable writing of accounting records for the SAP.
2. Change the counter mode to the needed option by executing the **config service vprn interface sap counter-mode** {**in-out-profile-count** | **forward-drop-count**} command.
3. Execute the **config service vprn interface sap collect-stats** command to enable writing of accounting records for the SAP.

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

Default

in-out-profile-count

Parameters

in-out-profile-count

Specifies that one counter counts the total in-profile packets and octets received on ingress of a SAP, and another counts the total out-of-profile packets and octets received on ingress of a SAP. A packet is determined to be in-profile or out-of-profile based on the meter rate parameters configured. A packet is dropped by the policer if it exceeds the configured PIR rate. Dropped counts are not maintained in hardware when this mode is used. It is obtained by subtracting the sum of in-profile count and out-of-profile count from the total SAP ingress received count and displayed.

forward-drop-count

Specifies that one counter counts the forwarded packets and octets received on ingress of a SAP and another counts the dropped packets. The forwarded count is the sum of in-profile and out-of-profile packets and octets received on SAP ingress. The dropped count is count of packets and octets dropped by the policer. A packet is determined to be in-profile or out-of-profile based on the meter rate parameters configured. A packet is dropped by the policer if it exceeds the configured PIR rate. The in-profile count and out-of-profile count is not individually available when operating in this mode.

7.4.2.1.14 BGP commands

bgp

Syntax

[**no**] **bgp**

Context

config>service>vprn

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables the BGP protocol on the VPRN service.

The **no** form of this command disables the BGP protocol on the VPRN service.

Default

no bgp

advertise-inactive

Syntax

[**no**] **advertise-inactive**

Context

config>service>vprn>bgp

config>service>vprn>bgp>group

config>service>vprn>bgp>group>neighbor

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the advertising of inactive BGP routers to other BGP peers.

By default, BGP only advertises BGP routes to other BGP peers if a specified BGP route is chosen by the route table manager as the most preferred route within the system and is active in the forwarding plane. This command allows system administrators to advertise a BGP route even though it is not the most preferred route within the system for a specified destination.

Default

no advertise-inactive

aggregator-id-zero

Syntax

[**no**] **aggregator-id-zero**

Context

config>service>vprn>bgp

config>service>vprn>bgp>group

config>service>vprn>bgp>group>neighbor

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command sets the router ID in the BGP aggregator path attribute to zero when BGP aggregates routes. This prevents different routers within an AS from creating aggregate routes that contain different AS paths.

When BGP is aggregating routes, it adds the aggregator path attribute to the BGP update messages. By default, BGP adds the ASN and router ID to the aggregator path attribute.

When this command is enabled, BGP adds the router ID to the aggregator path attribute. This command is used at the group level to revert to the value defined under the global level, and is used at the neighbor level to revert to the value defined under the group level.

The **no** form of this command used at the global level reverts to the default, where BGP adds the ASN and router ID to the aggregator path attribute.

The **no** form of this command used at the group level reverts to the value defined at the group level.

The **no** form of this command used at the neighbor level reverts to the value defined at the group level.

Default

no aggregator-id-zero

always-compare-med

Syntax

always-compare-med {**zero** | **infinity**}

no always-compare-med

Context

config>service>vprn>bgp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures how the Multi-Exit Discriminator (MED) path attribute is used in the BGP route selection process. The MED attribute is always used in the route selection process regardless of the peer AS that advertised the route. This parameter determines what MED value is inserted in the RIB-IN. If this parameter is not configured, only the MEDs of routes that have the same peer ASs are compared.

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

Default

no always-compare-med

Parameters

zero

Keyword to specify that for routes learned without a MED attribute that a zero (0) value is used in the MED comparison. The routes with the lowest metric are the most preferred.

infinity

Keyword to specify that for routes learned without a MED attribute that a value of infinity (4294967295) is used in the MED comparison. This in effect makes these routes the least desirable.

as-path-ignore

Syntax

[**no**] **as-path-ignore**

Context

config>service>vprn>bgp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command determines whether the AS path is used to determine the best BGP route.

If this option is enabled, the AS paths of incoming routes are not used in the route selection process.

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

Default

no as-path-ignore

as-override

Syntax

[**no**] **as-override**

Context

config>service>vprn>bgp>group

config>service>vprn>bgp>group>neighbor

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command replaces all instances of the peer AS number with the local ASN in a BGP route AS_PATH.

This command breaks the BGP loop detection mechanism. It should be used carefully.

Default

no as-override

authentication-key

Syntax

authentication-key [*authentication-key* | *hash-key*] [**hash** | **hash2**]

no authentication-key

Context

config>service>vprn>bgp

config>service>vprn>bgp>group

config>service>vprn>bgp>group>neighbor

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the BGP authentication key.

Authentication is performed between neighboring routers before setting up the BGP session by verifying the password. Authentication is performed using the MD-5 message-based digest. The authentication key can be any combination of letters or numbers from 1 to 16.

The **no** form of this command removes the authentication password from the configuration and effectively disables authentication.

Parameters

authentication-key

Specifies the authentication key. The key can be any combination of ASCII characters up to 255 characters (unencrypted). If spaces are used in the string, enclose the entire string in quotation marks (" ").

hash-key

Specifies the hash key. The key can be any combination of ASCII characters up to 342 characters (encrypted). If spaces are used in the string, enclose the entire string in quotation marks (" ").

This is useful when a user must configure the parameter, but, for security purposes, the actual unencrypted key value is not provided.

hash

Keyword to specify the key is entered in an encrypted form. If the **hash** parameter is not used, the key is assumed to be in a non-encrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** parameter specified.

hash2

Keyword to specify the key is entered in a more complex encrypted form. If the **hash2** parameter is not used, the less encrypted **hash** form is assumed.

auth-keychain

Syntax

auth-keychain *name*

Context

config>service>vprn>bgp

config>service>vprn>bgp>group

config>service>vprn>bgp>group>neighbor

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the BGP authentication key for all peers.

The keychain allows the rollover of authentication keys during the lifetime of a session.

Default

no auth-keychain

Parameters

name

Specifies the name of an existing keychain, up to 32 characters, to use for the specified TCP session or sessions.

connect-retry

Syntax

connect-retry *seconds*

no connect-retry

Context

config>service>vprn>bgp

config>service>vprn>bgp>group

config>service>vprn>bgp>group>neighbor

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the BGP connect retry timer value.

When this timer expires, BGP tries to reconnect to the configured peer. This configuration parameter can be set at three levels: global level (applies to all peers), peer-group level (applies to all peers in group), or neighbor level (only applies to specified peer). The most specific value is used.

The **no** form of this command used at the global level reverts to the default value.

The **no** form of this command used at the group level reverts to the value defined at the global level.

The **no** form of this command used at the neighbor level reverts to the value defined at the group level.

Default

120 seconds

Parameters

seconds

Specifies the BGP connect retry timer value, in seconds, expressed as a decimal integer.

Values 1 to 65535

damping

Syntax

[**no**] **damping**

Context

config>service>vprn>bgp

config>service>vprn>bgp>group

config>service>vprn>bgp>group>neighbor

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables BGP route damping for learned routes that are defined within the route policy. Use damping to reduce the number of update messages sent between BGP peers and reduce the load on peers without affecting the route convergence time for stable routes. Damping parameters are set via route policy definition.

The **no** form of this command used at the global level disables route damping.

The **no** form of this command used at the group level reverts to the value defined at the global level.

The **no** form of this command used at the neighbor level reverts to the value defined at the group level.

When damping is enabled and the route policy does not specify a damping profile, the default damping profile is used. This profile is always present and consists of the following parameters:

Half-life:	15 minutes
Max-suppress:	60 minutes
Suppress-threshold:	3000
Reuse-threshold:	750

Default

no damping

disable-4byte-asn

Syntax

[**no**] **disable-4byte-asn**

Context

config>service>vprn>bgp

config>service>vprn>bgp>group

config>service>vprn>bgp>group>neighbor

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command disables the use of 4-byte ASNs. It can be configured at all 3 level of the hierarchy, so it can be specified down to the per-peer basis.

If this command is enabled 4-byte ASN support should not be negotiated with the associated remote peers.

The **no** form of this command reverts to the default behavior, which is to enable the use of 4-byte ASN.

disable-capability-negotiation

Syntax

[**no**] **disable-capability-negotiation**

Context

config>service>vprn>bgp>group

config>service>vprn>bgp>group>neighbor

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command disables the exchange of capabilities. When this command is enabled and after the peering is flapped, any new capabilities are not negotiated and strictly support IPv4 routing exchanges with that peer.

The **no** form of this command removes this command from the configuration and restores the normal behavior.

Default

no disable-capability-negotiation

disable-capability-negotiation

Syntax

[**no**] **disable-capability-negotiation**

Context

config>service>vprn>bgp

config>service>vprn>bgp>group

config>service>vprn>bgp>group>neighbor

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command disables the exchange of capabilities. When this command is enabled and after the peering is flapped, any new capabilities are not negotiated and strictly support IPv4 routing exchanges with that peer.

The **no** form of this command removes this command from the configuration and restores the normal behavior.

Default

no disable-capability-negotiation

disable-communities

Syntax

disable-communities [**standard**] [**extended**]

no disable-communities

Context

config>service>vprn>bgp

config>service>vprn>bgp>group

config>service>vprn>bgp>group>neighbor

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures BGP to disable sending communities.

Parameters

standard

Keyword to specify standard communities that existed before VPRNs or 2547.

extended

Keyword to specify BGP communities used were expanded after the concept of 2547 was introduced, to include handling the VRF target.

disable-fast-external-failover

Syntax

[**no**] **disable-fast-external-failover**

Context

config>service>vprn>bgp

config>service>vprn>bgp>group

config>service>vprn>bgp>group>neighbor

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures BGP fast external failover.

enable-peer-tracking

Syntax

[**no**] **enable-peer-tracking**

Context

config>service>vprn>bgp

config>service>vprn>bgp>group

config>service>vprn>bgp>group>neighbor

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables BGP peer tracking.

Default

no enable-peer-tracking

export

Syntax

export *policy* [*policy*...]

no export

Context

config>service>vprn>bgp

config>service>vprn>bgp>group

config>service>vprn>bgp>group>neighbor

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command specifies the export policies to control routes advertised to BGP neighbors.

When multiple policy names are specified, the policies are evaluated in the order they are specified. A maximum of five (5) policy names can be configured. The first policy that matches is applied.

If a non-existent route policy is applied to a VPRN instance, the CLI generates a warning message. This message is only generated at an interactive CLI session and the route policy association is made. No warning message is generated when a non-existent route policy is applied to a VPRN instance in a configuration file or when SNMP is used.

The **no** form of this command removes all route policy names from the export list.

Default

no export

Parameters

policy

Specifies the route policy statement name.

family

Syntax

family [**ipv4**] [**ipv6**]

no family

Context

config>service>vprn>bgp

config>service>vprn>bgp>group

config>service>vprn>bgp>group>neighbor

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the IP family capability.

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

Default

no family

Parameters

ipv4

Keyword that provisions IPv4 support.

ipv6

Keyword that provisions IPv6 support.

group

Syntax

group *name* [**dynamic-peer**]

no group

Context

config>service>vprn>bgp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures a BGP peer group.

The **no** form of this command deletes the specified peer group and all configurations associated with the peer group. The group must be shut down before it can be deleted.

Parameters

name

Specifies the peer group name. Allowed values are any string up to 32 characters composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

dynamic-peer

Keyword to specify that the BGP group is used by BGP peers created dynamically based on subscriber-hosts pointing to corresponding BGP peering policy. There can be only one BGP group with this keyword set in any specified VPRN. No BGP neighbors can be manually configured in a BGP group with this keyword set.

Default disabled

neighbor

Syntax

[**no**] **neighbor** *ip-address*

Context

config>service>vprn>bgp>group

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command creates a BGP peer/neighbor instance within the context of the BGP group.

This command can be issued repeatedly to create multiple peers and their associated configuration.

The **no** form of this command is used to remove the specified neighbor and the entire configuration associated with the neighbor. The neighbor must be administratively shut down before attempting to delete it. If the neighbor is not shut down, the command does not result in any action except a warning message on the console indicating that neighbor is still administratively up.

Parameters

ip-address

Specifies the IP address of the BGP peer router in dotted-decimal notation.

Values *ipv4-address*: a.b.c.d

family

Syntax

family [**ipv4**] [**ipv6**]

no family

Context

config>service>vprn>bgp>group

config>service>vprn>bgp>group>neighbor

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command specifies the address family or families to be supported over BGP peerings in the base router. This command is additive so issuing the **family** command adds the specified address family to the list.

The **no** form of this command removes the specified address family from the associated BGP peerings. If an address family is not specified, the supported address family reverts back to the default.

Default

ipv4

Parameters

ipv4

Keyword to provision support for IPv4 routing information.

ipv6

Keyword to provision support for IPv6 routing information.

hold-time

Syntax

hold-time *seconds* [**strict**]

no hold-time

Context

config>service>vprn>bgp

config>service>vprn>bgp>group

config>service>vprn>bgp>group>neighbor

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the BGP hold time, expressed in seconds.

The BGP hold time specifies the maximum time BGP waits between successive messages (either keepalive or update) from its peer, before closing the connection. This configuration parameter can be set at three levels: global level (applies to all peers), group level (applies to all peers in group), or neighbor level (only applies to specified peer). The most specific value is used.

The strict option ensures that the negotiated hold time value is not set to a value less than the configured value.

Even though the 7210 SAS implementation allows setting the time separately, the configured **keepalive** timer is overridden by the **hold-time** value under the following circumstances.

- If the specified **hold-time** value is less than the configured **keepalive** time, the operational **keepalive** time is set to a third of the **hold-time**; the configured **keepalive** time is not changed.
- If the **hold-time** is set to zero, the operational value of the **keepalive** time is set to zero; the configured **keepalive** time is not changed. This means that the connection with the peer is up permanently, and no keepalive packets are sent to the peer.

The **no** form of this command used at the global level reverts to the default value.

The **no** form of this command used at the group level reverts to the value defined at the global level.

The **no** form of this command used at the neighbor level reverts to the value defined at the group level.

Default

90 seconds

Parameters

seconds

Specifies the hold-time, in seconds, expressed as a decimal integer. A value of 0 indicates the connection to the peer is permanently up.

Values 0, 3 to 65535

strict

Keyword to specifies that the advertised BGP hold-time from the far-end BGP peer must be greater than or equal to the specified value.

import

Syntax

import *policy* [*policy*...]

no import

Context

config>service>vprn>bgp

config>service>vprn>bgp>group

config>service>vprn>bgp>group>neighbor

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the import policies to be used to control routes advertised to BGP neighbors. Route policies are configured in the **config>router>policy-options** context. When multiple policy names are specified, the policies are evaluated in the order they are specified. A maximum of five (5) policy names can be specified. The first policy that matches is applied.

The **no** form of this command removes all route policy names from the import list.

Default

no import

Parameters

policy

Specifies a route policy statement name.

keepalive

Syntax

keepalive *seconds*

no keepalive

Context

config>service>vprn>bgp

config>service>vprn>bgp>group

config>service>vprn>bgp>group>neighbor

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the BGP keepalive timer. A keepalive message is sent every time this timer expires.

This command can be set at three levels: global level (applies to all peers), group level (applies to all peers in peer-group), or neighbor level (only applies to specified peer). The most specific value is used.

The **keepalive** value is generally one-third of the interval. Even though the 7210 SAS implementation allows the **keepalive**value and the **hold-time** interval to be independently set, under the following circumstances, the configured **keepalive** value is overridden by the **hold-time** value.

- If the specified **keepalive** value is greater than the configured **hold-time**, the specified value is ignored, and the **keepalive** is set to one third of the current **hold-time** value.
- If the specified **hold-time** interval is less than the configured **keepalive** value, the **keepalive** value is reset to one-third of the specified **hold-time** interval.
- If the **hold-time** interval is set to zero, the configured value of the **keepalive** value is ignored. This means that the connection with the peer is up permanently and no **keepalive** packets are sent to the peer.

The **no** form of this command used at the global level reverts to the default value.

The **no** form of this command used at the group level reverts to the value defined at the global level.

The **no** form of this command used at the neighbor level reverts to the value defined at the group level.

Default

30 seconds

Parameters

seconds

Specifies the keepalive timer in seconds, expressed as a decimal integer.

Values 0 to 21845

local-address

Syntax

local-address *ip-address*

no local-address

Context

config>service>vprn>bgp>group

config>service>vprn>bgp>group>neighbor

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the local IP address used by the group or neighbor when communicating with BGP peers.

Outgoing connections use the **local-address** as the source of the TCP connection when initiating connections with a peer.

When a local address is not specified, the 7210 SAS uses the system IP address when communicating with iBGP peers and uses the interface address for directly connected eBGP peers. This command is used at the neighbor level to revert to the value defined under the group level.

The router ID is used when communicating with iBGP peers and the interface address is used for directly connected eBGP peers.

The **no** form of this command removes the configured **local-address** for BGP.

The **no** form of this command used at the group level reverts to the value defined at the global level.

The **no** form of this command used at the neighbor level reverts to the value defined at the group level.

Default

no local-address

Parameters

ip-address

Specifies the local address, expressed in dotted-decimal notation. Allowed values are a valid routable IP address on the router, either an interface or system IP address.

local-as

Syntax

local-as *as-number* [**private**]

no local-as

Context

config>service>vprn>bgp

config>service>vprn>bgp>group

config>service>vprn>bgp>group>neighbor

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures a BGP virtual autonomous system (AS) number.

In addition to the AS number configured for BGP in the **config>router>autonomous-system** context, a virtual (local) AS number is configured.The virtual AS number is added to the as-path message before the router AS number makes the virtual AS the second AS in the as-path.

This configuration parameter can be set at three levels: global level (applies to all peers), group level (applies to all peers in peer-group), or neighbor level (only applies to specified peer). Therefore, by specifying this at each neighbor level, it is possible to have a separate AS number per eBGP session.

When a command is entered multiple times for the same AS, the last command entered is used in the configuration. The **private** keyword can be added or removed dynamically by reissuing the command.

Changing the local AS at the global level in an active BGP instance causes the BGP instance to restart with the new local AS number. Changing the local AS at the global level in an active BGP instance causes BGP to reestablish the peer relationships with all peers in the group with the new local AS number. Changing the local AS at the neighbor level in an active BGP instance causes BGP to reestablish the peer relationship with the new local AS number.

This is an optional command and can be used in the following example.

Example: Provider router P is moved from AS1 to AS2. The customer router that is connected to P, however, is configured to belong to AS1. To avoid reconfiguring the customer router, the **local-as** value on router P can be set to AS1. Therefore, router P adds AS1 to the as-path message for routes it advertises to the customer router.

The **no** form of this command used at the global level will remove any virtual AS number configured.

The **no** form of this command used at the group level reverts to the value defined at the global level.

The **no** form of this command used at the neighbor level reverts to the value defined at the group level.

Default

no local-as

Parameters

as-number

Specifies the virtual AS number, expressed as a decimal integer.

Values 1 to 65535

private

Specifies that the local AS is hidden in paths learned from the peering.

local-preference

Syntax

local-preference *local-preference*

no local-preference

Context

config>service>vprn>bgp

config>service>vprn>bgp>group

config>service>vprn>bgp>group>neighbor

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the default value of the BGP local preference attribute if it is not already specified in incoming routes. This value is used if the BGP route arrives from a BGP peer without the **local-preference** integer set.

The specified value can be overridden by any value set via a route policy. This configuration parameter can be set at three levels: global level (applies to all peers), group level (applies to all peers in peer-group), or neighbor level (only applies to specified peer). The most specific value is used.

The **no** form of this command at the global level specifies that incoming routes with local preference set are not overridden, and routes arriving without local preference set are interpreted as if the route had a local preference value of 100.

The **no** form of this command used at the group level reverts to the value defined at the global level.

The **no** form of this command used at the neighbor level reverts to the value defined at the group level.

Default

no local-preference

Parameters

local-preference

Specifies the local preference value to be used as the override value, expressed as a decimal integer.

Values 0 to 4294967295

loop-detect

Syntax

loop-detect {**drop-peer** | **discard-route** | **ignore-loop** | **off**}

no loop-detect

Context

config>service>vprn>bgp

config>service>vprn>bgp>group

config>service>vprn>bgp>group>neighbor

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures how the BGP peer session handles loop detection in the AS path.

This configuration parameter can be set at three levels: global level (applies to all peers), group level (applies to all peers in peer-group), or neighbor level (only applies to specified peer). The most specific value is used.

Dynamic configuration changes of **loop-detect** are not recognized.

The **no** form of this command used at the global level reverts to default, which is **loop-detect ignore-loop**.

The **no** form of this command used at the group level reverts to the value defined at the global level.

The **no** form of this command used at the neighbor level reverts to the value defined at the group level.

Default

loop-detect ignore-loop

Parameters

drop-peer

Keyword that specifies to send a notification to the remote peer and drops the session.

discard-route

Keyword that specifies to discard routes received with loops in the AS path.

ignore-loop

Keyword that specifies to ignore routes with loops in the AS path but maintain peering.

off

Keyword that disables loop detection.

med-out

Syntax

med-out [*number* | **igp-cost**]

no med-out

Context

config>service>vprn>bgp

config>service>vprn>bgp>group

config>service>vprn>bgp>group>neighbor

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures advertising the Multi-Exit Discriminator (MED) and assigns the value used for the path attribute for the MED advertised to BGP peers if the MED is not already set.

The specified value can be overridden by any value set via a route policy.

This configuration parameter can be set at three levels: global level (applies to all peers), group level (applies to all peers in peer-group), or neighbor level (only applies to specified peer). The most specific value is used.

The **no** form of this command used at the global level reverts to default where the MED is not advertised.

The **no** form of this command used at the group level reverts to the value defined at the global level.

The **no** form of this command used at the neighbor level reverts to the value defined at the group level.

Default

no med-out

Parameters

number

Specifies the MED path attribute value, expressed as a decimal integer.

Values 0 to 4294967295

igp-cost

Keyword to specify that the MED is set to the IGP cost of the specified IP prefix.

min-as-origination

Syntax

min-as-origination *seconds*

no min-as-origination

Context

config>service>vprn>bgp

config>service>vprn>bgp>group

config>service>vprn>bgp>group>neighbor

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the minimum interval, in seconds, at which a path attribute, originated by the local router, can be advertised to a peer.

This configuration parameter can be set at three levels: global level (applies to all peers), group level (applies to all peers in peer-group), or neighbor level (only applies to specified peer). The most specific value is used.

The **no** form of this command used at the global level reverts to default.

The **no** form of this command used at the group level reverts to the value defined at the global level.

The **no** form of this command used at the neighbor level reverts to the value defined at the group level.

Default

15 seconds

Parameters

seconds

Specifies the minimum path attribute advertising interval in seconds, expressed as a decimal integer.

Values 2 to 255

min-route-advertisement

Syntax

min-route-advertisement *seconds*

no min-route-advertisement

Context

config>service>vprn>bgp

config>service>vprn>bgp>group

config>service>vprn>bgp>group>neighbor

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the minimum interval, in seconds, at which a prefix can be advertised to a peer.

This configuration parameter can be set at three levels: global level (applies to all peers), group level (applies to all peers in peer-group), or neighbor level (only applies to specified peer). The most specific value is used.

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

Default

30 seconds

Parameters

seconds

Specifies the minimum route advertising interval, in seconds, expressed as a decimal integer.

Values 1 to 255

multihop

Syntax

multihop *ttl-value*

no multihop

Context

config>service>vprn>bgp

config>service>vprn>bgp>group

config>service>vprn>bgp>group>neighbor

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the time to live (TTL) value entered in the IP header of packets sent to an eBGP peer that is multiple hops away.

This parameter is meaningful only when configuring eBGP peers. It is ignored if set for an iBGP peer.

The **no** form of this command is used to convey to the BGP instance that the eBGP peers are directly connected.

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

Default

1 — eBGP peers are directly connected.

64 — iBGP

Parameters

ttl-value

Specifies the TTL value, expressed as a decimal integer.

Values 1 to 255

next-hop-self

Syntax

[**no**] **next-hop-self**

Context

config>service>vprn>bgp>group

config>service>vprn>bgp>group>neighbor

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the group or neighbor to always set the next-hop path attribute to its own physical interface when advertising to a peer.

This command is primarily used to avoid third-party route advertisements when connected to a multi-access network.

The **no** form of this command used at the group level allows third-party route advertisements in a multi-access network.

The **no** form of this command used at the neighbor level reverts to the value defined at the group level.

Default

no next-hop-self

peer-as

Syntax

peer-as *as-number*

Context

config>service>vprn>bgp>group

config>service>vprn>bgp>group>neighbor

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the AS number for the remote peer. The peer AS number must be configured for each configured peer.

For eBGP peers, the peer AS number configured must be different from the autonomous system number configured for this router under the global level, because the peer is in a different autonomous system than that of this router

For iBGP peers, the peer AS number must be the same as the AS number of this router configured under the global level.

This is a required command for each configured peer. This may be configured under the group level for all neighbors in a specific group.

Parameters

as-number

Specified the autonomous system number, expressed as a decimal integer.

Values 1 to 65535

preference

Syntax

[**no**] **preference** *preference*

Context

config>service>vprn>bgp

config>service>vprn>bgp>group

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the route preference for routes learned from the configured peers.

This configuration parameter can be set at three levels: global level (applies to all peers), group level (applies to all peers in peer-group), or neighbor level (only applies to specified peer). The most specific value is used.

The lower the preference, the higher the chance of the route being the active route. The 7210 SAS assigns the highest default preference to BGP routes, as compared to routes that are direct, static, or learned via MPLS or OSPF.

The **no** form of this command used at the global level reverts to default value.

The **no** form of this command used at the group level reverts to the value defined at the global level.

The **no** form of this command used at the neighbor level reverts to the value defined at the group level.

Default

170

Parameters

preference

Specifies the route preference, expressed as a decimal integer.

Values 1 to 255

path-mtu-discovery

Syntax

[**no**] **path-mtu-discovery**

Context

config>router>bgp

config>router>bgp>group

config>router>bgp>group>neighbor

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures path MTU discovery for the associated TCP connections.

The MTU for the associated TCP session is initially set to the egress interface MTU. The DF bit is also set so that if a router along the path of the TCP connection cannot handle a packet of a particular size without fragmenting, the router sends back an ICMP message to set the path MTU for the specified session to a lower value that can be forwarded without fragmenting.

The **no** form of this command disables path MTU discovery.

Default

no path-mtu-discovery

prefix-limit

Syntax

prefix-limit *limit* [**log-only**] [**threshold** *percent*]

no prefix-limit

Context

config>service>vprn>bgp>group

config>service>vprn>bgp>group>neighbor

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the maximum number of routes BGP can learn from a peer.

When the number of routes reaches the specified percentage (the default is 90% of this limit), an SNMP trap is sent. When the limit is exceeded, BGP peering is dropped and disabled.

The **no** form of this command removes the **prefix-limit**.

Default

no prefix-limit

Parameters

limit

Specifies the number of routes that can be learned from a peer, expressed as a decimal integer.

Values 1 to 4294967295

log-only

Keyword that enables the warning message to be sent at the specified threshold percentage and also when the limit is exceeded; however, the BGP peering is not dropped.

threshold *percent*

Specifies the threshold value (as a percentage) that triggers a warning message to be sent.

Default 90%

rapid-withdrawal

Syntax

[**no**] **rapid-withdrawal**

Context

config>service>vprn>bgp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command disables the delay (Minimum Route Advertisement) on sending BGP withdrawals. Normal route withdrawals may be delayed up to the minimum route advertisement to allow for efficient packing of BGP updates.

The **no** form of this command removes this command from the configuration and reverts withdrawal processing to the default behavior.

Default

no rapid-withdrawal

remove-private

Syntax

[**no**] **remove-private**

Context

config>service>vprn>bgp

config>service>vprn>bgp>group

config>service>vprn>bgp>group>neighbor

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command allows private AS numbers to be removed from the AS path before advertising them to BGP peers.

When the **remove-private** parameter is set at the global level, it applies to all peers regardless of group or neighbor configuration. When the parameter is set at the group level, it applies to all peers in the group regardless of the neighbor configuration.

The 7210 SAS recognizes the set of AS numbers that are defined by IANA as private. These are AS numbers in the range 64512 through 65535, inclusive.

The **no** form of this command used at the global level reverts to the default value.

The **no** form of this command used at the group level reverts to the value defined at the global level.

The **no** form of this command used at the neighbor level reverts to the value defined at the group level.

Default

no remove-private

type

Syntax

[**no**] **type** {**internal** | **external**}

Context

config>service>vprn>bgp>group

config>service>vprn>bgp>group>neighbor

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the BGP peer as an internal or external type.

The **internal** type indicates the peer is an iBGP peer; the **external** type indicates that the peer is an eBGP peer.

By default, the 7210 SAS derives the type of neighbor based on the local AS specified. If the local AS specified is the same as the AS of the router, the peer is considered **internal**. If the local AS is different, the peer is considered **external**.

The **no** form of this command used at the group level reverts to the default value.

The **no** form of this command used at the neighbor level reverts to the value defined at the group level.

Default

no type

Parameters

internal

Keyword that configures the peer as internal.

external

Keyword that configures the peer as external.

ttl-security

Syntax

ttl-security *min-ttl-value*

no ttl-security

Context

config>service>vprn>bgp>group

config>service>vprn>bgp>group>neighbor

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures TTL security parameters for incoming packets.

The **no** form of this command disables TTL security.

Parameters

min-ttl-value

Specifies the minimum TTL value for an incoming BGP packet.

Values 1 to 255

Default 1

7.4.2.1.15 OSPF commands

ospf

Syntax

[**no**] **ospf**

Context

config>service>vprn

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

Commands in this context configure OSPF parameters for VPRN.

When an OSPF instance is created, the protocol is enabled. To start or suspend execution of the OSPF protocol without affecting the configuration, use the **no shutdown** command.

The **no** form of this command deletes the OSPF protocol instance and removes all associated configuration parameters.

Default

no ospf

area

Syntax

[**no**] **area** *area-id*

Context

config>service>vprn>ospf

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures an OSPF area. An area is a collection of network segments within an AS that have been administratively grouped together. The area ID can be specified in dotted-decimal notation or as a 32-bit decimal integer.

The **no** form of this command deletes the specified area from the configuration. Deleting the area also removes the OSPF configuration of all the interfaces, virtual-links, sham-links, address-ranges, and so on, that are currently assigned to this area.

Default

no area

Parameters

area-id

Specifies the OSPF area ID expressed in dotted-decimal notation or as a 32-bit decimal integer.

Values 0.0.0.0 to 255.255.255.255 (dotted-decimal)

0 to 4294967295 (decimal integer)

area-range

Syntax

area-range *ip-prefix/prefix-length* [**advertise** | **not-advertise**]

no area-range *ip-prefixlmask*

no area-range *ip-prefixlmask*

Context

config>service>vprn>ospf>area

ospf>service>vprn>nssa

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command creates ranges of addresses on an Area Border Router (ABR) for the purpose of route summarization or suppression. When created, a range is configured to be advertised or not advertised into other areas. Multiple range commands may be used to summarize or hide different ranges. In the case of overlapping ranges, the most specific range command applies.

ABRs send summary link advertisements to describe routes to other areas. To minimize the number of advertisements that are flooded, you can summarize a range of IP addresses and send reachability information about these addresses in an LSA.

The **no** form of this command deletes the range advertisement or non-advertisement.

Default

no area-range

Special Cases

NSSA Context

In the NSSA context, the option specifies that the range applies to external routes (via type-7 LSAs) learned within the NSSA when the routes are advertised to other areas as type-5 LSAs.

Area Context

If this command is not entered under the NSSA context, the range applies to summary LSAs even if the area is an NSSA.

Parameters

ipv6-prefix/prefix-length

Specifies the IP prefix in dotted-decimal notation for the range used by the ABR to advertise the area into another area.

Values *ipv6-prefix*: x:x:x:x:x:x:x:x (eight 16-bit pieces)

x:x:x:x:x:x:d.d.d.d

x: [0 to FFFF]H

d: [0 to 255]D

prefix-length: 0 to 128

mask

Specifies the subnet mask for the range expressed as a decimal integer mask length or in dotted-decimal notation.

Values 0 to 32 (mask length)

0.0.0.0 to 255.255.255.255 (dotted-decimal)

advertise | not-advertise

Keywords that specify whether to advertise the summarized range of addresses to other areas.

Default advertise

blackhole-aggregate

Syntax

[**no**] **blackhole-aggregate**

Context

config>service>vprn>ospf>area

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command installs a low priority blackhole route for the entire aggregate. Existing routes that make up the aggregate have a higher priority and only the components of the range for which no route exists are blackholed.

When performing area aggregation, addresses may be included in the range for which no actual route exists. This can cause routing loops. To avoid this problem, configure the blackhole aggregate option.

The **no** form of this command removes this option.

Default

blackhole-aggregate

interface

Syntax

[**no**] **interface** *ip-int-name* [**secondary**]

Context

config>service>vprn>ospf>area

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures an OSPF interface.

By default, interfaces are not activated in any interior gateway protocol, such as OSPF, unless explicitly configured.

The **no** form of this command deletes the OSPF interface configuration for this interface. The **shutdown** command in the **config>router>ospf>interface** context can be used to disable an interface without removing the configuration for the interface.

Default

no interface

Parameters

ip-int-name

Specifies the IP interface name. Interface names must be unique within the group of defined IP interfaces for **config router interface** and **config service vprn interface** commands. An interface name cannot be in the form of an IP address. Interface names can be any string up to 32 characters composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

If the IP interface name does not exist or does not have an IP address configured, an error message is returned.

If the IP interface exists in a different area, it is moved to this area.

secondary

Keyword that allows multiple secondary adjacencies to be established over a single IP interface.

sham-link

Syntax

sham-link *ip-int-name ip-address*

Context

config>service>vprn>ospf>area

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command is similar to a virtual link with the exception that metric must be included to distinguish the cost between the MPLS-VPRN link and the backdoor.

Parameters

ip-int-name

Specifies the local interface name used for the sham-link. This is a mandatory parameter and interface names must be unique within the group of defined IP interfaces for **config router interface**, **config service ies interface**, and **config service vprn interface** commands. An interface name cannot be in the form of an IP address. Interface names can be any string up to 32 characters composed of printable, 7-bit ASCII characters. If the string contains special characters, the entire string must be enclosed within double quotes. If the IP interface name does not exist or does not have an IP address configured, an error message will be returned.

ip-address

Specifies the IP address of the sham-link neighbor in IP address dotted-decimal notation. This parameter is the remote peer of the sham-link IP address used to set up the sham link. This is a mandatory parameter and must be a valid IP address.

advertise-subnet

Syntax

[**no**] **advertise-subnet**

Context

config>service>vprn>ospf>area>if

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables advertising point-to-point interfaces as subnet routes (network number and mask). When disabled, point-to-point interfaces are advertised as host routes.

The **no** form of this command disables advertising point-to-point interfaces as subnet routes, meaning they are advertised as host routes.

Default

advertise-subnet

authentication-key

Syntax

authentication-key [*authentication-key* | *hash-key*] [**hash** | **hash2**]

no authentication-key

Context

config>service>vprn>ospf>area>if

config>service>vprn>ospf>area>virtual-link

config>service>vprn>ospf>area>sham-link

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the password used by the OSPF interface or virtual-link to send and receive OSPF protocol packets on the interface when simple password authentication is configured.

All neighboring routers must use the same type of authentication and password for correct protocol communication. If the **authentication-type** is configured as password, this key must be configured.

By default, no authentication key is configured.

The **no** form of this command removes the authentication key.

Default

no authentication-key

Parameters

authentication-key

Specifies the authentication key. The key can be any combination of ASCII characters up to 8 characters (unencrypted). If spaces are used in the string, enclose the entire string in quotation marks (" ").

hash-key

Specifies the hash key. The key can be any combination of ASCII characters up to 22 characters (encrypted). If spaces are used in the string, enclose the entire string in quotation marks (" ").

This is useful when a user must configure the parameter, but, for security purposes, the actual unencrypted key value is not provided.

hash

Keyword that specifies the key is entered in an encrypted form. If the **hash** parameter is not used, the key is assumed to be in a non-encrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** parameter specified.

hash2

Keyword that specifies the key is entered in a more complex encrypted form. If the **hash2** parameter is not used, the less encrypted **hash** form is assumed.

authentication-type

Syntax

authentication-type {**password** | **message-digest**}

no authentication-type

Context

config>service>vprn>ospf>area>if

config>service>vprn>ospf>area>virtual-link

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables authentication and specifies the type of authentication to be used on the OSPF interface, virtual-link, and sham-link.

Both simple **password** and **message-digest** authentication are supported.

By default, authentication is not enabled on an interface.

The **no** form of this command disables authentication on the interface.

Default

no authentication

Parameters

password

Keyword that enables simple password (plain text) authentication. If authentication is enabled and no authentication type is specified in the command, simple password authentication is enabled.

message-digest

Keyword that enables message digest MD5 authentication in accordance with RFC1321. If this option is configured, at least one message-digest-key must be configured.

bfd-enable

Syntax

bfd-enable [**remain-down-on-failure**]

no bfd-enable

Context

config>service>vprn>ospf>area>if

config>service>vprn>ospf>area>virtual-link

config>service>vprn>ospf>area>sham-link

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables the use of bidirectional forwarding (BFD) to control the state of the associated protocol interface. By enabling BFD on a specific protocol interface, the state of the protocol interface is tied to the state of the BFD session between the local node and the remote node. The parameters used for the BFD are set using the BFD command under the IP interface.

Note:

- BFD is not supported for IPv6 interfaces.
- See the *7210 SAS-Mxp, R6, R12, S, Sx, T Router Configuration Guide* for more information about the protocols and platforms that support BFD.

The **no** form of this command removes BFD from the associated IGP protocol adjacency.

Default

no bfd-enable

Parameters

remain-down-on-failure

Keyword that forces adjacency down on BFD failure.

dead-interval

Syntax

dead-interval *seconds*

no dead-interval

Context

config>service>vprn>ospf>area>if

config>service>vprn>ospf>area>virtual-link

config>service>vprn>ospf>area>sham-link

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the time, in seconds, that OSPF waits before declaring a neighbor router down. If no hello packets are received from a neighbor for the duration of the dead interval, the router is assumed to be down. The minimum interval must be two times the hello interval.

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

Default

40

Special Cases

OSPF Interface

If the **dead-interval** configured applies to an interface, all nodes on the subnet must have the same dead interval.

Virtual Like

If the **dead-interval** configured applies to a virtual link, the interval on both termination points of the virtual link must have the same dead interval.

Sham-link

If the **dead-interval** configured applies to a sham-link, the interval on both endpoints of the sham-link must have the same dead interval.

Parameters

seconds

Specifies the dead interval in seconds, expressed as a decimal integer.

Values 2 to 2147483647 seconds

hello-interval

Syntax

hello-interval *seconds*

no hello-interval

Context

config>service>vprn>ospf>area>if

config>service>vprn>ospf>area>virtual-link

config>service>vprn>ospf>area>sham-link

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the interval between OSPF hellos issued on the interface, virtual link, or sham-link.

The **hello-interval**, in combination with the **dead-interval**, is used to establish and maintain the adjacency. Use this parameter to edit the frequency that hello packets are sent.

Reducing the interval, in combination with a corresponding reduction in the associated **dead-interval**, allows for faster detection of link or router failures at the cost of higher processing costs.

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

Default

hello-interval 10

Special Cases

OSPF Interface

If the **hello-interval** configured applies to an interface, all nodes on the subnet must have the same hello interval.

Virtual Link

If the **hello-interval** configured applies to a virtual link, the interval on both termination points of the virtual link must have the same hello interval.

Sham Link

If the **hello-interval** configured applies to a sham-link, the interval on both endpoints of the sham-link must have the same hello interval

Parameters

seconds

Specifies the hello interval in seconds, expressed as a decimal integer.

Values 1 to 65535

interface-type

Syntax

interface-type {**broadcast** | **point-to-point**}

no interface-type

Context

config>service>vprn>ospf>area>if

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the interface type to be either broadcast or point-to-point.

Use this command to set the interface type of an Ethernet link to point-to-point to avoid having to carry the broadcast adjacency maintenance overhead if the Ethernet link, provided the link is used as a point-to-point link.

If the interface type is not known at the time the interface is added to OSPF, and the subsequent IP interface is bound (or moved) to a different interface type, this command must be entered manually.

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

Default

point-to-point — If the physical interface is SONET.

broadcast — If the physical interface is Ethernet or unknown.

Special Cases

Virtual-Link

A virtual link is always regarded as a point-to-point interface and is not configurable.

Parameters

broadcast

Keyword that configures the interface to maintain this link as a broadcast network. To significantly improve adjacency forming and network convergence, a network should be configured as point-to-point if only two routers are connected, even if the network is a broadcast media such as Ethernet.

point-to-point

Keyword that configures the interface to maintain this link as a point-to-point link.

message-digest-key

Syntax

message-digest-key *keyid* **md5** [*key* | *hash-key*] [**hash**]

no message-digest-key *keyid*

Context

config>service>vprn>ospf>area>if

config>service>vprn>ospf>area>virtual-link

config>service>vprn>ospf>area>sham-link

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures a message digest key when MD5 authentication is enabled on the interface, virtual-link, or sham-link. Multiple message digest keys can be configured. By default, no message digest keys are defined.

The **no** form of this command removes the message digest key identified by the *key-id*.

Parameters

keyid

Specifies the key ID, expressed as a decimal integer.

Values 1 to 255

md5 ***key***

Specifies the MD5 key. The key can be any alphanumeric string up to 16 characters.

md5 ***hash-key***

Specifies the MD5 hash key. The key can be any combination of ASCII characters up to 32 characters (encrypted). If spaces are used in the string, enclose the entire string in quotation marks (" ").

This is useful when a user must configure the parameter, but, for security purposes, the actual unencrypted key value is not provided.

hash

Keyword to specify that the key is entered in an encrypted form. If the **hash** parameter is not used, the key is assumed to be in a non-encrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file, with the **hash** parameter specified.

metric

Syntax

metric *metric*

no metric

Context

config>service>vprn>ospf>area>if

config>service>vprn>ospf>area>sham-link

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures an explicit route cost metric for the OSPF interface that overrides the metrics calculated based on the speed of the underlying link.

The **no** form of this command deletes the manually configured interface metric, so the interface uses the computed metric based on the **reference-bandwidth** command setting and the speed of the underlying link.

Default

no metric

Parameters

metric

Specifies the metric to be applied to the interface, expressed as a decimal integer.

Values 1 to 65535

mtu

Syntax

mtu *bytes*

no mtu

Context

config>service>vprn>ospf>area>if

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the OSPF packet size used on the interface.

If this command is not configured, OSPF derives the MTU value from the MTU configured (default or explicitly) in the **config>port>ethernet** context.

If this parameter is configured, the smaller value between the value configured here and the MTU configured (default or explicitly) in a previously mentioned context is used.

To determine the actual packet size, add 14 bytes for an Ethernet packet and 18 bytes for a tagged Ethernet packet to the size of the OSPF (IP) packet MTU configured using this command.

The **no** form of this command reverts to default value.

Default

no mtu

Parameters

bytes

Specifies the MTU to be used by OSPF for this logical interface in bytes.

Values 512 to 9198 (9212 – 14) (depends on the physical media)

passive

Syntax

[**no**] **passive**

Context

config>service>vprn>ospf>area>if

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command adds the passive property to an OSPF interface.

By default, only interface addresses that are configured for OSPF are advertised as OSPF interfaces. The **passive** command allows an interface to be advertised as an OSPF interface without running the OSPF protocol.

While in passive mode, the interface ignores ingress OSPF protocol packets and does not transmit any OSPF protocol packets.

Service interfaces defined in the **config>router>service-prefix** context are passive. All other interfaces are not passive.

The **no** form of this command removes the passive property from the OSPF interface.

priority

Syntax

priority *number*

no priority

Context

config>service>vprn>ospf>area>if

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the priority of the OSPF interface that is used in an election of the designated router on the subnet.

This command is used only when the interface is of type broadcast. The router with the highest priority interface becomes the designated router. A router with priority 0 is not eligible to be a designated router or backup designated router.

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

Default

priority 1

Parameters

number

Specifies the interface priority expressed as a decimal integer. A value of 0 indicates the router is not eligible to be the designated router or backup designated router on the interface subnet.

Values 0 to 255

retransmit-interval

Syntax

retransmit-interval *seconds*

no retransmit-interval

Context

config>service>vprn>ospf>area>if

config>service>vprn>ospf>area>virtual-link

config>service>vprn>ospf>area>sham-link

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command specifies the length of time, in seconds, that OSPF waits before retransmitting an unacknowledged Link State Advertisement (LSA) to an OSPF neighbor.

The value should be longer than the expected round trip delay between any two routers on the attached network. When the retransmit interval expires and no acknowledgment has been received, the LSA isretransmitted.

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

Default

retransmit-interval 5

Parameters

seconds

Specifies the retransmit interval in seconds, expressed as a decimal integer.

Values 1 to 3600

transit-delay

Syntax

transit-delay *seconds*

no transit-delay

Context

config>service>vprn>ospf>area>if

config>service>vprn>ospf>area>virtual-link

config>service>vprn>ospf>area>sham-link

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the estimated time, in seconds, that it takes to transmit an LSA on the interface, virtual link, or sham-link.

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

Default

transit-delay 1

Parameters

seconds

Specifies the transit delay in seconds, expressed as a decimal integer.

Values 0 to 3600

nssa

Syntax

[**no**] **nssa**

Context

config>service>vprn>ospf>area

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures an OSPF Not So Stubby Area (NSSA) and adds or removes the NSSA designation from the area.

NSSAs are similar to stub areas in that no external routes are imported into the area from other OSPF areas. The major difference between a stub area and an NSSA is an NSSA has the capability to flood external routes that it learns throughout its area and via an ABR to the entire OSPF domain.

Existing virtual links of a non-stub or NSSA area are removed when the designation is changed to NSSA or stub.

An area can be designated as stub or NSSA but never both at the same time.

By default, an area is not configured as an NSSA area.

The **no** form of this command removes the NSSA designation and configuration context from the area.

Default

no nssa

originate-default-route

Syntax

originate-default-route [**type-7**]

no originate-default-route

Context

config>service>vprn>ospf>area>nssa

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables the generation of a default route and its LSA type (3 or 7) into an NSSA by an NSSA Area Border Router (ABR).

When configuring an NSSA with no summaries, the ABR injects a type-3 LSA default route into the NSSA area. Some older implementations expect a type-7 LSA default route.

The **no** form of this command disables origination of a default route.

Default

no originate-default-route

Parameters

type-7

Keyword that specifies a type-7 LSA should be used for the default route.

Configure this parameter to inject a type-7 LSA default route instead of the type-3 LSA into the NSSA configured with no summaries. To revert to a type-3 LSA, enter **originate-default-route** without the **type-7** parameter.

Default type 3 LSA for the default route

redistribute-external

Syntax

[**no**] **redistribute-external**

Context

config>service>vprn>ospf>area>nssa

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables the redistribution of external routes into the NSSA or an NSSA ABR that is exporting the routes into non-NSSA areas.

NSSAs are similar to stub areas in that no external routes are imported into the area from other OSPF areas. The major difference between a stub area and an NSSA is that the NSSA has the capability to flood external routes that it learns (providing it is an ASBR) throughout its area and via an ABR to the entire OSPF domain.

The **no** form of this command disables the default behavior to automatically redistribute external routes into the NSSA area from the NSSA ABR.

Default

redistribute-external

summaries

Syntax

[**no**] **summaries**

Context

config>service>vprn>ospf>area>nssa

config>service>vprn>ospf>area>stub

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables sending summary (type-3) advertisements into a stub area or NSSA on an ABR.

This command is particularly useful to reduce the size of the routing and Link State Database (LSDB) tables within the stub or nssa area. By default, summary route advertisements are sent into the stub area or NSSA.

The **no** form of this command disables sending summary route advertisements and, for stub areas, only the default route is advertised by the ABR.

Default

summaries

stub

Syntax

[**no**] **stub**

Context

config>service>vprn>ospf>area

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures an OSPF stub area and adds or removes the stub designation from the area.

External routing information is not flooded into stub areas. All routers in the stub area must be configured with the **stub** command. An OSPF area cannot be both an NSSA and a stub area. Existing virtual links of a non-stub area or NSSA are removed when its designation is changed to NSSA or stub.

By default, an area is not a stub area.

The **no** form of this command removes the stub designation and configuration context from the area.

Default

no stub

default-metric

Syntax

default-metric *metric*

no default-metric

Context

config>service>vprn>ospf>area>stub

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the metric used by the ABR for the default route into a stub area.

The default metric should be configured only on an ABR of a stub area. An ABR generates a default route if the area is a stub area.

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

Default

default-metric 1

Parameters

metric

Specifies the metric, expressed as a decimal integer, for the default route cost to be advertised into the stub area.

Values 1 to 16777215

virtual-link

Syntax

[**no**] **virtual-link** *router-id* **transit-area** *area-id*

Context

config>service>vprn>ospf>area

Platforms

Supported on all 7210 SAS platforms as described in this document

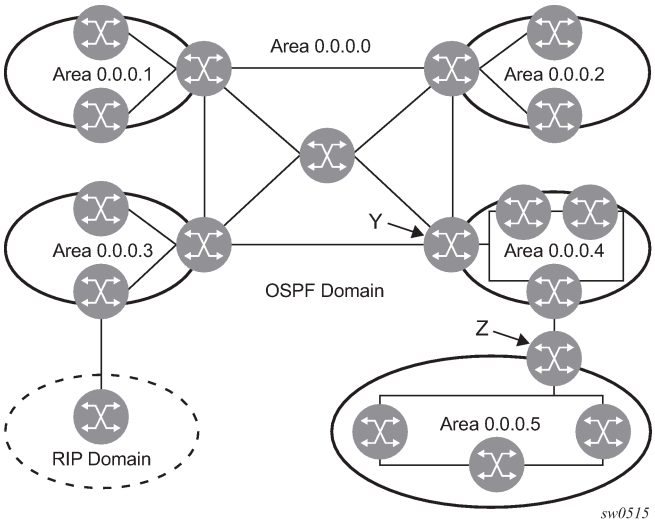
Description

This command configures a virtual link to connect ABRs to the backbone.

The backbone area (area 0.0.0.0) must be contiguous and all other areas must be connected to the backbone area. If it is not practical to connect an area to the backbone (see area 0.0.0.2 in Figure 79: OSPF areas), the area border routers (routers 1 and 2 in Figure 79: OSPF areas) must be connected via a virtual link. The two area border routers form a point-to-point like adjacency across the transit area (area 0.0.0.1 in Figure 79: OSPF areas). A virtual link can be configured only while in the area 0.0.0.0 context.

The OSPF backbone area, area 0.0.0.0, must be contiguous and all other areas must be connected to the backbone area. The backbone distributes routing information between areas. If it is not practical to connect an area to the backbone (see area 0.0.0.5 in the following figure), the area border routers (such as routers Y and Z) must be connected via a virtual link. The two area border routers form a point-to-point-like adjacency across the transit area (see area 0.0.0.4).

Figure 79: OSPF areas



The *router-id* specified in this command must be associated with the virtual neighbor. The transit area cannot be a stub area or an NSSA.

The **no** form of this command deletes the virtual link.

Parameters

router-id

Specifies the router ID of the virtual neighbor, in IP address dotted-decimal notation.

transit-area *area-id*

Specifies the area ID for the transit area that links the backbone area with the area that has no physical connection with the backbone.

compatible-rfc1583

Syntax

[**no**] **compatible-rfc1583**

Context

config>service>vprn>ospf

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables OSPF summary and external route calculations in compliance with RFC1583 and earlier RFCs.

RFC1583 and earlier RFCs use a different method to calculate summary and external route costs. To avoid routing loops, all routers in an OSPF domain should perform the same calculation method.

Although it would be favorable to require all routers to run a more current compliance level, this command allows the router to use obsolete methods of calculation.

The **no** form of this command enables the post-RFC1583 method of summary and external route calculation.

Default

compatible-rfc1583

export

Syntax

export *policy-name* [*policy-name…*]

no export

Context

config>service>vprn>ospf

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command associates export route policies to determine which routes are exported from the route table to OSPF. Export polices are in effect only if OSPF is configured as an ASBR.

If no export policy is specified, non-OSPF routes are not exported from the routing table manager to OSPF.

If multiple policy names are specified, the policies are evaluated in the order they are specified. The first policy that matches is applied. If multiple export commands are issued, the last command entered overrides the previous command. A maximum of five policy names can be specified. The specified names must already be defined.

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

Default

no export

Parameters

policy-name

The export route policy name. Allowed values are any string up to 32 characters composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

external-db-overflow

Syntax

external-db-overflow *limit seconds*

no external-db-overflow

Context

config>service>vprn>ospf

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures limits on the number of non-default AS-external LSA entries that can be stored in the link-state database (LSDB) and specifies a wait timer before processing these after the limit is exceeded.

The *limit* value specifies the maximum number of non-default AS-external LSA entries that can be stored in the LSDB. Placing a limit on the non-default AS-external LSAs in the LSDB protects the router from receiving an excessive number of external routes that consume excessive memory or CPU resources. If the number of routes reach or exceed the *limit*, the table is in an overflow state. When in an overflow state, the router will not originate any new AS-external LSAs and withdraws all the self-originated non-default external LSAs.

The *seconds* value specifies the amount of time to wait after an overflow state before regenerating and processing non-default, AS-external LSAs. The waiting period acts like a dampening period, preventing the router from continuously running shortest path first (SPF) calculations caused by the excessive number of non-default, AS-external LSAs.

The **external-db-overflow** command must be set identically on all routers attached to any regular OSPF area. OSPF stub areas and NSSAs are excluded.

The **no** form of this command disables limiting the number of non-default, AS-external LSA entries.

Default

no external-db-overflow

Parameters

limit

Specifies the maximum number of non-default, AS-external LSA entries that can be stored in the LSDB before going into an overflow state, expressed as a decimal integer.

Values 1 to 2147483647

seconds

Specifies the number of seconds after entering an overflow state before attempting to process non-default AS-external LSAs, expressed as a decimal integer.

Values 0 to 2147483647

external-preference

Syntax

external-preference *preference*

no external-preference

Context

config>service>vprn>ospf

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the preference for OSPF external routes.

A route can be learned by the router from different protocols, in which case the costs are not comparable. When this occurs, the preference is used to decide which route is used.

Different protocols should not be configured with the same preference. If this occurs, the tiebreaker is based on the default preference table, as shown in the following table.

Table 95: Route preference defaults by route type

Route type	Preference	Configurable
Direct attached	0	No
Static routes	5	Yes
OSPF internal	10	Yes[18]
IS-IS level 1 internal	15	Yes
IS-IS level 2 internal	18	Yes
RIP	100	Yes
OSPF external	150	Yes
IS-IS level 1 external	160	Yes
IS-IS level 2 external	165	Yes
BGP	170	Yes

[18] Preference for OSPF internal routes is configured with the preference command.

If multiple routes are learned with an identical preference using the same protocol, the lowest cost route is used. If multiple routes are learned with an identical preference using the same protocol and the costs (metrics) are equal, the decision of which route to use is determined by the configuration of the **ecmp** command in the **config>router** context

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

Default

external-preference 150

Parameters

preference

Specifies the preference for external routes expressed as a decimal integer (see Table 95: Route preference defaults by route type).

Values 1 to 255

ignore-dn-bit

Syntax

[**no**] **ignore-dn-bit**

Context

config>service>vprn>ospf

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command specifies whether to ignore the DN (down) bit for OSPF LSA packets for this instance of OSPF on the router. When enabled, the DN bit for OSPF LSA packets is ignored. When disabled, the DN bit is not ignored for OSPF LSA packets.

import

Syntax

import *policy-name* [*policy-name*...(up to 5 max)]

no import

Context

config>service>vprn>ospf

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command specifies the import route policy that determines which routes are accepted from peers. Route policies are configured in the **config>router>policy-options** context.

This configuration parameter can be set at three levels: global level (applies to all peers), group level (applies to all peers in peer-group), or neighbor level (only applies to specified peer). The most specific level is used.

When multiple policy names are specified, the policies are evaluated in the order they are specified. A maximum of five (5) policy names can be specified. The first policy that matches is applied.

When multiple import commands are issued, the last command entered overrides the previous command.

The **no** form of this command removes the policy association. To remove the association of all policies, use **no import** without arguments.

Default

no import

Parameters

policy-name

Specifies the route policy name. Allowed values are any string up to 32 characters composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), the entire string must be enclosed within double quotes.

overload

Syntax

overload [**timeout** *seconds*]

no overload

Context

config>service>vprn>ospf

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command changes the overload state of the local router so that it appears to be overloaded. When overload is enabled, the router can participate in OSPF routing, but is not used for transit traffic. Traffic that is destined for directly attached interfaces continues to reach the router.

To put the IGP in an overload state, enter a timeout value. The IGP enters the overload state until the timeout timer expires or a **no overload** command is executed.

If the **overload** command is encountered during the execution of an command, this command takes precedence. This could occur as a result of a saved configuration file where both parameters are saved. When the file is saved by the system, the **overload-on-boot** command is saved after the **overload** command.

The **no** form of this command reverts to the default value. When the **no overload** command is executed, the overload state is terminated, regardless of the reason the protocol entered overload state.

Default

no overload

Parameters

timeout *seconds*

Specifies the number of seconds to reset overloading.

Values 60 to 1800

Default 60

overload-include-stub

Syntax

[**no**] **overload-include-stub**

Context

config>service>vprn>ospf

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures whether the OSPF stub networks should be advertised with a maximum metric value when the system goes into an overload state for any reason. When enabled, the system uses the maximum metric value. When this command is enabled and the router is in overload, all stub interfaces, including loopback and system interfaces, are advertised at the maximum metric.

Default

no overload-include-stub

overload-on-boot

Syntax

overload-on-boot [**timeout** *seconds*]

no overload

Context

config>service>vprn>ospf

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

When the router is in an overload state, the router is used only if there is no other router to reach the destination. This command configures the IGP upon bootup in the overload state until one of the following events occur:

- the timeout timer expires
- a manual override of the current overload state is entered with the **no overload** command

The **no overload** command does not affect the **overload-on-boot** function.

The **no** form of this command removes the **overload-on-boot** functionality from the configuration.

Default

no overload-on-boot

Parameters

timeout *seconds*

Specifies the number of seconds to reset overloading.

Values 60 to 1800

Default 60

preference

Syntax

preference *preference*

no preference

Context

config>service>vprn>ospf

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the preference for OSPF internal routes.

A route can be learned by the router from different protocols, in which case the costs are not comparable. When this occurs, the preference is used to decide to which route is used.

Different protocols should not be configured with the same preference. If this occurs, the tiebreaker is based on the default preference table, as listed in Table 95: Route preference defaults by route type. If multiple routes are learned with an identical preference using the same protocol, the lowest cost route is used.

If multiple routes are learned with an identical preference using the same protocol and the costs (metrics) are equal, the decision of which route to use is determined by the configuration of the **ecmp** command in the **config>router** context.

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

Default

preference 10

Parameters

preference

Specifies the preference for internal routes, expressed as a decimal integer. Table 95: Route preference defaults by route type lists the defaults for different route types.

Values 1 to 255

reference-bandwidth

Syntax

reference-bandwidth *bandwidth-in-kbps*

no reference-bandwidth

Context

config>service>vprn>ospf

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the reference bandwidth used to calculate the default costs of interfaces based on their underlying link speed.

The default interface cost is calculated as follows:

cost = reference - bandwidth # bandwidth

The default reference bandwidth is 100,000,000 kb/s or 100 Gb/s; therefore, the default auto-cost metrics for various link speeds are as follows:

- 10 Mb/s link default cost of 10000
- 100 Mb/s link default cost of 1000
- 1 Gb/s link default cost of 100
- 10 Gb/s link default cost of 10

The **reference-bandwidth** command assigns a default cost to the interface based on the interface speed. To override this default cost on an interface, use the **metric** command in the **config>router>ospf>area>interface** *ip-int-name* context.

The **no** form of this command reverts the reference-bandwidth to the default value.

Default

reference-bandwidth 100000000

Parameters

bandwidth-in-kbps

Specifies the reference bandwidth in kilobits per second, expressed as a decimal integer.

Values 1 to 4000000000

super-backbone

Syntax

[**no**] **super-backbone**

Context

config>service>vprn>ospf

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command specifies whether CE-PE functionality is required.

The OSPF super backbone indicates the type of the LSA generated as a result of routes redistributed into OSPF. When enabled, the redistributed routes are injected as summary, external, or NSSA LSAs. When disabled, the redistributed routes are injected as either external or NSSA LSAs only.

Default

no super-backbone

suppress-dn-bit

Syntax

[**no**] **suppress-dn-bit**

Context

config>service>vprn>ospf

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command specifies whether to suppress the setting of the DN (down) bit for OSPF LSA packets generated by this instance of OSPF on the router. When enabled, the DN bit for OSPF LSA packets generated by this instance of the OSPF router is not set. When disabled, this instance of the OSPF router follows the normal procedure to determine whether to set the DN bit.

Default

no suppress-dn-bit

timers

Syntax

timers

Context

config>service>vprn>ospf

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures OSPF timers. Timers control the delay between receipt of an LSA requiring an SPF calculation and the minimum time between successive SPF calculations.

Changing the timers affects CPU utilization and network reconvergence times. Lower values reduce convergence time but increase CPU utilization. Higher values reduce CPU utilization but increase reconvergence time.

spf-wait

Syntax

spf-wait *max-spf-wait* [*spf-initial-wait* [*spf-second-wait*]]

no spf-wait

Context

config>service>vprn>ospf>timers

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command defines the maximum interval between two consecutive SPF calculations. in milliseconds. Timers that determine when to initiate the first, second, and subsequent SPF calculations after a topology change occurs can be controlled with this command. Subsequent SPF runs (if required) occur at

exponentially increasing intervals of the *spf-second-wait* interval. For example, if the *spf-second-wait* interval is 1000, the next SPF runs after 2000 milliseconds, and the next SPF runs after 4000 milliseconds, and so on, until it reaches the **spf-wait** value. The SPF interval stays at the **spf-wait** value until there are no more SPF runs scheduled in that interval. After a full interval without any SPF runs, the SPF interval drops back to *spf-initial-wait*.

The timer must be entered in increments of 100 milliseconds. Values entered that do not match this requirement are rejected.

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

Default

no spf-wait

Parameters

max-spf-wait

Specifies the maximum interval, in milliseconds, between two consecutive SPF calculations.

Values 1 to 120000

Default 1000

spf-initial-wait

Specifies the initial SPF calculation delay, in milliseconds, after a topology change.

Values 10 to 100000

Default 1000

spf-second-wait

Specifies the hold time, in milliseconds, between the first and second SPF calculation.

Values 10 to 100000

Default 1000

vpn-domain

Syntax

vpn-domain *id* {**0005** | **0105** | **0205** | **8005**}

no vpn-domain

Context

config>service>vprn>ospf

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command specifies the type of the extended community attribute exchanged using BGP to carry the OSPF VPN domain ID. This command applies to VPRN instances of OSPF only. An attempt to modify the value of this object results in an inconsistent value error when the instance is not a VPRN instance. The parameters are mandatory and can be entered in any order.

Default

no vpn-domain

Parameters

id

Specifies the OSPF VPN domain in the format "xxxx.xxxx.xxxx". This ID is exchanged using BGP in the extended community attribute associated with a prefix. This object applies to VPRN instances of OSPF only.

0005 | 0105 | 0205 | 8005

Specifies the type of the extended community attribute exchanged using BGP to carry the OSPF VPN domain ID.

vpn-tag

Syntax

vpn-tag *vpn-tag*

no vpn-tag

Context

config>service>vprn>ospf

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command specifies the route tag for an OSPF VPN on a PE router. This field is set in the tag field of the OSPF external LSAs generated by the PE. This command is mainly used to prevent routing loops. This applies to VPRN instances of OSPF only. An attempt to modify the value of this object results in an inconsistent value error when the instance is not a VPRN instance.

Default

vpn-tag 0

Parameters

vpn-tag

Specifies the route tag for an OSPF VPN.

Default 0 to 4294967295

lsa-arrival

Syntax

lsa-arrival *lsa-arrival-time*

no lsa-arrival

Context

config>service>vprn>ospf>timers

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This parameter defines the minimum delay that must pass between receipt of the same LSAs arriving from neighbors.

Nokia recommends that the configured **lsa-generate** *lsa-second-wait* interval for the neighbors be equal or greater than the *lsa-arrival-time*.

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

Default

no lsa-arrival

Parameters

lsa-arrival-time

Specifies the timer in milliseconds. Values entered that do not match this requirement are rejected.

Values 0 to 600000

lsa-generate

Syntax

lsa-generate *max-lsa-wait* [*lsa-initial-wait* [*lsa-second-wait*]]

no lsa-generate-interval

Context

config>service>vprn>ospf>timers

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command configures the throttling of OSPF LSA generation. Timers that determine when to generate the first, second, and subsequent LSAs can be controlled with this command. Subsequent LSAs are generated at increasing intervals of the *lsa-second-wait* timer until a maximum value is reached. It is recommended that the *lsa-arrival-time* value be equal or less than the *lsa-second-wait* value configured in the **lsa-generate** command .

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

Default

no lsa-generate

Parameters

max-lsa-wait

Specifies the maximum interval, in milliseconds, between two consecutive occurrences of an LSA being generated.

The timer must be entered as either 1 or in millisecond increments. Values entered that do not match this requirement are rejected.

Values 1 to 600000

7.4.2.2 Show commands

egress-label

Syntax

egress-label *start-label* [*end-label*]

Context

show>service

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays service information using the range of egress labels.

If only the mandatory *start-label* parameter is specified, only services using the specified label are displayed.

If both *start-label* and *end-label* parameters are specified, the services using the labels in the specified range are displayed.

Use the **show router ldp bindings** command to display dynamic labels.

Parameters

start-label

Specifies the starting egress label value for which to display services using the label range. If only *egress-label1* is specified, services only using *egress-label1* are displayed.

Values 0 | 2048 to 131071

end-label

Specifies the ending egress label value for which to display services using the label range.

Default the *egress-label1* value

Values 2049 to 131071

Output

The following output is an example of egress label information, and Table 96: Output fields: egress label describes the output fields.

Sample output

```
*A:ALA-12# show service egress-label 0 10000
==============================================================================
Martini Service Labels
==============================================================================
Svc Id     Sdp Id             Type I.Lbl        E.Lbl
------------------------------------------------------------------------------
1          10:1               Mesh 0            0
1          20:1               Mesh 0            0
1          30:1               Mesh 0            0
1          100:1              Mesh 0            0
...
1          107:1              Mesh 0            0
1          108:1              Mesh 0            0
1          300:1              Mesh 0            0
1          301:1              Mesh 0            0
1          302:1              Mesh 0            0
1          400:1              Mesh 0            0
1          500:2              Spok 131070       2001
1          501:1              Mesh 131069       2000
100        300:100            Spok 0            0
200        301:200            Spok 0            0
300        302:300            Spok 0            0
400        400:400            Spok 0            0
------------------------------------------------------------------------------
Number of Bindings Found : 23
==============================================================================
*A:ALA-12#
```

Table 96: Output fields: egress label

Label	Description
Svc Id	The ID that identifies a service.
Sdp Id	The ID that identifies an SDP.

Label	Description
Type	Indicates whether the SDP binding is a spoke or a mesh.
I. Lbl	The VC label used by the far-end device to send packets to this device in this service by the SDP.
E. Lbl	The VC label used by this device to send packets to the far-end device in this service by the SDP.
Number of bindings found	The total number of SDP bindings that exist within the specified egress label range.

ingress-label

Syntax

ingress-label *start-label* [*end-label*]

Context

show>service

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays services using the range of ingress labels.

If only the mandatory *start-label* parameter is specified, only services using the specified label are displayed.

If both *start-label* and *end-label* parameters are specified, the services using the labels in the specified range are displayed.

Use the **show router** *vprn-service-id* **ldp bindings** command to display dynamic labels.

Parameters

start-label

Specifies the starting ingress label value for which to display services using the label range. If only *start-label* is specified, services only using *start-label* are displayed.

Values 0, 2048 to 131071

end-label

Specifies the ending ingress label value for which to display services using the label range.

Default the *start-label* value

Values 2048 to 131071

Output

The following output is an example of ingress label information, and Table 97: Output fields: ingress label describes the output fields.

Sample output

```
*A:ALA-12# show service ingress-label 0
===============================================================================
Martini Service Labels
===============================================================================
Svc Id     Sdp Id             Type I.Lbl        E.Lbl
-------------------------------------------------------------------------------
1          10:1               Mesh 0            0
1          20:1               Mesh 0            0
1          30:1               Mesh 0            0
1          50:1               Mesh 0            0
1          100:1              Mesh 0            0
1          101:1              Mesh 0            0
1          102:1              Mesh 0            0
1          103:1              Mesh 0            0
1          104:1              Mesh 0            0
1          105:1              Mesh 0            0
1          106:1              Mesh 0            0
1          107:1              Mesh 0            0
1          108:1              Mesh 0            0
1          300:1              Mesh 0            0
1          301:1              Mesh 0            0
1          302:1              Mesh 0            0
1          400:1              Mesh 0            0
100        300:100            Spok 0            0
200        301:200            Spok 0            0
300        302:300            Spok 0            0
400        400:400            Spok 0            0
-------------------------------------------------------------------------------
Number of Bindings Found : 21
-------------------------------------------------------------------------------
*A:ALA-12#
```

Table 97: Output fields: ingress label

Label	Description
Svc ID	The service identifier.
SDP Id	The SDP identifier.
Type	Indicates whether the SDP is a spoke or a mesh.
I.Lbl	The ingress label used by the far-end device to send packets to this device in this service by the SDP.
E.Lbl	The egress label used by this device to send packets to the far-end device in this service by the SDP.
Number of Bindings Found	The number of SDP bindings within the label range specified.

sap-using

Syntax

sap-using [**sap** *sap-id*]

sap-using interface [*ip-address* | *ip-int-name*]

sap-using [**ingress** | **egress**] **filter** *filter-id*

sap-using [**ingress** | **egress**] **qos-policy** *qos-policy-id*

Context

show>service

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays SAP information.

If no optional parameters are specified, the command displays a summary of all defined SAPs.

The optional parameters restrict output to only SAPs matching the specified properties.

Parameters

sap-id

Specifies the physical port identifier portion of the SAP definition. See Common CLI command descriptions for command syntax.

interface

Keyword to specify matching SAPs with the specified IP interface.

ip-address

Specifies the IP address of the interface for which to display matching SAPs.

Values a.b.c.d

ip-int-name

Specifies the IP interface name for which to display matching SAPs.

ingress

Keyword to specify matching an ingress policy.

egress

Keyword to specify matching an egress policy.

qos-policy *qos-policy-id*

Specifies the ingress or egress QoS policy ID for which to display matching SAPs.

Values 1 to 65535

filter *filter-id*

Specifies the ingress or egress filter policy ID for which to display matching SAPs.

Values 1 to 65535

Output

The following output is an example of SAP service using information, and Table 98: Output fields: service SAP using describes the output fields.

Sample output

```
*A:ALA-12# show service sap-using sap 1/1
===============================================================================
Service Access Points
===============================================================================
PortId         SvcId      SapMTU I.QoS I.Mac/IP E.QoS E.Mac/IP A.Pol  Adm  Opr
-------------------------------------------------------------------------------
1/1/7:0        1          1518   10    8        10    none     none   Up   Up
1/1/11:0       100        1514   1     none     1     none     none   Down Down
1/1/7:300      300        1518   10    none     10    none     1000   Up   Up
-------------------------------------------------------------------------------
Number of SAPs : 3
-------------------------------------------------------------------------------
*A:ALA-12#
```

Table 98: Output fields: service SAP using

Label	Description
Port ID	The ID of the access port where the SAP is defined.
Svc ID	The service identifier.
SapMTU	The SAP MTU value.
I.QoS	The SAP ingress QoS policy number specified on the ingress SAP.
I.MAC/IP	The MAC or IP filter policy ID applied to the ingress SAP.
E.QoS	The SAP egress QoS policy number specified on the egress SAP.
E.Mac/IP	The MAC or IP filter policy ID applied to the egress SAP
A.Pol	The accounting policy ID assigned to the SAP.
Adm	The configured state of the SAP.
Opr	The actual state of the SAP.

sdp

Syntax

sdp [*sdp-id* | **far-end** *ip-address*] [**detail** | **keep-alive-history**]

Context

show>service

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays SDP information.

If no optional parameters are specified, a summary SDP output for all SDPs is displayed.

Parameters

sdp-id

Specifies the SDP ID for which to display information.

Default All SDPs.

Values 1 to 17407

far-end *ip-address*

Displays only SDPs matching with the specified far-end IP address.

Default SDPs with any far-end IP address.

detail

Displays detailed SDP information.

Default SDP summary output.

keep-alive-history

Displays the last fifty SDP keepalive events for the SDP.

Default SDP summary output.

Output

The following output is an example of SDP information, and Table 99: Output fields: service SDP describes the output fields.

Sample output

```
*A:ALA-12# show service sdp
===============================================================================
Services: Service Destination Points
===============================================================================
```

```
SdpId    Adm MTU   Opr MTU   IP address       Adm  Opr         Deliver Signal
-------------------------------------------------------------------------------
10       4462      4462      10.20.1.3        Up   Dn NotReady MPLS    TLDP
40       4462      1534      10.20.1.20       Up   Up          MPLS    TLDP
-------------------------------------------------------------------------------
Number of SDPs : 5
===============================================================================
*A:ALA-12#

*A:ALA-12# show service sdp 8
===============================================================================
Service Destination Point (Sdp Id : 8)
===============================================================================
SdpId    Adm MTU   Opr MTU   IP address       Adm  Opr         Deliver Signal
-------------------------------------------------------------------------------
8        4462      4462      10.10.10.104     Up   Dn NotReady MPLS    TLDP
===============================================================================
Service Destination Point (Sdp Id : 8) Details
-------------------------------------------------------------------------------
 Sdp Id 8  -(10.10.10.104)
-------------------------------------------------------------------------------
Description           : MPLS-10.10.10.104
SDP Id               : 8
Admin Path MTU       : 0                    Oper Path MTU      : 0
Far End              : 10.10.10.104         Delivery           : MPLS
Admin State          : Up                   Oper State         : Down
Flags                : SignalingSessDown TransportTunnDown
Signaling            : TLDP                 VLAN VC Etype      : 0x8100
Last Status Change   : 02/01/2007 09:11:39  Adv. MTU Over.     : No
Last Mgmt Change     : 02/01/2007 09:11:46

KeepAlive Information :
Admin State          : Disabled             Oper State         : Disabled
Hello Time           : 10                   Hello Msg Len      : 0
Hello Timeout        : 5                    Unmatched Replies  : 0
Max Drop Count       : 3                    Hold Down Time     : 10
Tx Hello Msgs        : 0                    Rx Hello Msgs      : 0

Associated LSP LIST :
Lsp Name             : to-104
Admin State          : Up                   Oper State         : Down
Time Since Last Tran*: 01d07h36m
===============================================================================
* indicates that the corresponding row element may have been truncated.
*A:ALA-12#
```

Table 99: Output fields: service SDP

Label	Description
SDP Id	The SDP identifier.
Adm MTU	Specifies the largest service frame size (in octets) that can be transmitted through this SDP to the far-end router, without requiring the packet to be fragmented.
Opr MTU	Specifies the actual largest service frame size (in octets) that can be transmitted through this SDP to the far-end router, without requiring the packet to be fragmented.

Label	Description
IP address	Specifies the IP address of the remote end of the MPLS tunnel defined by this SDP.
Adm Admin State	Specifies the state of the SDP.
Opr Oper State	Specifies the operating state of the SDP.
Flags	Specifies all the conditions that affect the operating status of this SDP.
Signal Signaling	Specifies the signaling protocol used to obtain the ingress and egress labels used in frames transmitted and received on the SDP.
Last Status Change	Specifies the time of the most recent operating status change to this SDP.
Last Mgmt Change	Specifies the time of the most recent management-initiated change to this SDP.
Number of SDPs	Specifies the total number of SDPs displayed according to the criteria specified.
Hello Time	Specifies how often the SDP echo request messages are transmitted on this SDP.
Deliver Delivered	Specifies the type of delivery used by the SDP: MPLS.
Number of SDPs	Specifies the total number of SDPs displayed according to the criteria specified.
Hello Time	Specifies how often the SDP echo request messages are transmitted on this SDP.
Hello Msg Len	Specifies the length of the SDP echo request messages transmitted on this SDP.
Hello Timeout	Specifies the number of seconds to wait for an SDP echo response message before declaring a timeout.
Unmatched Replies	Specifies the number of SDP unmatched message replies.
Max Drop Count	Specifies the maximum number of consecutive SDP echo request messages that can be unacknowledged before the keepalive protocol reports a fault.

Label	Description
Hold Down Time	Specifies the maximum number of consecutive SDP echo request messages that can be unacknowledged before the keepalive protocol reports a fault.
TX Hello Msgs	Specifies the number of SDP echo request messages transmitted after the keepalive was administratively enabled or the counter was cleared.
Rx Hello Msgs	Specifies the number of SDP echo request messages received after the keepalive was administratively enabled or the counter was cleared.
Associated LSP List	When the SDP type is MPLS, a list of LSPs used to reach the far-end router displays. All the LSPs in the list must terminate at the IP address specified in the far end field.

sdp-using

Syntax

sdp-using [*sdp-id*[**:***vc-id*] | **far-end** *ip-address*]

Context

show>service

Platforms

Supported on all 7210 SAS platforms as described in this document

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 to 17407

vc-id

Specifies the virtual circuit identifier.

Values 1 to 4294967295

far-end *ip-address*

Displays only services matching with the specified far-end IP address.

Default services with any far-end IP address

Output

The following output is an example of SDP service information, and Table 100: Output fields: service SDP using describes the output fields.

Sample output

```
*A:ALA-1# show service sdp-using 300
===============================================================================
Service Destination Point (Sdp Id : 300)
===============================================================================
SvcId       SdpId               Type Far End        Opr State I.Label  E.Label
-------------------------------------------------------------------------------
1           300:1               Mesh 10.0.0.13      Up        131071   131071
2           300:2               Spok 10.0.0.13      Up        131070   131070
100         300:100             Mesh 10.0.0.13      Up        131069   131069
101         300:101             Mesh 10.0.0.13      Up        131068   131068
102         300:102             Mesh 10.0.0.13      Up        131067   131067
-------------------------------------------------------------------------------
Number of SDPs : 5
-------------------------------------------------------------------------------
*A:ALA-1#


A:ALA-48# show service sdp-using
===============================================================================
SDP Using
===============================================================================
SvcId       SdpId               Type Far End        Opr State I.Label  E.Label
-------------------------------------------------------------------------------
3           2:3                 Spok 10.20.1.2      Up        n/a      n/a
103         3:103               Spok 10.20.1.3      Up        131067   131068
103         4:103               Spok 10.20.1.2      Up        131065   131069
105         3:105               Spok 10.20.1.3      Up        131066   131067
-------------------------------------------------------------------------------
Number of SDPs : 4
-------------------------------------------------------------------------------
A:ALA-48
```

Table 100: Output fields: service SDP using

Label	Description
Svc ID	The service identifier.
Sdp ID	The SDP identifier.
Type	Type of SDP: spoke or mesh.
Far End	The far end address of the SDP.
Oper State	The operational state of the service.
Ingress Label	The label used by the far-end device to send packets to this device in this service by this SDP.
Egress Label	The label used by this device to send packets to the far-end device in this service by this SDP.

service-using

Syntax

service-using [**epipe**] [**ies**] [**vpls**] [**vprn**][**sdp** *sdp-id*] [*customer customer-id*]

Context

show>service

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays the services matching specified usage properties.

If no optional parameters are specified, all services defined on the system are displayed.

Parameters

epipe

Displays matching Epipe services.

ies

Displays matching IES instances.

vpls

Displays matching VPLS instances.

vprn

Displays matching VPRN services.

sdp *sdp-id*

Displays only services bound to the specified SDP ID.

Default Services bound to any SDP ID.

Values 1 to 17407

customer *customer-id*

Displays services only associated with the specified customer ID.

Default Services associated with a customer.

Values 1 to 2147483647

Output

The following output is an example of service using information, and Table 101: Output fields: service using describes the output fields.

Sample output

```
*A:ALA-12# show service service-using customer 10
===============================================================================
Services
===============================================================================
ServiceId    Type      Adm    Opr        CustomerId        Last Mgmt Change
-------------------------------------------------------------------------------
1            VPLS      Up     Up         10                09/05/2006 13:24:15
100          IES       Up     Up         10                09/05/2006 13:24:15
300          Epipe     Up     Up         10                09/05/2006 13:24:15
900          VPRN      Up     Up         2                 11/04/2006 04:55:12
-------------------------------------------------------------------------------
Matching Services : 4
===============================================================================
*A:ALA-12#

*A:ALA-12# show service service-using epipe
===============================================================================
Services [epipe]
===============================================================================
ServiceId    Type      Adm    Opr        CustomerId        Last Mgmt Change
-------------------------------------------------------------------------------
6            Epipe     Up     Up         6                 06/22/2006 23:05:58
7            Epipe     Up     Up         6                 06/22/2006 23:05:58
8            Epipe     Up     Up         3                 06/22/2006 23:05:58
103          Epipe     Up     Up         6                 06/22/2006 23:05:58
-------------------------------------------------------------------------------
Matching Services : 4
===============================================================================
*A:ALA-12#


A:de14# show service service-using
===============================================================================
Services
===============================================================================
ServiceId    Type      Adm    Opr        CustomerId        Last Mgmt Change
-------------------------------------------------------------------------------
1            uVPLS     Up     Up         1                 10/26/2006 15:44:57
2            Epipe     Up     Down       1                 10/26/2006 15:44:57
10           mVPLS     Down   Down       1                 10/26/2006 15:44:57
11           mVPLS     Down   Down       1                 10/26/2006 15:44:57
100          mVPLS     Up     Up         1                 10/26/2006 15:44:57
101          mVPLS     Up     Up         1                 10/26/2006 15:44:57
102          mVPLS     Up     Up         1                 10/26/2006 15:44:57
999          uVPLS     Down   Down       1                 10/26/2006 16:14:33
-------------------------------------------------------------------------------
Matching Services : 8
-------------------------------------------------------------------------------
A:de14#
```

Table 101: Output fields: service using

Label	Description
Service Id	The service identifier.
Type	Specifies the service type configured for the service ID.
Adm	The configured state of the service.

Label	Description
Opr	The operating state of the service.
CustomerID	The ID of the customer who owns this service.
Last Mgmt Change	The date and time of the most recent management-initiated change to this service.

id

Syntax

id *service-id* {**all** | **arp** | **base** | **fdb** | **labels** | **mfib** | **sap** | **sdp** | **split-horizon-group** | **stp**}

Context

show>service

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays information for a specified service ID.

Parameters

service-id

Specifies the unique service identification number that identifies the service in the service domain.

all

Displays detailed information about the service.

arp

Displays ARP entries for the service.

base

Displays basic service information.

fdb

Displays FDB entries.

interface

Displays service interfaces.

labels

Displays labels being used by this service.

sap

Displays SAPs associated with the service.

sdp

Displays SDPs associated with the service.

split-horizon-group

Displays split horizon group information.

stp

Displays STP information.

all

Syntax

all

Context

show>service>id

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays detailed information for all aspects of the service.

Output

The following output is an example of detailed service information, and Table 102: Output fields: service ID All describes the output fields.

Sample output

```
*A:7210SAS>show>service>id# all

===============================================================================
Service Detailed Information
===============================================================================
Service Id        : 1                   Vpn Id            : 0
Service Type      : Epipe
Description       : (Not Specified)
Customer Id       : 1
Last Status Change: 02/12/2002 23:51:07
Last Mgmt Change  : 02/12/2002 23:50:18
Admin State       : Up                  Oper State        : Up
SAP Count         : 2
Uplink Type:      : L2
SAP Type:         : Any                 Customer vlan:    : n/a
-------------------------------------------------------------------------------
Service Access Points
-------------------------------------------------------------------------------

-------------------------------------------------------------------------------
SAP 1/1/9:600.*
-------------------------------------------------------------------------------
Service Id        : 1
SAP               : 1/1/9:600.*             Encap             : qinq
```

```
QinQ Dot1p         : Default
Description        : (Not Specified)
Admin State        : Up                      Oper State        : Up
Flags              : None
Last Status Change : 02/12/2002 23:51:06
Last Mgmt Change   : 02/12/2002 23:50:18
Dot1Q Ethertype    : 0x8100                  QinQ Ethertype    : 0x8100

Admin MTU          : 9212                    Oper MTU          : 9212
Ingr IP Fltr-Id    : n/a                     Egr IP Fltr-Id    : n/a
Ingr Mac Fltr-Id   : n/a                     Egr Mac Fltr-Id   : n/a
Ingr IPv6 Fltr-Id  : n/a                     Egr IPv6 Fltr-Id  : n/a
tod-suite          : None
Endpoint           : N/A

Acct. Pol          : None                    Collect Stats     : Disabled


-------------------------------------------------------------------------------
QOS
-------------------------------------------------------------------------------
Ingress qos-policy : n/a
-------------------------------------------------------------------------------
Aggregate Policer
-------------------------------------------------------------------------------
rate               : n/a                     burst             : n/a
-------------------------------------------------------------------------------
Ingress QoS Classifier Usage
-------------------------------------------------------------------------------
Classifiers Allocated: 2                   Meters Allocated   : 1
Classifiers Used     : 1                   Meters Used        : 1
-------------------------------------------------------------------------------
Sap Statistics
-------------------------------------------------------------------------------
                      Packets                 Octets
Ingress Stats:        0                       0
Egress Stats:         26941105                18014193523

Extra-Tag Drop Stats:   n/a                   n/a

-------------------------------------------------------------------------------
SAP 1/1/12:90
-------------------------------------------------------------------------------
Service Id         : 1
SAP                : 1/1/12:90               Encap             : q-tag
Description        : (Not Specified)
Admin State        : Up                      Oper State        : Up
Flags              : None
Last Status Change : 02/12/2002 23:51:07
Last Mgmt Change   : 02/13/2002 00:05:46
Dot1Q Ethertype    : 0x8100                  QinQ Ethertype    : 0x8100
Loopback Mode      : Internal                No-svc-port used  : 1/1/25
Loopback Src Addr  : 00:00:01:00:02:00
Loopback Dst Addr  : 00:00:01:00:03:00

Admin MTU          : 1518                    Oper MTU          : 1518
Ingr IP Fltr-Id    : n/a                     Egr IP Fltr-Id    : n/a
Ingr Mac Fltr-Id   : n/a                     Egr Mac Fltr-Id   : n/a
Ingr IPv6 Fltr-Id  : n/a                     Egr IPv6 Fltr-Id  : n/a
tod-suite          : None
Endpoint           : N/A

Acct. Pol          : None                    Collect Stats     : Disabled
```

```
-------------------------------------------------------------------------------
QOS
-------------------------------------------------------------------------------
Ingress qos-policy : 1
-------------------------------------------------------------------------------
Aggregate Policer
-------------------------------------------------------------------------------
rate               : n/a                      burst             : n/a
-------------------------------------------------------------------------------
Ingress QoS Classifier Usage
-------------------------------------------------------------------------------
Classifiers Allocated: 2                    Meters Allocated   : 1
Classifiers Used     : 1                    Meters Used        : 1
-------------------------------------------------------------------------------
Sap Statistics
-------------------------------------------------------------------------------
                        Packets                 Octets
Ingress Stats:          26940595                18013850572
Egress Stats:           0                       0
Ingress Drop Stats:     0                       0

Extra-Tag Drop Stats:   n/a                     n/a
-------------------------------------------------------------------------------
Sap per Meter stats (in/out counter mode)
-------------------------------------------------------------------------------
                        Packets                 Octets

Ingress Meter 1
For. InProf           : 8                       4265
For. OutProf          : 26941156                18014224039

-------------------------------------------------------------------------------
Service Endpoints
-------------------------------------------------------------------------------
No Endpoints found.
===============================================================================
*A:7210SAS>show>service>id#
```

Table 102: Output fields: service ID All

Label	Description
Service Detailed Information	
Service Id	The service identifier.
VPN Id	The number that identifies the VPN.
Customer Id	The customer identifier.
Last Status Change	The date and time of the most recent change in the administrative or operating status of the service.
Last Mgmt Change	The date and time of the most recent management-initiated change to this customer.
Admin State	The current administrative state.
Oper State	The current operational state.

Label	Description
Route Dist.	Displays the route distribution number.
AS Number	Displays the autonomous system number.
Router Id	Displays the router ID for this service.
Auto Bind	Specifies the automatic binding type for the SDP assigned to this service.
Vrf Target	Specifies the VRF target applied to this service.
Vrf Import	Specifies the VRF import policy applied to this service.
Vrf Export	Specifies the VRF export policy applied to this service.
Description	Generic information about the service.
SAP Count	The number of SAPs specified for this service.
SDP Bind Count	The number of SDPs bound to this service.
Split Horizon Group	Name of the split horizon group for this service.
Description	Description of the split horizon group.
Last Changed	The date and time of the most recent management-initiated change to this split horizon group.
Service Destination Points (SDPs)	
SDP Id	The SDP identifier.
Type	Indicates whether this service SDP binding is a spoke or a mesh.
Admin Path MTU	The configured largest service frame size (in octets) that can be transmitted through this SDP to the far-end router without requiring the packet to be fragmented.
Oper Path MTU	The actual largest service frame size (in octets) that can be transmitted through this SDP to the far-end router without requiring the packet to be fragmented.
Delivery	Specifies the type of delivery used by the SDP: MPLS.
Admin State	The administrative state of this SDP.
Oper State	The operational state of this SDP.
Ingress Label	The label used by the far-end device to send packets to this device in this service by this SDP.
Egress Label	The label used by this device to send packets to the far-end device in this service by this SDP.

Label	Description
Ingress Filter	The ID of the ingress filter policy.
Egress Filter	The ID of the egress filter policy.
Far End	Specifies the IP address of the remote end of the MPLS tunnel defined by this SDP.
Last Changed	The date and time of the most recent change to this customer.
Signaling	Specifies the signaling protocol used to obtain the ingress and egress labels used in frames transmitted and received on this SDP.
Admin State	Specifies the operating status of the keepalive protocol.
Oper State	The current status of the keepalive protocol.
Hello Time	Specifies how often the SDP echo request messages are transmitted on this SDP.
Hello Msg Len	Specifies the length of the SDP echo request messages transmitted on this SDP.
Max Drop Count	Specifies the maximum number of consecutive SDP Echo Request messages that can be unacknowledged before the keepalive protocol reports a fault.
Hold Down Time	Specifies the amount of time to wait before the keepalive operating status is eligible to enter the alive state.
SDP Delivery Mechanism	When the SDP type is MPLS, a list of LSPs used to reach the far-end router displays. All the LSPs in the list must terminate at the IP address specified in the far end field.
Max Drop Count	Specifies the maximum number of consecutive SDP Echo Request messages that can be unacknowledged before the keepalive protocol reports a fault.
Number of SDPs	The total number SDPs applied to this service ID.
Service Access Points	
Service Id	The service identifier.
Port Id	The ID of the access port where this SAP is defined.
Description	Generic information about the SAP.
Admin State	The configured state of the SAP.
Oper State	The operating state of the SAP.
Last Changed	The date and time of the last change.

Label	Description
Admin MTU	The configured largest service frame size (in octets) that can be transmitted through this SDP to the far-end router without requiring the packet to be fragmented.
Oper MTU	The actual largest service frame size (in octets) that can be transmitted through this SDP to the far-end router without requiring the packet to be fragmented.
Ingress qos-policy	The SAP ingress QoS policy ID.
Acct. Pol	Indicates the accounting policy applied to the SAP.
Collect Stats	Specifies whether accounting statistics are collected on the SAP.
Spoke SDPs	
Managed by Service	Specifies the service ID of the management VPLS managing this spoke-SDP.
Managed by Spoke	Specifies the SAP ID inside the management VPLS managing this spoke-SDP.
Prune state	Specifies the STP state inherited from the management VPLS.
Peer Pw Bits	Indicates the bits set by the LDP peer when there is a fault on its side of the pseudowire. LAC failures occur on the SAP that has been configured on the pipe service. PSN bits are set by SDP-binding failures on the pipe service. The pwNotForwarding bit is set when none of the preceding failures apply, such as an MTU mismatch failure. This value is applicable only if the peer is using the pseudowire status signaling method to indicate faults. pwNotForwarding — Pseudowire not forwarding lacIngressFault Local — Attachment circuit RX fault lacEgresssFault Local — Attachment circuit TX fault psnIngressFault Local — PSN-facing PW RX fault psnEgressFault Local — PSN-facing PW TX fault pwFwdingStandby — Pseudowire in standby mode
Max IPv4 Routes	Maximum IPv4 routes configured for use with the service.
Last Changed	The date and time of the most recent management-initiated change.
Dot1Q Ethertype	The dot1q Ethertype used by the SAP.
Ingr IP Fltr-Id	The policy ID of the IP filter applied at ingress.
Ingr Mac Fltr-Id	The policy ID of the MAC filter applied at ingress.
Egr IP Fltr-Id	The policy ID of the IP filter applied at egress.

Label	Description
Egr Mac Fltr-Id	The policy ID of the MAC filter applied at egress.
tod-suite	The TOD suite applied for use by this SAP.
rate	Specifies the SAP aggregate rate configured for the aggregate policer/meter used by this SAP.
burst	Specifies the burst to be used with SAP aggregate policer/meter used by this SAP.
Classifiers Allocated	Number of SAP ingress QoS resources allocated for use by this SAP.
Classifiers Used	Number of SAP ingress QoS resources in use by this SAP.
Meters Allocated	Number of SAP ingress meter resources allocated for use by this SAP. This is set to half the number of classifiers allocated to this SAP.
Meters Used	Number of SAP ingress meters in use.
Ingress Stats	The number of received packets/octets for this SAP.
Egress Stats	The number of packets/octets forwarded out of this SAP.
Ingress Drop Stats	Number of packets/octets dropped by the system.
Extra-Tag Drop Stats	Number of packets received with the count of VLAN tags exceeding the count of VLAN tags implied by the SAP encapsulation.
Ingress Meter 1	The index of the ingress QoS meter of this SAP.
For. InProf	Number of in-profile packets/octets received on this SAP.
For. OutProf	Number of out-of-profile packets/octets received on this SAP.
If Name	IP interface name assigned by user.
Protocols	Protocols enabled for use on this interface.
Oper (v4/v6)	Operational status of this interface for IPv4 and IPv6.
IP Addr/mask	IPv4 address and mask assigned to this interface.
Address Type	Whether the address is a primary or secondary address.
Broadcast Address	Type of broadcast address used: host-ones or all-ones.
If Index	The interface index assigned by the system. It is used with SNMP IfTable.

Label	Description
Virt. If Index	The interface index assigned by the system. It is used with SNMP.
Last Oper Chg	Timestamp associated with the last operational change.
Global If Index	This is the system wide Interface index allotted by the system.
If Type	Network — The IP interface is a network/core IP interface. Service — The IP interface is a service IP interface.
SNTP B.Cast	Specifies whether SNTP broadcast client mode is enabled or disabled.
Arp Timeout	Specifies the timeout for an ARP entry learned on the interface.
IP Oper MTU	The actual largest service frame size (in octets) that can be transmitted through the port to the far-end router, without requiring the packet to be fragmented.
LdpSyncTimer	Specifies the value used for IGP-LDP synchronization.
Redirects	Specifies the rate for ICMP redirect messages.
Unreachables	Specifies the rate for ICMP unreachable messages.
TTL Expired	Specifies the rate for ICMP TTL messages.
MAC Address	Specifies the 48-bit IEEE 802.3 MAC address.

authentication

Syntax

authentication

Context

show>service>id

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

Commands in this context display subscriber authentication information.

statistics

Syntax

statistics [**policy** *name*] [**sap** *sap-id*]

Context

show>service>id>authentication

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays session authentication statistics for the service.

Parameters

policy *name*

Specifies the subscriber authentication policy statistics to display.

sap *sap-id*

Specifies the SAP ID statistics to display. See Common CLI command descriptions for command syntax.

Output

The following output is an example of service ID statistics information.

Sample output

```
*A:ALA-1# show service id 11 authentication statistics
===============================================================
Authentication statistics
===============================================================
Interface / SAP                Authentication  Authentication
                               Successful      Failed
---------------------------------------------------------------
abc-11-90.1.0.254              1582            3
---------------------------------------------------------------
Number of entries: 1
===============================================================
*A:ALA-1#
```

arp

Syntax

arp [*ip-address*] | [**mac** *ieee-address*] | [**sap** *sap-id*] | [**interface** *ip-int-name*] [**sdp sdp-id:vc-id**] [**summary**]

Context

show>service>id

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays the ARP table for the IES instance.

Parameters

ip-address

Displays only ARP entries in the ARP table with the specified IP address.

Default All IP addresses.

mac *ieee-address*

Displays only ARP entries in the ARP table with the specified 48-bit MAC address. The MAC address can be expressed in the form *aa*:*bb*:*cc*:*dd*:*ee*:*ff* or *aa-bb-cc-dd-ee-ff* where *aa*, *bb*, *cc*, *dd*, *ee* and *ff* are hexadecimal numbers.

Default All MAC addresses.

sap *sap-id*

Displays SAP information for the specified SAP ID. See Common CLI command descriptions for command syntax.

port id

Specifies matching service ARP entries associated with the specified IP interface.

ip-address

Specifies the IP address of the interface for which to display matching ARP entries.

Values a.b.c.d

ip-int-name

Specifies the IP interface name for which to display matching ARPs.

Output

The following output is an example of ARP information, and Table 103: Output fields: service ID ARP describes the output fields.

Sample output

```
*A:ALA-12# show service id 2 arp
===============================================================================
ARP Table
===============================================================================
IP Address      MAC Address       Type    Age       Interface         Port
-------------------------------------------------------------------------------
10.11.1.1       00:03:fa:00:08:22 Other   00:00:00  ies-100-190.11.1  1/1/11:0
===============================================================================
*A:ALA-12#
```

Table 103: Output fields: service ID ARP

Label	Description
Service ID	The service ID number.
MAC	The specified MAC address.
Source-Identifier	The location the MAC is defined.
Type	Static FDB entries created by management.
	Learned Dynamic entries created by the learning process.
	OAM Entries created by the OAM process.
Age	The time elapsed after the service was enabled.
Interface	The interface applied to the service.
Port	The port where the SAP is applied.

base

Syntax

base

Context

show>service>id

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays basic information about the service ID, including service type, description, SAPs, and SDPs.

Output

The following output is an example of basic service information, and Table 104: Output fields: service ID base describes the output fields.

Sample output

```
*A:ALA-12# show service id 1 base
```

```
===============================================================================
Service Basic Information
===============================================================================
Service Id        : 1                   Vpn Id            : 0
Service Type      : VPRN
Customer Id       : 1
Last Status Change: 02/01/2007 09:11:39
Last Mgmt Change  : 02/01/2007 09:11:46
Admin State       : Up                  Oper State        : Down
Route Dist.       : 10001:1
AS Number         : 10000               Router Id         : 10.10.10.103
ECMP              : Enabled             ECMP Max Routes   : 8
Max Routes        : No Limit            Auto Bind         : LDP
Vrf Target        : target:10001:1
Vrf Import        : vrfImpPolCust1
Vrf Export        : vrfExpPolCust1
SAP Count         : 1                   SDP Bind Count    : 18
-------------------------------------------------------------------------------
Service Access & Destination Points
-------------------------------------------------------------------------------
Identifier                      Type         AdmMTU  OprMTU  Adm     Opr
-------------------------------------------------------------------------------
sap:1/1/7:0                     q-tag        1518    1518    Up      Up
sdp:10:1 M(10.20.1.3)           TLDP         4462    4462    Up      TLDP Down
sdp:20:1 M(10.20.1.4)           TLDP         4462    4462    Up      TLDP Down
sdp:30:1 M(10.20.1.5)           TLDP         4462    4462    Up      TLDP Down
sdp:40:1 M(10.20.1.20)          TLDP         1534    4462    Up      Up
sdp:200:1 M(10.20.1.30)         TLDP         1514    4462    Up      Up
sdp:300:1 M(10.20.1.31)         TLDP         4462    4462    Up      TLDP Down
sdp:500:1 M(10.20.1.50)         TLDP         4462    4462    Up      TLDP Down
===============================================================================
*A:ALA-12#
```

Table 104: Output fields: service ID base

Label	Description
Service Id	The service identifier.
Vpn Id	Specifies the VPN ID assigned to the service.
Service Type	Specifies the type of service.
Description	Generic information about the service.
Customer Id	The customer identifier.
Last Mgmt Change	The date and time of the most recent management-initiated change to this customer.
Adm	The configured state of the service.
Oper	The operating state of the service.
Mtu	The largest frame size (in octets) that the service can handle.
Def. Mesh VC Id	This object is only valid in services that accept mesh SDP bindings. It is used to validate the VC ID portion of each mesh SDP binding defined in the service.

Label	Description
SAP Count	The number of SAPs defined on the service.
SDP Bind Count	The number of SDPs bound to the service.
Identifier	Specifies the service access (SAP) and destination (SDP) points.
Type	Specifies the signaling protocol used to obtain the ingress and egress labels used in frames transmitted and received on the SDP.
AdmMTU	Specifies the configured largest service frame size (in octets) that can be transmitted through this SDP to the far-end ESR, without requiring the packet to be fragmented.
OprMTU	Specifies the actual largest service frame size (in octets) that can be transmitted through this SDP to the far-end ESR, without requiring the packet to be fragmented.
Opr	The operating state of the SDP.

statistics

Syntax

statistics [**sap** *sap-id*]

statistics [**sdp** *sdp-id*:*vc-id*]

statistics [**interface** *interface-name*]

Context

show>service>id>dhcp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays DHCP statistics information.

Parameters

sap-id

Specifies the physical port identifier portion of the SAP definition. See Common CLI Command Descriptions on page 973 for command syntax.

sdp-id

Specifies the SDP identifier.

Values 1 to 17407

vc-id

Specifies the virtual circuit ID on the SDP ID for which to display information.

Values 1 to 4294967295

interface-name

Displays information for the specified IP interface.

Output

The following output is an example of DHCP statistics information, and Table 105: Output fields: DHCP statistics describes the output fields.

Sample output

```
A:sim1# show service id 11 dhcp statistics
===============================================================
DHCP Global Statistics, service 11
===============================================================
Rx Packets                          : 32
Tx Packets                          : 12
Rx Malformed Packets                : 0
Rx Untrusted Packets                : 0
Client Packets Discarded            : 0
Client Packets Relayed              : 11
Client Packets Snooped              : 21
Server Packets Discarded            : 0
Server Packets Relayed              : 0
Server Packets Snooped              : 0
===============================================================
A:sim1#
```

Table 105: Output fields: DHCP statistics

Label	Description
Received Packets	The number of packets received from the DHCP clients.
Transmitted Packets	The number of packets transmitted to the DHCP clients.
Received Malformed Packets	The number of corrupted and invalid packets received from the DHCP clients.
Received Untrusted Packets	The number of untrusted packets received from the DHCP clients. In this case, a frame is dropped because of the client sending a DHCP packet with Option 82 filled in before "trust" is set under the DHCP interface command.
Client Packets Discarded	The number of packets received from the DHCP clients that were discarded.
Client Packets Relayed	The number of packets received from the DHCP clients that were forwarded.
Client Packets Snooped	The number of packets received from the DHCP clients that were snooped.

Label	Description
Server Packet Discarded	The number of packets received from the DHCP server that were discarded.
Server Packets Relayed	The number of packets received from the DHCP server that were forwarded.
Server Packets Snooped	The number of packets received from the DHCP server that were snooped.

interface

Syntax

interface [*ip-address* | *ip-int-name*] [**detail**]

Context

show>service>id

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays information for the IP interfaces associated with the service.

If no optional parameters are specified, a summary of all IP interfaces associated with the service are displayed.

Parameters

ip-address

Specifies the IP address of the interface for which to display information.

Values

ipv4-address:	a.b.c.d
ipv6-address:	x:x:x:x:x:x:x:x (eight 16-bit pieces)
	x:x:x:x:x:x:d.d.d.d
	x - [0 to FFFF]H
	d - [0 to 255]D

ip-int-name

Specifies the IP interface name, up to 32 characters, for which to display information.

detail

Displays detailed IP interface information.

Default IP interface summary output.

Output

The following output is an example of service interface information, and Table 106: Output fields: service ID interface describes the output fields.

Sample output

```
*A:ALA-12# show service id 321 interface
===============================================================================
Interface Table
===============================================================================
Interface-Name                   Type IP-Address         Adm    Opr  Type
-------------------------------------------------------------------------------
test                             Pri  10.11.1.1/24       Up     Up   IES
-------------------------------------------------------------------------------
Interfaces : 1
===============================================================================
*A:ALA-12#


A:ALA-49# show service id 88 interface detail
===============================================================================
Interface Table
===============================================================================
Interface
-------------------------------------------------------------------------------
If Name      : Sector A
Admin State  : Up                               Oper State       : Down
Protocols    : None

IP Addr/mask : Not Assigned
-------------------------------------------------------------------------------
Details
-------------------------------------------------------------------------------
Description  :
If Index     : 26                               Virt. If Index   : 26
SAP Id       : 71/1/1.2.2
TOS Marking  : Untrusted                        If Type          : IES
SNTP B.Cast  : False                            IES ID           : 88
MAC Address  : Not configured.                  Arp Timeout      : 14400
IP MTU       : 1500                             ICMP Mask Reply  : True
Arp Populate : Disabled
Cflowd       : None

Proxy ARP Details
Proxy ARP    : Enabled                          Local Proxy ARP  : Disabled
Policies     : ProxyARP

DHCP Details
Admin State  : Up                               Lease Populate   : 0
Action       : Keep                             Trusted          : Disabled
ICMP Details
Redirects    : Number - 100                     Time (seconds)   - 10
Unreachables : Number - 100                     Time (seconds)   - 10
TTL Expired  : Number - 100                     Time (seconds)   - 10
-------------------------------------------------------------------------------
Interface
-------------------------------------------------------------------------------
If Name      : test
Admin State  : Up                               Oper State       : Down
```

```
Protocols    : None
IP Addr/mask : Not Assigned
-------------------------------------------------------------------------------
Details
-------------------------------------------------------------------------------
Description  :
If Index     : 27                              Virt. If Index   : 27
SAP Id       : 101/1/2:0
TOS Marking  : Untrusted                       If Type          : IES
SNTP B.Cast  : False                           IES ID           : 88
MAC Address  : Not configured.                 Arp Timeout      : 14400
Arp Populate : Disabled

Proxy ARP Details
Proxy ARP    : Disabled                        Local Proxy ARP  : Disabled

ICMP Details
Redirects    : Number - 100                    Time (seconds)   - 10
Unreachables : Number - 100                    Time (seconds)   - 10
TTL Expired  : Number - 100                    Time (seconds)   - 10
-------------------------------------------------------------------------------
Interfaces : 2
===============================================================================
A:ALA-49#
```

Table 106: Output fields: service ID interface

Label	Description
Interface-Name	The name of the interface.
Type	Specifies the interface type.
IP-Address	Specifies the IP address/IP subnet/broadcast address of the interface.
Adm	The configured state of the interface.
Opr	The operating state of the interface.
Interface	
If Name	The name of the interface.
Admin State	The configured state of the interface.
Oper State	The operating state of the interface.
IP Addr/mask	Specifies the IP address/IP subnet/broadcast address of the interface.
Details	
If Index	The index corresponding to this interface. The primary index is 1. For example, all interfaces are defined in the Base virtual router context.
If Type	Specifies the interface type.

Label	Description
Port Id	Specifies the SAP port ID.
SNTP B.Cast	Specifies whether SNTP broadcast client mode is enabled or disabled.
Arp Timeout	Specifies the timeout for an ARP entry learned on the interface.
MAC Address	Specifies the 48-bit IEEE 802.3 MAC address.
ICMP Mask Reply	Specifies whether ICMP mask reply is enabled or disabled.
ICMP Details	
Redirects	Specifies the rate for ICMP redirect messages.
Unreachables	Specifies the rate for ICMP unreachable messages.
TTL Expired	Specifies the rate for ICMP TTL messages.

sap

Syntax

sap *sap-id* [**detail**]

Context

show>service>id

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays information for the SAPs associated with the service.

If no optional parameters are specified, a summary of all associated SAPs is displayed.

Parameters

sap-id

Specifies the ID that displays SAPs for the service. See Common CLI command descriptions for command syntax.

detail

Displays detailed information for the SAP.

Output

The following output is an example of SAP information, and Table 107: Output fields: service ID SAP describes the output fields.

Sample output

```
*A:ALA-12# show service id 321 sap 1/1/4:0
===============================================================================
Service Access Points(SAP)
===============================================================================
Service Id         : 321
SAP                : 1/1/4:0                Encap             : q-tag
Dot1Q Ethertype    : 0x8100                  QinQ Ethertype    : 0x8100
Admin State        : Up                      Oper State        : Down
Flags              : PortOperDown
                     SapIngressQoSMismatch
Last Status Change : 02/03/2007 12:58:37
Last Mgmt Change   : 02/03/2007 12:59:10
Admin MTU          : 1518                    Oper MTU          : 1518
Ingress qos-policy : 100                     Egress qos-policy : 1
Ingress Filter-Id  : n/a                     Egress Filter-Id  : n/a
Multi Svc Site     : None
Acct. Pol          : None                    Collect Stats     : Disabled
===============================================================================
*A:ALA-12#


*A:ALA-12# show service id 321 sap 1/1/4:0 detail
===============================================================================
Service Access Points(SAP)
===============================================================================
Service Id         : 321
SAP                : 1/1/4:0                Encap             : q-tag
Dot1Q Ethertype    : 0x8100                  QinQ Ethertype    : 0x8100

Admin State        : Up                      Oper State        : Down
Flags              : PortOperDown
                     SapIngressQoSMismatch
Last Status Change : 02/03/2007 12:58:37
Last Mgmt Change   : 02/03/2007 12:59:10
Admin MTU          : 1518                    Oper MTU          : 1518
Ingress qos-policy : 100                     Egress qos-policy : 1
Ingress Filter-Id  : n/a                     Egress Filter-Id  : n/a
Multi Svc Site     : None
Acct. Pol          : None                    Collect Stats     : Disabled
-------------------------------------------------------------------------------
Sap Statistics
-------------------------------------------------------------------------------
                        Packets                  Octets
Forwarding Engine Stats
Dropped               : 0                        0
Off. HiPrio           : 0                        0
Off. LowPrio          : 0                        0
Off. Uncolor          : 0                        0
Queueing Stats(Egress QoS Policy 1)
Dro. InProf           : 0                        0
Dro. OutProf          : 0                        0
For. InProf           : 0                        0
For. OutProf          : 0                        0
-------------------------------------------------------------------------------
===============================================================================
*A:ALA-12#
```

```
*A:dut-a>config>log# /show service id 100 sap 1/1/22:100 sap-stats

===============================================================================
Service Access Points(SAP)
===============================================================================
Service Id         : 100
SAP                : 1/1/22:100              Encap             : q-tag
Description        : (Not Specified)
Admin State        : Up                      Oper State        : Up
Flags              : None
Last Status Change : 02/17/2016 10:24:49
Last Mgmt Change   : 02/17/2016 10:24:46

-------------------------------------------------------------------------------
Ingress QoS Classifier Usage
-------------------------------------------------------------------------------
Classifiers Allocated: 2                   Meters Allocated   : 1
Classifiers Used     : 1                   Meters Used        : 1
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
Sap Statistics
-------------------------------------------------------------------------------
                        Packets                Octets
Ingress Stats:          0                      0
Egress Stats:           76990984               116872316748
Ingress Drop Stats:     0                      0

Extra-Tag Drop Stats:   n/a                    n/a
-------------------------------------------------------------------------------
Sap per Meter stats (in/out counter mode)
-------------------------------------------------------------------------------
                        Packets                Octets

Ingress Meter 1
For. InProf           : 0                      0
For. OutProf          : 0                      0
-------------------------------------------------------------------------------
Egr sap agg-meter stats
-------------------------------------------------------------------------------
                        Packets                Octets
Drop           :        385943060              73232696583
Forward        :        74671326               14168884298
-------------------------------------------------------------------------------
===============================================================================
*A:dut-a>
```

Table 107: Output fields: service ID SAP

Label	Description
Service Id	The service identifier.
SAP	The SAP and qtag.
Encap	The encapsulation type of the SAP.
Ethertype	Specifies an Ethernet type II Ethertype value.
Admin State	The administrative state of the SAP.
Oper State	The operating state of the SAP.

Label	Description
Flags	Specifies the conditions that affect the operating status of this SAP. Display output includes: ServiceAdminDown, SapAdmin Down, InterfaceAdminDown, PortOperDown, PortMTUToo Small, L2OperDown, SapIngressQoSMismatch, SapEgress QoSMismatch,RelearnLimitExceeded, RxProtSrcMac, Parent IfAdminDown, TodResourceUnavail, TodMssResourceUnavail, SapParamMismatch, ServiceMTUTooSmall, SapIngressNamed PoolMismatch, SapEgressNamedPoolMismatch, NoSapEpipe RingNode.
Last Status Change	Specifies the time of the most recent operating status change to this SAP.
Last Mgmt Change	Specifies the time of the most recent management-initiated change to this SAP.
Admin MTU	The configured largest service frame size (in octets) that can be transmitted through the SAP to the far-end router without requiring the packet to be fragmented.
Oper MTU	The actual largest service frame size (in octets) that can be transmitted through the SAP to the far-end router, without requiring the packet to be fragmented.
Ingress qos-policy	The ingress QoS policy ID assigned to the SAP.
Egress qos-policy	The egress QoS policy ID assigned to the SAP.
Ingress Filter-Id	The ingress filter policy ID assigned to the SAP.
Table-based	Indicates the use of table-based resource classification: Enabled (table-based) or Disabled (CAM-based).
Egress Filter-Id	The egress filter policy ID assigned to the SAP.
Acct. Pol	The accounting policy ID assigned to the SAP.
Collect Stats	Specifies whether collect stats is enabled.
Dropped	The number of packets and octets dropped because of SAP state, ingress MAC or IP filter, same segment discard, bad checksum, and so on.
Off. HiPrio	The number of high priority packets and octets, as determined by the SAP ingress QoS policy, offered by the Pchip to the Qchip.
Off. LowPrio	The number of low priority packets and octets, as determined by the SAP ingress QoS policy, offered by the Pchip to the Qchip.
Off. Uncolor	The number of uncolored packets and octets, as determined by the SAP ingress QoS policy, offered by the Pchip to the Qchip.

Label	Description
Dro. HiPrio	The number of high priority packets and octets, as determined by the SAP ingress QoS policy, dropped by the Qchip because of MBS exceeded, buffer pool limit exceeded, and so on.
Dro. LowPrio	The number of low priority packets and octets, as determined by the SAP ingress QoS policy, dropped by the Qchip because of MBS exceeded, buffer pool limit exceeded, and so on.
For. InProf	The number of in-profile packets and octets (rate below CIR) forwarded by the ingress Qchip.
For. OutProf	The number of out-of-profile packets and octets discarded by the egress Qchip because of MBS exceeded, buffer pool limit exceeded, and so on.
Dro. InProf	The number of in-profile packets and octets discarded by the egress Qchip because of MBS exceeded, buffer pool limit exceeded, and so on.
Dro. OutProf	The number of out-of-profile packets and octets discarded by the egress Qchip because of MBS exceeded, buffer pool limit exceeded, and so on.
For. InProf	The number of in-profile packets and octets (rate below CIR) forwarded by the egress Qchip.
For. OutProf	The number of out-of-profile packets and octets (rate above CIR) forwarded by the egress Qchip.
Ingress TD Profile	The profile ID applied to the ingress SAP.
Egress TD Profile	The profile ID applied to the egress SAP.
Alarm Cell Handling	The indication that OAM cells are being processed.
AAL-5 Encap	The AAL-5 encapsulation type.

sdp

Syntax

sdp [*sdp-id* | **far-end** *ip-addr*] [**detail**]

Context

show>service>id

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays information for the SDPs associated with the service. If no optional parameters are specified, a summary of all associated SDPs is displayed.

Parameters

sdp-id

Displays only information for the specified SDP ID.

Default All SDPs.

Values 1 to 17407

far-end *ip-addr*

Displays only SDPs matching with the specified far-end IP address.

Default SDPs with any far-end IP address.

detail

Displays detailed SDP information.

Output

The following output is an example of SDP information, and Table 108: Output fields: service ID SDP describes the output fields.

Sample output

```
A:Dut-A# show service id  1 sdp detail
===============================================================================
Services: Service Destination Points Details
===============================================================================
 Sdp Id 1:1  -(10.20.1.2)
-------------------------------------------------------------------------------
Description     : Default sdp description
SDP Id             : 1:1                      Type              : Spoke
VC Type            : Ether                    VC Tag            : n/a
Admin Path MTU     : 0                        Oper Path MTU     : 9186
Far End            : 10.20.1.2                Delivery          : MPLS

Admin State        : Up                       Oper State        : Up
Acct. Pol          : None                     Collect Stats     : Disabled
Ingress Label      : 2048                     Egress Label      : 2048
Ing mac Fltr       : n/a                      Egr mac Fltr      : n/a
Ing ip Fltr        : n/a                      Egr ip Fltr       : n/a
Ing ipv6 Fltr      : n/a                      Egr ipv6 Fltr     : n/a
Admin ControlWord  : Not Preferred            Oper ControlWord  : False
Last Status Change : 05/31/2007 00:45:43      Signaling         : None
Last Mgmt Change   : 05/31/2007 00:45:43
Class Fwding State : Up
Flags              : None
Peer Pw Bits       : None
Peer Fault Ip      : None
Peer Vccv CV Bits  : None
Peer Vccv CC Bits  : None
Max Nbr of MAC Addr: No Limit                 Total MAC Addr    : 0
Learned MAC Addr   : 0                        Static MAC Addr   : 0

MAC Learning       : Enabled                  Discard Unkwn Srce: Disabled
```

```
MAC Aging          : Enabled
L2PT Termination   : Disabled               BPDU Translation  : Disabled
MAC Pinning        : Disabled

KeepAlive Information :
Admin State        : Disabled               Oper State        : Disabled
Hello Time         : 10                     Hello Msg Len     : 0
Max Drop Count     : 3                      Hold Down Time    : 10

Statistics           :
I. Fwd. Pkts.      : 0                      I. Dro. Pkts.     : 0
I. Fwd. Octs.      : 0                      I. Dro. Octs.     : 0
E. Fwd. Pkts.      : 0                      E. Fwd. Octets    : 0
MCAC Policy Name   :
MCAC Max Unconst BW: no limit               MCAC Max Mand BW  : no limit
MCAC In use Mand BW: 0                      MCAC Avail Mand BW: unlimited
MCAC In use Opnl BW: 0                      MCAC Avail Opnl BW: unlimited

Associated LSP LIST :
Lsp Name           : A_B_1
Admin State        : Up                     Oper State        : Up
Time Since Last Tr*: 00h26m35s

Lsp Name           : A_B_2
Admin State        : Up                     Oper State        : Up
Time Since Last Tr*: 00h26m35s

Lsp Name           : A_B_3
Admin State        : Up                     Oper State        : Up
Time Since Last Tr*: 00h26m34s

Lsp Name           : A_B_4
Admin State        : Up                     Oper State        : Up
Time Since Last Tr*: 00h26m34s

Lsp Name           : A_B_5
Admin State        : Up                     Oper State        : Up
Time Since Last Tr*: 00h26m34s

Lsp Name           : A_B_6
Admin State        : Up                     Oper State        : Up
Time Since Last Tr*: 00h26m34s

Lsp Name           : A_B_7
Admin State        : Up                     Oper State        : Up
Time Since Last Tr*: 00h26m34s

Lsp Name           : A_B_8
Admin State        : Up                     Oper State        : Up
Time Since Last Tr*: 00h26m35s

Lsp Name           : A_B_9
Admin State        : Up                     Oper State        : Up
Time Since Last Tr*: 00h26m34s

Lsp Name           : A_B_10
Admin State        : Up                     Oper State        : Up
Time Since Last Tr*: 00h26m34s
-------------------------------------------------------------------------------
Class-based forwarding :
-------------------------------------------------------------------------------
Class forwarding   : enabled
Default LSP        : A_B_10                 Multicast LSP     : A_B_9
===============================================================================
```

```
FC Mapping Table
===============================================================================
FC Name             LSP Name
-------------------------------------------------------------------------------
af                  A_B_3
be                  A_B_1
ef                  A_B_6
h1                  A_B_7
h2                  A_B_5
l1                  A_B_4
l2                  A_B_2
nc                  A_B_8
===============================================================================
Stp Service Destination Point specifics
-------------------------------------------------------------------------------
Mac Move           : Blockable
Stp Admin State    : Up                       Stp Oper State    : Down
Core Connectivity  : Down
Port Role          : N/A                      Port State        : Forwarding
Port Number        : 2049                     Port Priority     : 128
Port Path Cost     : 10                       Auto Edge         : Enabled
Admin Edge         : Disabled                 Oper Edge         : N/A
Link Type          : Pt-pt                    BPDU Encap        : Dot1d
Root Guard         : Disabled                 Active Protocol   : N/A
Last BPDU from     : N/A
Designated Bridge  : N/A                      Designated Port Id: 0

Fwd Transitions    : 0                        Bad BPDUs rcvd    : 0
Cfg BPDUs rcvd     : 0                        Cfg BPDUs tx      : 0
TCN BPDUs rcvd     : 0                        TCN BPDUs tx      : 0
RST BPDUs rcvd     : 0                        RST BPDUs tx      : 0
-------------------------------------------------------------------------------
Number of SDPs : 1
-------------------------------------------------------------------------------
* indicates that the corresponding row element may have been truncated.
-------------------------------------------------------------------------------
A:Dut-A#
```

Table 108: Output fields: service ID SDP

Label	Description
Sdp Id	The SDP identifier.
Type	Indicates whether the SDP is a spoke or a mesh.
Split Horizon Group	Name of the split horizon group that the SDP belongs to.
VC Type	Displays the VC type: ether or vlan.
VC Tag	Displays the explicit dot1Q value used when encapsulating to the SDP far end.
I. Lbl	The VC label used by the far-end device to send packets to this device in this service by the SDP.
Admin Path MTU	The operating path MTU of the SDP is equal to the admin path MTU (when one is set) or the dynamically computed tunnel MTU, when no admin path MTU is set (the default case).

Label	Description
Oper Path MTU	The actual largest service frame size (in octets) that can be transmitted through this SDP to the far-end router, without requiring the packet to be fragmented.
Far End	Specifies the IP address of the remote end of the MPLS tunnel defined by this SDP.
Delivery	Specifies the type of delivery used by the SDP: MPLS.
Admin State	The administrative state of this SDP.
Oper State	The operational state of this SDP.
Ingress Label	The label used by the far-end device to send packets to this device in this service by this SDP.
Egress Label	The label used by this device to send packets to the far-end device in this service by the SDP.
Last Changed	The date and time of the most recent change to the SDP.
Signaling	Specifies the signaling protocol used to obtain the ingress and egress labels used in frames transmitted and received on this SDP.
Admin State	The administrative state of the keepalive process.
Oper State	The operational state of the keepalive process.
Hello Time	Specifies how often the SDP echo request messages are transmitted on this SDP.
Max Drop Count	Specifies the maximum number of consecutive SDP echo request messages that can be unacknowledged before the keepalive protocol reports a fault.
Hello Msg Len	Specifies the length of the SDP echo request messages transmitted on this SDP.
Hold Down Time	Specifies the amount of time to wait before the keepalive operating status is eligible to enter the alive state.
I. Fwd. Pkts.	Specifies the number of forwarded ingress packets.
I. Dro. Pkts.	Specifies the number of dropped ingress packets.
E. Fwd. Pkts.	Specifies the number of forwarded egress packets.
Associated LSP List	When the SDP type is MPLS, a list of LSPs used to reach the far-end router displays. All the LSPs in the list must terminate at the IP address specified in the far-end field.

aggregate

Syntax

aggregate [**active**]

Context

show>router

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays aggregated routes.

Parameters

active

Keyword that filters out inactive aggregates.

Output

The following output is an example of aggregate route information, and Table 109: Output fields: router aggregate describes the output fields.

Sample output

```
*A:ALA-12# show router 3 aggregate
===============================================================================
Aggregates (Service: 3)
===============================================================================
Prefix                Summary  AS Set   Aggr AS     Aggr IP-Address   State
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
No. of Aggregates: 0
-------------------------------------------------------------
*A:ALA-12#
```

Table 109: Output fields: router aggregate

Label	Definition
Prefix	Displays the destination address of the aggregate route in dotted-decimal notation.
Summary	Specifies whether the aggregate or more specific components are advertised.
AS Set	Displays an aggregate where the path advertised for the route consists of all elements contained in all paths that are being summarized.

Label	Definition
Aggr AS	Displays the aggregator path attribute to the aggregate route.
Aggr IP-Address	The IP address of the aggregated route.
State	The operational state of the aggregated route.
No. of Aggregates	The total number of aggregated routes.

arp

Syntax

arp [*ip-address* | *ip-int-name* | **mac** *ieee-mac-addr*]

Context

show>router

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays the router ARP table sorted by IP address.

If no command line options are specified, all ARP entries are displayed.

Parameters

ip-addr

Displays only ARP entries associated with the specified IP address.

ip-int-name

Displays only ARP entries associated with the specified IP interface name.

macieee-mac-addr

Displays only ARP entries associated with the specified MAC address.

Output

The following output is an example of router ARP table information, and Table 110: Output fields: ARP table describes the output fields.

Sample output

```
*A:ALA-12# show router 3 arp
===============================================================================
ARP Table (Service: 3)
===============================================================================
IP Address      MAC Address       Expiry    Type   Interface
-------------------------------------------------------------------------------
10.10.10.103    04:67:ff:00:00:01 00h00m00s Oth    system
10.10.4.3       00:00:00:00:00:00 00h00m00s Oth    ALA-1-2
```

```
10.10.5.3       00:00:00:00:00:00 00h00m00s Oth    ALA-1-3
10.10.7.3       00:00:00:00:00:00 00h00m00s Oth    ALA-1-5
10.10.0.16      00:00:00:00:00:00 00h00m00s Oth    bozo
10.10.3.3       00:00:00:00:00:00 00h00m00s Oth    gizmo
10.10.2.3       00:00:00:00:00:00 00h00m00s Oth    hobo
10.10.1.17      00:00:00:00:00:00 00h00m00s Oth    int-cflowd
10.0.0.92       00:00:00:00:00:00 04h00m00s Dyn    to-104
10.0.0.103      04:67:01:01:00:01 00h00m00s Oth[I] to-104
10.0.0.104      04:68:01:01:00:01 03h59m49s Dyn[I] to-104
10.10.36.2      00:00:00:00:00:00 00h00m00s Oth    tuesday
192.168.2.98    00:03:47:c8:b4:86 00h14m37s Dyn[I] management
192.168.2.103   00:03:47:dc:98:1d 00h00m00s Oth[I] management
-------------------------------------------------------------------------------
No. of ARP Entries: 14
===============================================================================
*A:ALA-12#


*A:ALA-12# show router 3 arp 10.10.0.3
===============================================================================
ARP Table
===============================================================================
IP Address      MAC Address       Expiry    Type   Interface
-------------------------------------------------------------------------------
10.10.0.3       04:5d:ff:00:00:00 00:00:00  Oth    system
===============================================================================
*A:ALA-12#


*A:ALA-12# show router 3 arp to-ser1
===============================================================================
ARP Table
===============================================================================
IP Address      MAC Address       Expiry    Type   Interface
-------------------------------------------------------------------------------
10.10.13.1      04:5b:01:01:00:02 03:53:09  Dyn    to-ser1
===============================================================================
*A:ALA-12#
```

Table 110: Output fields: ARP table

Label	Description
IP Address	The IP address of the ARP entry.
MAC Address	The MAC address of the ARP entry.
Expiry	The age of the ARP entry.
Type	Dyn The ARP entry is a dynamic ARP entry.
	Inv The ARP entry is an inactive static ARP entry (invalid).
	Oth The ARP entry is a local or system ARP entry.
	Sta

Label	Description
	The ARP entry is an active static ARP entry.
Interface	The IP interface name associated with the ARP entry.
No. of ARP Entries	The number of ARP entries displayed in the list.

damping

Syntax

damping [*ip-prefix/mask* | *ip-address*] [**detail**]

damping [*damp-type*] [**detail**]

Context

show>router>bgp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays BGP routes with have been dampened because of route flapping. This command can be entered with or without a route parameter.

Include the **detail** keyword to display more information.

When only the command is entered (without any parameters included except **detail**), all dampened routes are listed.

When a parameter is specified, the matching route or routes are listed.

When a **decayed**, **history**, or **suppressed** keyword is specified, only those types of dampened routes are listed.

Parameters

ip-prefix/mask

Displays damping information for the specified IP prefix and mask length.

ip-address

Displays the damping entry for the best match route for the specified IP address.

damp-type

Displays the damping type for the specified IP address.

decayed

Displays damping entries that are decayed but are not suppressed.

history

Displays damping entries that are withdrawn but have history.

suppressed

Displays damping entries suppressed because of route damping.

detail

Displays detailed information.

Output

The following output is an example of BGP damping, and Table 111: Output fields: BGP damping describes the output fields.

Sample output

```
*A:ALA-12# show router 3 bgp damping
===============================================================================
  BGP Router ID : 10.0.0.14         AS : 65206   Local AS : 65206
===============================================================================
  Legend -
  Status codes  : u - used, s - suppressed, h - history, d - decayed, * - valid
  Origin codes  : i - IGP, e - EGP, ? - incomplete,  - best
===============================================================================
BGP Damped Routes
===============================================================================
Flag  Network            From            Reuse       AS-Path
-------------------------------------------------------------------------------
ud*i  10.149.7.0/24      10.0.28.1       00h00m00s   60203 65001 19855 3356
                                                      1239  22406
si    19.155.6.0/23      10.0.28.1       00h43m41s   60203 65001 19855 3356
                                                      2914  7459
si    10.155.8.0/22      10.0.28.1       00h38m31s   60203 65001 19855 3356
                                                      2914  7459
si    10.155.12.0/22     10.0.28.1       00h35m41s   60203 65001 19855 3356
                                                      2914  7459
si    10.155.22.0/23     10.0.28.1       00h35m41s   60203 65001 19855 3356
                                                      2914  7459
si    10.155.24.0/22     10.0.28.1       00h35m41s   60203 65001 19855 3356
                                                      2914  7459
si    10.155.28.0/22     10.0.28.1       00h34m31s   60203 65001 19855 3356
                                                      2914  7459
si    10.155.40.0/21     10.0.28.1       00h28m24s   60203 65001 19855 3356
                                                      7911  7459
si    10.155.48.0/20     10.0.28.1       00h28m24s   60203 65001 19855 3356
                                                      7911  7459
ud*i  10.8.140.0/24      10.0.28.1       00h00m00s   60203 65001 19855 3356
                                                      4637  17447
ud*i  10.8.141.0/24      10.0.28.1       00h00m00s   60203 65001 19855 3356
                                                      4637  17447
ud*i  10.9.0.0/18        10.0.28.1       00h00m00s   60203 65001 19855 3356
                                                      3561  9658  6163
. . .
ud*i  10.213.184.0/23    10.0.28.1       00h00m00s   60203 65001 19855 3356
                                                      6774  6774  9154
-------------------------------------------------------------------------------
*A:ALA-12#


*A:ALA-12# show router 3 bgp damping detail
===============================================================================
  BGP Router ID : 10.0.0.14         AS : 65206   Local AS : 65206
===============================================================================
  Legend -
  Status codes  : u - used, s - suppressed, h - history, d - decayed, * -
```

```
 valid
  Origin codes  : i - IGP, e - EGP, ? - incomplete,  - best
===============================================================================
BGP Damped Routes
===============================================================================
-------------------------------------------------------------------------------
Network : 10.149.7.0/24
-------------------------------------------------------------------------------
Network          : 10.149.7.0/24        Peer             : 10.0.28.1
NextHop          : 10.0.28.1            Reuse time       : 00h00m00s
Peer AS          : 60203                Peer Router-Id   : 32.32.27.203
Local Pref       : none
Age              : 00h22m09s            Last update      : 02d00h58m
FOM Present      : 738                  FOM Last upd.    : 2039
Number of Flaps  : 2                    Flags            : ud*i
Path             : 60203 65001 19855 3356  1239  22406
Applied Policy   : default-damping-profile
-------------------------------------------------------------------------------
Network : 10.142.48.0/20
-------------------------------------------------------------------------------
Network          : 10.142.48.0/20       Peer             : 10.0.28.1
NextHop          : 10.0.28.1            Reuse time       : 00h00m00s
Peer AS          : 60203                Peer Router-Id   : 32.32.27.203
Local Pref       : none
Age              : 00h00m38s            Last update      : 02d01h20m
FOM Present      : 2011                 FOM Last upd.    : 2023
Number of Flaps  : 2                    Flags            : ud*i
Path             : 60203 65001 19855 3356  3561  5551  1889
Applied Policy   : default-damping-profile
-------------------------------------------------------------------------------
Network : 10.200.128.0/19
-------------------------------------------------------------------------------
Network          : 10.200.128.0/19      Peer             : 10.0.28.1
NextHop          : 10.0.28.1            Reuse time       : 00h00m00s
Peer AS          : 60203                Peer Router-Id   : 32.32.27.203
Local Pref       : none
Age              : 00h00m38s            Last update      : 02d01h20m
FOM Present      : 2011                 FOM Last upd.    : 2023
Number of Flaps  : 2                    Flags            : ud*i
Path             : 60203 65001 19855 1299  702   1889
Applied Policy   : default-damping-profile
-------------------------------------------------------------------------------
Network : 10.203.192.0/18
-------------------------------------------------------------------------------
Network          : 10.203.192.0/18      Peer             : 10.0.28.1
NextHop          : 10.0.28.1            Reuse time       : 00h00m00s
Peer AS          : 60203                Peer Router-Id   : 32.32.27.203
Local Pref       : none
Age              : 00h00m07s            Last update      : 02d01h20m
FOM Present      : 1018                 FOM Last upd.    : 1024
Number of Flaps  : 1                    Flags            : ud*i
Path             : 60203 65001 19855 1299  702   1889
Applied Policy   : default-damping-profile
-------------------------------------------------------------------------------
*A:ALA-12#


*A:ALA-12# show router 3 bgp damping 10.203.192.0/18 detail
===============================================================================
  BGP Router ID : 10.0.0.14         AS : 65206   Local AS : 65206
===============================================================================
  Legend -
  Status codes  : u - used, s - suppressed, h - history, d - decayed, * - valid
  Origin codes  : i - IGP, e - EGP, ? - incomplete,  - best
```

```
===============================================================================
BGP Damped Routes 10.203.192.0/18
===============================================================================
Network : 10.203.192.0/18
-------------------------------------------------------------------------------
Network          : 10.203.192.0/18      Peer             : 10.0.28.1
NextHop          : 10.0.28.1            Reuse time       : 00h00m00s
Peer AS          : 60203                Peer Router-Id   : 32.32.27.203
Local Pref       : none
Age              : 00h00m42s            Last update      : 02d01h20m
FOM Present      : 2003                 FOM Last upd.    : 2025
Number of Flaps  : 2                    Flags            : ud*i
Path             : 60203 65001 19855 3356  702   1889
Applied Policy   : default-damping-profile
-------------------------------------------------------------------------------
Paths : 1
===============================================================================
*A:ALA-12#
*A:ALA-12# show router 3 bgp damping suppressed detail
===============================================================================
  BGP Router ID : 10.0.0.14         AS : 65206   Local AS : 65206
===============================================================================
  Legend -
  Status codes  : u - used, s - suppressed, h - history, d - decayed, * - valid
  Origin codes  : i - IGP, e - EGP, ? - incomplete,  - best
===============================================================================
BGP Damped Routes (Suppressed)
===============================================================================
Network : 10.142.48.0/20
-------------------------------------------------------------------------------
Network          : 10.142.48.0/20       Peer             : 10.0.28.1
NextHop          : 10.0.28.1            Reuse time       : 00h29m22s
Peer AS          : 60203                Peer Router-Id   : 32.32.27.203
Local Pref       : none
Age              : 00h01m28s            Last update      : 02d01h20m
FOM Present      : 2936                 FOM Last upd.    : 3001
Number of Flaps  : 3                    Flags            : si
Path             : 60203 65001 19855 3356  702   1889
Applied Policy   : default-damping-profile
-------------------------------------------------------------------------------
Network : 10.200.128.0/19
-------------------------------------------------------------------------------
Network          : 10.200.128.0/19      Peer             : 10.0.28.1
NextHop          : 10.0.28.1            Reuse time       : 00h29m22s
Peer AS          : 60203                Peer Router-Id   : 32.32.27.203
Local Pref       : none
Age              : 00h01m28s            Last update      : 02d01h20m
FOM Present      : 2936                 FOM Last upd.    : 3001
Number of Flaps  : 3                    Flags            : si
Path             : 60203 65001 19855 3356  702   1889
Applied Policy   : default-damping-profile
-------------------------------------------------------------------------------
Network : 10.203.240.0/20
-------------------------------------------------------------------------------
Network          : 10.203.240.0/20      Peer             : 10.0.28.1
NextHop          : 10.0.28.1            Reuse time       : 00h29m22s
Peer AS          : 60203                Peer Router-Id   : 32.32.27.203
Local Pref       : none
Age              : 00h01m28s            Last update      : 02d01h20m
FOM Present      : 2936                 FOM Last upd.    : 3001
Number of Flaps  : 3                    Flags            : si
Path             : 60203 65001 19855 3356  702   1889
Applied Policy   : default-damping-profile
-------------------------------------------------------------------------------
```

```
Network : 10.206.0.0/17
-------------------------------------------------------------------------------
Network          : 10.206.0.0/17        Peer             : 10.0.28.1
NextHop          : 10.0.28.1            Reuse time       : 00h29m22s
Peer AS          : 60203                Peer Router-Id   : 32.32.27.203
Local Pref       : none
Age              : 00h01m28s            Last update      : 02d01h20m
FOM Present      : 2936                 FOM Last upd.    : 3001
Number of Flaps  : 3                    Flags            : si
Path             : 60203 65001 19855 3356  702   1889
Applied Policy   : default-damping-profile
-------------------------------------------------------------------------------
*A:ALA-12#
```

Table 111: Output fields: BGP damping

Label	Description
BGP Router ID	The local BGP router ID.
AS	The configured AS number.
Local AS	The configured or inherited local AS for the specified peer group. If not configured, it is the same value as the AS.
Network	Route IP prefix and mask length for the route.
Flags	Legend: Status codes: u- used, s-suppressed, h-history, d-decayed, *-valid. If a * is not present, then the status is invalid. Origin codes: i-IGP, e-EGP, ?-incomplete, >-best
Network	The IP prefix and mask length for the route.
From	The originator ID path attribute value.
Reuse time	The time when a suppressed route can be used again.
AS Path	The BGP AS path for the route.
Peer	The router ID of the advertising router.
NextHop	BGP next hop for the route.
Peer AS	The AS number of the advertising router.
Peer Router-Id	The router ID of the advertising router.
Local Pref	BGP local preference path attribute for the route.
Age	The time elapsed after the service was enabled.
Last update	The time when BGP was updated last in second/minute/hour (SS:MM:HH) format.
FOM Present	The current Figure of Merit (FOM) value.

Label	Description
Number of Flaps	The number of flaps in the neighbor connection.
Reuse time	The time when the route can be reused.
Path	The BGP AS path for the route.
Applied Policy	The applied route policy name.

group

Syntax

group [*name*] [**detail**]

Context

show>router>bgp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays group information for a BGP peer group. This command can be entered with or without parameters.

When this command is entered without a group name, information about all peer groups displays.

When the command is issued with a specific group name, only information pertaining to that specific peer group is displayed.

The "State" field displays the BGP group operational state. Other valid states are the following:

- **Up**

  BGP global process is configured and running.
- **Down**

  BGP global process is administratively shutdown and not running.
- **Disabled**

  BGP global process is operationally disabled. The process must be restarted by the operator.

Parameters

name

Displays information for the BGP group specified.

detail

Displays detailed information.

Output

The following output is an example of BGP peer group information, and Table 112: Output fields: BGP group describes the output fields.

Sample output

```
*A:ALA-12# show router 3 bgp group
===============================================================================
BGP Groups
===============================================================================
Group            : To_AS_40000
-------------------------------------------------------------------------------
Description      : Not Available
Group Type       : No Type              State            : Up
Peer AS          : 40000                Local AS         : 65206
Local Address    : n/a                  Loop Detect      : Ignore
Export Policy    : direct2bgp
Hold Time        : 90                   Keep Alive       : 30
Cluster Id       : None                 Client Reflect   : Enabled
NLRI             : Unicast              Preference       : 170

List of Peers
- 10.0.0.1       : To_Jukebox
- 10.0.0.12      : Not Available
- 10.0.0.13      : Not Available
- 10.0.0.14      : To_ALA-1
- 10.0.0.15      : To_H-215
Total Peers      : 5                    Established      : 2
===============================================================================
*A:ALA-12#
```

Table 112: Output fields: BGP group

Label	Description
Group	BGP group name.
Group Type	No Type Peer type not configured.
	External Peer type configured as external BGP peers.
	Internal Peer type configured as internal BGP peers.
State	Disabled The BGP peer group has been operationally disabled.
	Down The BGP peer group is operationally inactive.
	Up The BGP peer group is operationally active.

Label	Description
Peer AS	The configured or inherited peer AS for the specified peer group.
Local AS	The configured or inherited local AS for the specified peer group.
Local Address	The configured or inherited local address for originating peering for the specified peer group.
Loop Detect	The configured or inherited loop detect setting for the specified peer group.
Connect Retry	The configured or inherited connect retry timer value.
	Authentication
	None No authentication is configured.
	MD5 MD5 authentication is configured.
Local Pref	The configured or inherited local preference value.
MED Out	The configured or inherited MED value assigned to advertised routes without a MED attribute.
Min Route Advt.	The minimum amount of time that must pass between route updates for the same IP prefix.
Min AS Originate	The minimum amount of time that must pass between updates for a route originated by the local router.
Multihop	The maximum number of router hops a BGP connection can traverse.
Multipath	The configured or inherited multipath value, determining the maximum number of ECMP routes BGP can advertise to the RTM.
Prefix Limit	No Limit No route limit assigned to the BGP peer group.
	1 to 4294967295 The maximum number of routes BGP can learn from a peer.
Passive	Disabled BGP attempts to establish BGP connections with neighbors in the specified peer group.
	Enabled

Label	Description
	BGP does not actively attempt to establish BGP connections with neighbors in the specified peer group.
Next Hop Self	Disabled BGP is not configured to send only its own IP address as the BGP next hop in route updates to neighbors in the peer group.
	Enabled BGP sends only its own IP address as the BGP nexthop in route updates to neighbors in the specified peer group.
Aggregator ID 0	Disabled BGP is not configured to set the aggregator ID to 0.0.0.0 in all originated route aggregates sent to the neighbor in the peer group.
	Enabled BGP is configured to set the aggregator ID to 0.0.0.0 in all originated route aggregates sent to the neighbor in the peer group.
Remove Private	Disabled BGP does not remove all private AS numbers from the AS path attribute in updates sent to the neighbor in the peer group.
	Enabled BGP removes all private AS numbers from the AS path attribute in updates sent to the neighbor in the peer group.
Damping	Disabled The peer group is configured not to dampen route flaps.
	Enabled The peer group is configured to dampen route flaps.
Export Policy	The configured export policies for the peer group.
Import Policy	The configured import policies for the peer group.
Hold Time	The configured hold time setting.
Keep Alive	The configured keepalive setting.
Cluster Id	None No cluster ID has been configured.
Client Reflect	Disabled The BGP route reflector does not reflect routes to this neighbor.

Label	Description
	Enabled The BGP route reflector is configured to reflect routes to this neighbor.
NLRI	The type of NLRI information that the specified peer group can accept.
	Unicast IPv4 unicast routing information can be carried.
Preference	The configured route preference value for the peer group.
List of Peers	A list of BGP peers configured under the peer group.
Total Peers	The total number of peers configured under the peer group.
Established	The total number of peers that are in an established state.

neighbor

Syntax

neighbor [*ip-address* [[**family** *family*] *filter1*]]

neighbor [*as-number* [[**family** *family*] *filter2*]]

Context

show>router>bgp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays BGP neighbor information. This command can be entered with or without parameters. When this command is issued without parameters, information about all BGP peers displays.

When the command is issued with a specific IP address or ASN, only information for that specific peer or peers with the same AS is displayed.

When either **received-routes** or **advertised-routes** is specified, the routes received from or sent to the specified peer is listed (see second output example). This information is not available by SNMP.

When either **history** or **suppressed** is specified, the routes learned from those peers that either have a history or are suppressed (respectively) are listed.

The "State" field displays the BGP peer protocol state. In additional to the standard protocol states, this field can also display the "Disabled" operational state, which indicates the peer is operationally disabled and must be restarted by the operator.

Parameters

ip-addr

Displays the BGP neighbor with the specified IP address.

family *family*

Specifies the type of routing information to be distributed by the BGP instance.

Values ipv4, vpn-ipv4, ipv6, vpn-ipv6, l2-vpn, ms-pw

filter1

Specifies route criteria.

Values received-routes, advertised-routes, history, suppressed, detail

filter2

Specifies route criteria.

Values history, suppressed, detail

Output

The following outputs are examples of BGP neighbor information, and the associated tables describe the output fields.

- Sample output, Table 113: Output fields: BGP neighbor
- Sample output for received routes, Table 114: Output fields: neighbor received routes
- Sample output for BGP PIC
- Sample output for add-path

Sample output

```
*A:ALA-12# show router 3 bgp neighbor
===============================================================================
BGP Neighbor
===============================================================================
-------------------------------------------------------------------------------
Peer : 10.0.0.15         Group : To_AS_40000
-------------------------------------------------------------------------------
Peer AS          : 65205
Peer Address     : 10.0.0.15           Peer Port        : 0
Local AS         : 65206
Local Address    : 10.0.0.16           Local Port       : 0
Peer Type        : External
State            : Active              Last State       : Connect
Last Event       : openFail
Last Error       : Hold Timer Expire
Hold Time        : 90                  Keep Alive       : 30
Active Hold Time : 0                   Active Keep Alive: 0
Cluster Id       : None
Preference       : 170                 Num of Flaps     : 0
Recd. Prefixes   : 0                   Active Prefixes  : 0
Recd. Paths      : 0                   Suppressed Paths : 0
Input Queue      : 0                   Output Queue     : 0
i/p Messages     : 0                   o/p Messages     : 0
i/p Octets       : 0                   o/p Octets       : 0
i/p Updates      : 0                   o/p Updates      : 0
Export Policy    : direct2bgp
```

```
===============================================================================
*A:ALA-12#


*A:ALA-12# show router 3 bgp neighbor detail
===============================================================================
BGP Neighbor (detail)
===============================================================================
-------------------------------------------------------------------------------
Peer : 10.0.0.15         Group : To_AS_40000
-------------------------------------------------------------------------------
Peer AS          : 65205
Peer Address     : 10.0.0.15           Peer Port        : 0
Local AS         : 65206
Local Address    : 10.0.0.16           Local Port       : 0
Peer Type        : External
State            : Active              Last State       : Connect
Last Event       : openFail
Last Error       : Hold Timer Expire
Connect Retry    : 20                  Local Pref.      : 100
Min Route Advt.  : 30                  Min AS Orig.     : 15
Multipath        : 1                   Multihop         : 5
Damping          : Disabled            Loop Detect      : Ignore
MED Out          : No MED Out          Authentication   : None
Next Hop Self    : Disabled            AggregatorID Zero: Disabled
Remove Private   : Disabled            Passive          : Disabled
Prefix Limit     : No Limit
Hold Time        : 90                  Keep Alive       : 30
Active Hold Time : 0                   Active Keep Alive: 0
Cluster Id       : None                Client Reflect   : Enabled
Preference       : 170                 Num of Flaps     : 0
Recd. Prefixes   : 0                   Active Prefixes  : 0
Recd. Paths      : 0                   Suppressed Paths : 0
Input Queue      : 0                   Output Queue     : 0
i/p Messages     : 0                   o/p Messages     : 0
i/p Octets       : 0                   o/p Octets       : 0
i/p Updates      : 0                   o/p Updates      : 0
Export Policy    : direct2bgp

===============================================================================
*A:ALA-12#
```

Table 113: Output fields: BGP neighbor

Label	Description
Peer	The IP address of the configured BGP peer.
Group	The BGP peer group to which this peer is assigned.
Peer AS	The configured or inherited peer AS for the peer group.
Peer Address	The configured address for the BGP peer.
Peer Port	The TCP port number used on the far-end system.
Local AS	The configured or inherited local AS for the peer group.
Local Address	The configured or inherited local address for originating peering for the peer group.

Label	Description
Local Port	The TCP port number used on the local system.
Peer Type	External Peer type configured as external BGP peers.
	Internal Peer type configured as internal BGP peers.
State	Idle The BGP peer is not accepting connections.
	Active BGP is listening for and accepting TCP connections from this peer.
	Connect BGP is attempting to establish a TCP connection from this peer.
	Open Sent BGP has sent an OPEN message to the peer and is waiting for an OPEN message from the peer.
	Open Confirm BGP has received a valid OPEN message from the peer and is awaiting a KEEPALIVE or NOTIFICATION.
	Established BGP has successfully established a peering and is exchanging routing information.
Last State	Idle The BGP peer is not accepting connections.
	Active BGP is listening for and accepting TCP connections from this peer.
	Connect BGP is attempting to establish a TCP connection with this peer.
	Connect BGP is attempting to establish a TCP connections from this peer.
	Open Sent BGP has sent an OPEN message to the peer and is waiting for an OPEN message from the peer.

Label	Description
	Open Confirm BGP has received a valid OPEN message from the peer and is awaiting a KEEPALIVE or NOTIFICATION.
	Open Confirm BGP has received a valid OPEN message from the peer and is awaiting a KEEPALIVE or NOTIFICATION.
Last Event	start BGP has initialized the BGP neighbor.
	stop BGP has disabled the BGP neighbor.
	open BGP transport connection opened.
	close BGP transport connection closed.
	openFail BGP transport connection failed to open.
	error BGP transport connection error.
	connectRetry Connect retry timer expired.
	holdTime Hold time timer expired.
	keepAlive Keepalive timer expired.
	recvOpen Receive an OPEN message.
	revKeepalive Receive an KEEPALIVE message.
	recvUpdate Receive an UPDATE message.
	recvNotify Receive an NOTIFICATION message.

Label	Description
	None No events have occurred.
Last Error	Displays the last BGP error and sub-code to occur on the BGP neighbor.
Connect Retry	The configured or inherited connect retry timer value.
Local Pref.	The configured or inherited local preference value.
Min Route Advt.	The minimum amount of time that must pass between route updates for the same IP prefix.
Min AS Originate	The minimum amount of time that must pass between updates for a route originated by the local router.
Multihop	The maximum number of router hops a BGP connection can traverse.
Multipath	The configured or inherited multipath value, determining the maximum number of ECMP routes BGP can advertise to the RTM.
Damping	Disabled BGP neighbor is configured not to dampen route flaps.
	Enabled BGP neighbor is configured to dampen route flaps.
Loop Detect	Ignore The BGP neighbor is configured to ignore routes with an AS loop.
	Drop The BGP neighbor is configured to drop the BGP peering if an AS loop is detected.
	Off AS loop detection is disabled for the neighbor.
MED Out	The configured or inherited MED value assigned to advertised routes without a MED attribute.
Authentication	None No authentication is configured.
	MD5 MD5 authentication is configured.

Label	Description
Next Hop Self	Disabled BGP is not configured to send only its own IP address as the BGP next hop in route updates to the specified neighbor.
	Enabled BGP sends only its own IP address as the BGP next-hop in route updates to the neighbor.
AggregatorID Zero	Disabled The BGP Neighbor is not configured to set the aggregator ID to 0.0.0.0 in all originated route aggregates.
	Enabled The BGP Neighbor is configured to set the aggregator ID to 0.0.0.0 in all originated route aggregates.
Remove Private	Disabled BGP does not remove all private AS numbers from the AS path attribute, in updates sent to the specified neighbor.
	Enabled BGP removes all private AS numbers from the AS path attribute, in updates sent to the specified neighbor.
Passive	Disabled BGP actively attempts to establish a BGP connection with the specified neighbor.
	Enabled BGP does not actively attempt to establish a BGP connection with the specified neighbor.
Prefix Limit	No Limit No route limit assigned to the BGP peer group.
	1 to 4294967295 The maximum number of routes BGP can learn from a peer.
Hold Time	The configured hold time setting.
Keep Alive	The configured keepalive setting.
Active Hold Time	The negotiated hold time, if the BGP neighbor is in an established state.
Active Keep Alive	The negotiated keepalive time, if the BGP neighbor is in an established state.

Label	Description
Cluster Id	The configured route reflector cluster ID. None No cluster ID has been configured
Client Reflect	Disabled The BGP route reflector is configured not to reflect routes to this neighbor.
	Enabled The BGP route reflector is configured to reflect routes to this neighbor.
Preference	The configured route preference value for the peer group.
Num of Flaps	The number of flaps in the neighbor connection.
Recd. Prefixes	The number of routes received from the BGP neighbor.
Active Prefixes	The number of routes received from the BGP neighbor and active in the forwarding table.
Recd. Paths	The number of unique sets of path attributes received from the BGP neighbor.
Suppressed Paths	The number of unique sets of path attributes received from the BGP neighbor and suppressed because of route damping.
Input Queue	The number of BGP messages to be processed.
Output Queue	The number of BGP messages to be transmitted.
i/p Messages	Total number of packets received from the BGP neighbor.
o/p Messages	Total number of packets sent to the BGP neighbor.
i/p Octets	Total number of octets received from the BGP neighbor.
o/p Octets	Total number of octets sent to the BGP neighbor.
i/p Updates	Total number of BGP updates received from the BGP neighbor.
o/p Updates	Total number of BGP updates sent to the BGP neighbor.
Export Policy	The configured export policies for the peer group.
Import Policy	The configured import policies for the peer group.

Sample output for received routes

```
*A:ALA-12# show router 3 bgp neighbor 10.0.0.16 received-routes
===============================================================================
 BGP Router ID : 10.0.0.16         AS : 65206   Local AS : 65206
```

```
===============================================================================
 Legend -
 Status codes  : u - used, s - suppressed, h - history, d - decayed, * - valid
 Origin codes  : i - IGP, e - EGP, ? - incomplete, > - best
===============================================================================
BGP Neighbor
===============================================================================
Flag  Network            Nexthop         LocalPref  MED        As-Path
-------------------------------------------------------------------------------
?     10.0.0.16/32       10.0.0.16       100        none       No As-Path
?     10.0.6.0/24        10.0.0.16       100        none       No As-Path
?     10.0.8.0/24        10.0.0.16       100        none       No As-Path
?     10.0.12.0/24       10.0.0.16       100        none       No As-Path
?     10.0.13.0/24       10.0.0.16       100        none       No As-Path
?     10.0.204.0/24      10.0.0.16       100        none       No As-Path
===============================================================================
*A:ALA-12#
```

Table 114: Output fields: neighbor received routes

Label	Description
BGP Router ID	The local BGP router ID.
AS	The configured AS number.
Local AS	The configured local AS setting. If not configured, it is the same value as the AS.
Flag	u used
	s suppressed
	h history
	d decayed
	* valid
	i igp
	? incomplete
	> best

Label	Description
Network	Route IP prefix and mask length for the route.
Next Hop	BGP next hop for the route.
LocalPref	BGP local preference path attribute for the route.
MED	BGP Multi-Exit Discriminator (MED) path attribute for the route.
AS Path	The BGP AS path for the route.

Sample output for BGP PIC

```
*A:7210SAS>show>service>id# show  service id 1 base

===============================================================================
Service Basic Information
===============================================================================
Service Id        : 1                   Vpn Id            : 0
Service Type      : VPRN
Name              : (Not Specified)
Description       : Default Description For VPRN ID 1
Customer Id       : 1
Last Status Change: 01/08/2000 22:57:35
Last Mgmt Change  : 01/08/2000 22:57:35
Admin State       : Up                  Oper State        : Up

Route Dist.       : 100:1               VPRN Type         : regular
AS Number         : 100                 Router Id         : 1.1.1.1
ECMP              : Enabled             ECMP Max Routes   : 1
Max IPv4 Routes   : No Limit            Auto Bind         : MPLS
Max IPv6 Routes   : No Limit
Ignore NH Metric  : Disabled
Hash Label        : Disabled
Vrf Target        : target:200:1
Vrf Import        : None
Vrf Export        : None
MVPN Vrf Target   : None
MVPN Vrf Import   : None
MVPN Vrf Export   : None
Label mode        : vrf
BGP VPN Backup    : ipv4 ipv6

SAP Count         : 1                   SDP Bind Count    : 3

-------------------------------------------------------------------------------
Service Access & Destination Points
-------------------------------------------------------------------------------
Identifier                              Type         AdmMTU  OprMTU  Adm  Opr
-------------------------------------------------------------------------------
sap:1/1/2:1                             q-tag        9212    9212    Up   Up
sdp:1002:1 S(2.2.2.2)                   Spok         0       9186    Up   Up
sdp:1003:1 S(3.3.3.3)                   Spok         0       9186    Up   Up
sdp:1004:1 S(4.4.4.4)                   Spok         0       9186    Up   Up
===============================================================================
*A:7210SAS>show>service>id#
```

Sample output for add-path

```
*A:7210SAS# show  router bgp neighbor 2.2.2.2
```

```
===============================================================================
BGP Neighbor
===============================================================================
-------------------------------------------------------------------------------
Peer  : 2.2.2.2
Group : toPE
-------------------------------------------------------------------------------
Peer AS              : 100              Peer Port            : 50854
Peer Address         : 10.2.2.2
Local AS             : 100              Local Port           : 179
Local Address        : 10.1.1.1
Peer Type            : Internal
State                : Established      Last State           : Established
Last Event           : recvKeepAlive
Last Error           : Cease (Connection Collision Resolution)
Local Family         : IPv4 VPN-IPv4 IPv6 VPN-IPv6
Remote Family        : IPv4 VPN-IPv4 IPv6 VPN-IPv6
Hold Time            : 90               Keep Alive           : 30
Min Hold Time        : 0
Active Hold Time     : 90               Active Keep Alive    : 30
Cluster Id           : None
Preference           : 170              Num of Update Flaps  : 0
Recd. Paths          : 0
IPv4 Recd. Prefixes  : 0                IPv4 Active Prefixes : 0
IPv4 Suppressed Pfxs : 0                VPN-IPv4 Suppr. Pfxs : 0
VPN-IPv4 Recd. Pfxs  : 0                VPN-IPv4 Active Pfxs : 0
Mc IPv4 Recd. Pfxs.  : 0                Mc IPv4 Active Pfxs. : 0
Mc IPv4 Suppr. Pfxs  : 0                IPv6 Suppressed Pfxs : 0
IPv6 Recd. Prefixes  : 0                IPv6 Active Prefixes : 0
VPN-IPv6 Recd. Pfxs  : 0                VPN-IPv6 Active Pfxs : 0
VPN-IPv6 Suppr. Pfxs : 0                L2-VPN Suppr. Pfxs   : 0
L2-VPN Recd. Pfxs    : 0                L2-VPN Active Pfxs   : 0
MVPN-IPv4 Suppr. Pfxs: 0                MVPN-IPv4 Recd. Pfxs : 0
MVPN-IPv4 Active Pfxs: 0                MDT-SAFI Suppr. Pfxs : 0
MDT-SAFI Recd. Pfxs  : 0                MDT-SAFI Active Pfxs : 0
FLOW-IPV4-SAFI Suppr*: 0                FLOW-IPV4-SAFI Recd.*: 0
FLOW-IPV4-SAFI Activ*: 0                Rte-Tgt Suppr. Pfxs  : 0
Rte-Tgt Recd. Pfxs   : 0                Rte-Tgt Active Pfxs  : 0
Backup IPv4 Pfxs     : 0                Backup IPv6 Pfxs     : 0
Mc Vpn Ipv4 Recd. Pf*: 0                Mc Vpn Ipv4 Active P*: 0
Backup Vpn IPv4 Pfxs : 0                Backup Vpn IPv6 Pfxs : 0
Input Queue          : 0                Output Queue         : 0
i/p Messages         : 9042             o/p Messages         : 65
i/p Octets           : 111              o/p Octets           : 278
i/p Updates          : 0                o/p Updates          : 0
TTL Security         : Disabled         Min TTL Value        : n/a
Graceful Restart     : Disabled         Stale Routes Time    : n/a
Advertise Inactive   : Disabled         Peer Tracking        : Disabled
Advertise Label      : ipv4 ipv6
Auth key chain       : n/a
Disable Cap Nego     : Disabled         Bfd Enabled          : Enabled
Flowspec Validate    : Disabled         Default Route Tgt    : Disabled
L2 VPN Cisco Interop : Disabled
Local Capability     : RtRefresh MPBGP 4byte ASN
Remote Capability    : RtRefresh MPBGP 4byte ASN
Local AddPath Capabi*: Send - VPN-IPv4 (1) VPN-IPv6 (4)
                     : Receive - VPN-IPv6
Remote AddPath Capab*: Send - VPN-IPv6
                     : Receive - VPN-IPv4 VPN-IPv6
Import Policy        : None Specified / Inherited
Export Policy        : P1

-------------------------------------------------------------------------------
```

```
Neighbors : 1
===============================================================================
* indicates that the corresponding row element may have been truncated.
*A:7210SAS#
```

paths

Syntax

paths

Context

show>router>bgp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays a summary of BGP path attributes.

Output

The following output is an example of BGP path information, and Table 115: Output fields: BGP paths describes the output fields.

Sample output

```
*A:ALA-12# show router 3 bgp paths
===============================================================================
 BGP Router ID : 10.0.0.14         AS : 65206   Local AS : 65206
===============================================================================
BGP Paths
-------------------------------------------------------------------------------
Path: 60203 65001 19855 3356  15412
-------------------------------------------------------------------------------
Origin           : IGP                  Next Hop         : 10.0.28.1
MED              : 60203                Local Preference : none
Refs             : 4                    ASes             : 5
Segments         : 1
Flags            : EBGP-learned
Aggregator       : 15412  62.216.140.1
-------------------------------------------------------------------------------
Path: 60203 65001 19855 3356  1     1236  1236  1236  1236
-------------------------------------------------------------------------------
Origin           : IGP                  Next Hop         : 10.0.28.1
MED              : 60203                Local Preference : none
Refs             : 2                    ASes             : 9
Segments         : 1
Flags            : EBGP-learned
-------------------------------------------------------------------------------
*A:ALA-12#
```

Table 115: Output fields: BGP paths

Label	Description
BGP Router ID	The local BGP router ID.
AS	The configured autonomous system number.
Local AS	The configured local AS setting. If not configured, the value is the same as the AS.
Path	The AS path attribute.
Origin	EGP The NLRI is learned by an EGP protocol.
	IGP The NLRI is interior to the originating AS.
	INCOMPLETE NLRI was learned another way.
Next Hop	The advertised BGP next hop.
MED	The Multi-Exit Discriminator value.
Local Preference	The local preference value.
Refs	The number of routes using a specified set of path attributes.
ASes	The number of autonomous system numbers in the AS path attribute.
Segments	The number of segments in the AS path attribute.
Flags	eBGP-learned Path attributes learned by an eBGP peering.
	iBGP-Learned Path attributes learned by an iBGP peering.
Aggregator	The route aggregator ID.
Community	The BGP community attribute list.
Originator ID	The originator ID path attribute value.
Cluster List	The route reflector cluster list.

routes

Syntax

routes [**family** *family*] [*prefix* [**detail** | **longer**]]

routes [*family family*] [*prefix* [**hunt** | **brief**]]

routes [**family** *family*] [**community** *comm-id*]

routes [**family** *family*] [**aspath-regex** *reg-ex1*]

routes [**family** *family*] [*ipv6-prefix*[*/prefix-length*] [**detail** | **longer**] | [**hunt** [**brief**]]]

Context

show>router>bgp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays BGP route information.

When this command is issued without any parameters, the entire BGP routing table displays.

When this command is issued with an IP prefix/mask or IP address, the best match for the parameter displays.

Parameters

family *family*

Specifies the type of routing information to be distributed by the BGP instance.

Values **ipv4** — Displays only those BGP peers that have the IPv4 family enable and not those capable of exchanging IP-VPN routes.

vpn-ipv4 — Displays the BGP peers that are IP-VPN capable.

ipv6 — Displays the BGP peers that are IPv6 capable.

mcast-ipv4 — Displays the BGP peers that are mcast-ipv4 capable.

prefix

Specifies the type of routing information to display.

Values *rd*|[*rd*:]*ip-address*[/*mask*]

rd {ip-address:number1
as-number1:number2
as-number2:number3}

number1 1 to 65535

as-number1	1 to 65535
number2	0 to 4294967295
as-number2	1 to 4294967295
number3	0 to 65535
ip-address	a.b.c.d
mask	0 to 32

filter

Specifies route criteria.

Values **hunt —** Displays entries for the specified route in the RIB-In, RIB-Out, and RTM.

longer — Displays the specified route and subsets of the route.

detail — Display the longer, more detailed version of the output.

aspath-regex "*reg-exp*"

Displays all routes with an AS path matching the specified regular expression *reg-exp*.

community *comm.-id*

Displays all routes with the specified BGP community.

Values [*as-number1:comm-val1* | *ext-comm* | *well-known-comm*]

ext-comm	type:{ip-address:comm-val1 | as-number1:comm-val2 | as- number2:comm-val1}
as-number1	0 to 65535
comm-val1	0 to 65535
type	keywords: target, origin
ip-address	a.b.c.d
comm-val2	0 to 4294967295
as-number2	0 to 4294967295
well-known-comm	no-export, no-export-subconfed, no-advertise

Output

The following outputs are examples of BGP route information, and Table 116: Output fields: BGP routes describes the output fields.

Sample output

```
*A:ALA-12>config>router>bgp# show router 3 bgp routes family ipv4
===============================================================================
 BGP Router ID : 10.10.10.103      AS : 200     Local AS : 200
```

```
===============================================================================
 Legend -
 Status codes  : u - used, s - suppressed, h - history, d - decayed, * - valid
 Origin codes  : i - IGP, e - EGP, ? - incomplete, > - best
===============================================================================
BGP Routes
===============================================================================
Flag  Network                           Nexthop         LocalPref  MED
      VPN Label                         As-Path
-------------------------------------------------------------------------------
No Matching Entries Found
===============================================================================
*A:ALA-12>config>router>bgp#

A:SR-12# show router bgp routes 10.0.0.0/31 hunt
===============================================================================
 BGP Router ID : 10.20.1.1   AS : 100Local AS : 100
===============================================================================
 Legend -
 Status codes  : u - used, s - suppressed, h - history, d - decayed, * - valid
 Origin codes  : i - IGP, e - EGP, ? - incomplete, > - best
===============================================================================
BGP Routes
===============================================================================
RIB In Entries
-------------------------------------------------------------------------------
Network        : 10.0.0.0/31
Nexthop        : 10.20.1.2
Route Dist.    : 10.20.1.2:1VPN Label: 131070
From       : 10.20.1.2
Res. Nexthop   : 10.10.1.2
Local Pref.    : 100Interface Name: to-sr7
Aggregator AS  : noneAggregator: none
Atomic Aggr.   : Not AtomicMED: none
Community      : target:10.20.1.2:1
Cluster        : No Cluster Members
Originator Id  : NonePeer Router Id: 10.20.1.2
Flags       : Used  Valid  Best  IGP
AS-Path        : No As-Path
VPRN Imported  : 1 2 10 12
-------------------------------------------------------------------------------
RIB Out Entries
-------------------------------------------------------------------------------
Routes : 1
===============================================================================
A:SR-12#
```

Table 116: Output fields: BGP routes

Label	Description
BGP Router ID	The local BGP router ID.
AS	The configured AS number.
Local AS	The configured local AS setting; if not configured, it is the same as the system AS.
Network	The IP prefix and mask length.
Nexthop	The BGP next hop.

Label	Description
From	The advertising BGP neighbor IP address.
Res. Nexthop	The resolved next hop.
Local Pref.	The local preference value.
Flag	u used
	s suppressed
	h history
	d decayed
	* valid
	i igp
	e egp
	? incomplete
	> best
Aggregator AS	The aggregator AS value. none No aggregator AS attributes are present.
Aggregator	The aggregator attribute value. none no Aggregator attributes are present.
Atomic Aggr.	Atomic The atomic aggregator flag is set.
	Not Atomic The atomic aggregator flag is not set.

Label	Description
MED	The MED metric value. none No MED metric is present.
Community	The BGP community attribute list.
Cluster	The route reflector cluster list.
Originator Id	The originator ID path attribute value.
	none The originator ID attribute is not present.
Peer Router Id	The router ID of the advertising router.
AS-Path	The BGP AS path attribute.
VPRN Imported	Displays the VPRNs where a particular BGP-VPN received route has been imported and installed.

summary

Syntax

summary [**all**]

Context

show>router>bgp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays a summary of BGP neighbor information.

If confederations are not configured, that portion of the output does not display.

The "State" field displays the global BGP operational state. The valid values are:

- **Up**

  BGP global process is configured and running.
- **Down**

  BGP global process is administratively shutdown and not running.
- **Disabled**

  BGP global process is operationally disabled. The process must be restarted by the operator.

For example, if a BGP peer is operationally disabled, the state in the summary table displays the state "Disabled".

Parameters

all

Displays BGP peers in all instances.

Output

The following output is an example of summary BGP information, and Table 117: Output fields: BGP summary describes the output fields.

Sample output

```
*A:ALA-12# show router 3 bgp summary
===============================================================================
 BGP Router ID : 10.0.0.14         AS : 65206   Local AS : 65206
===============================================================================
 BGP Admin State         : Up            BGP Oper State       : Up
 Confederation AS        : 40000
 Member Confederations   : 65205 65206 65207 65208

 Number of Peer Groups   : 2             Number of Peers      : 7
 Total BGP Active Routes : 86689         Total BGP Routes     : 116999
 Total BGP Paths         : 35860         Total Path Memory    : 2749476
 Total Supressed Routes  : 0             Total History Routes : 0
 Total Decayed Routes    : 0
===============================================================================
BGP Summary
===============================================================================
Neighbor           AS PktRcvd PktSent InQ OutQ   Up/Down State|Recv/Actv/Sent
-------------------------------------------------------------------------------
10.0.0.1        65206       5   21849   0    0 00h01m29s 32/0/86683
10.0.0.12       65206       0       0   0    0 00h01m29s Active
10.0.0.13       65206       5   10545   0   50 00h01m29s 6/0/86683
10.0.0.15       65205       0       0   0    0 00h01m29s Active
10.0.0.16       65206       5    9636   0   50 00h01m29s 6/0/86683
10.0.27.1           2       0       0   0    0 00h01m29s Active
10.0.28.1       60203   22512      15   0    0 00h01m29s 116955/86689/9
===============================================================================
*A:ALA-12#
```

Table 117: Output fields: BGP summary

Label	Description
BGP Router ID	The local BGP router ID.
AS	The configured autonomous system number.
Local AS	The configured local AS setting, if not configured it is the same as the system AS.
BGP Admin State	Down BGP is administratively disabled.
	Up

Label	Description
	BGP is administratively enabled.
BGP Oper State	Down BGP is operationally disabled.
	Up BGP is operationally enabled.
Confederation AS	The configured confederation AS.
Member Confederations	The configured members of the BGP confederation.
Number of Peer Groups	The total number of configured BGP peer groups.
Number of Peers	The total number of configured BGP peers.
Total BGP Active Routes	The total number of BGP routes used in the forwarding table.
Total BGP Routes	The total number of BGP routes learned from BGP peers.
Total BGP Paths	The total number of unique sets of BGP path attributes learned from BGP peers.
Total Path Memory	Total amount of memory used to store the path attributes.
Total Suppressed Routes	Total number of suppressed routes because of route damping.
Total History Routes	Total number of routes with history because of route damping.
Total Decayed Routes	Total number of decayed routes because of route damping.
Neighbor	BGP neighbor address.
AS (Neighbor)	BGP neighbor AS number.
PktRcvd	Total number of packets received from the BGP neighbor.
PktSent	Total number of packets sent to the BGP neighbor.
InQ	The number of BGP messages to be processed.
OutQ	The number of BGP messages to be transmitted.
Up/Down	The amount of time that the BGP neighbor has either been established or not established depending on its current state.

Label	Description
State|Recv/Actv/Sent	The BGP neighbor current state (if not established) or the number of received routes, active routes and sent routes (if established).

interface

Syntax

interface [{[*ip-address* | *ip-int-name*] [**detail**]} | **summary**]

Context

show>router

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays the router IP interface table sorted by interface index.

Parameters

ip-address

Displays only the interface information associated with the specified IP address.

ip-int-name

Displays only the interface information associated with the specified IP interface name.

detail

Displays detailed IP interface information.

summary

Displays summary IP interface information for the router.

Output

The following outputs are examples of router interface information, and the associated tables describe the output fields.

- Sample output — detailed, Table 118: Output fields: IP interface
- Sample output — standard, Table 119: Output fields: IP interface standard
- Sample output — summary, Table 120: Output fields: router IP interface summary

Sample output — detailed

```
*A:ALA-12# show router 3 interface detail
===============================================================================
Interface Table
===============================================================================
Interface
```

```
-------------------------------------------------------------------------------
If Name      : to-ser1
Admin State  : Up                                Oper State       : Up

IP Addr/mask : 10.10.13.3/24                     Address Type     : Primary
IGP Inhibit  : Disabled                          Broadcast Address: Host-ones

IP Addr/mask : 10.200.0.1/16                     Address Type     : Secondary
IGP Inhibit  : Enabled                           Broadcast Address: Host-ones
-------------------------------------------------------------------------------
Details
-------------------------------------------------------------------------------
If Index     : 2
Port Id     : 1/1/2                              If Type          : Network
Egress Filter: none                              Ingress Filter   : 100
QoS Policy   : 1                                 SNTP Broadcast   : False
MAC Address  : 04:5d:01:01:00:02                 Arp Timeout      : 14400

ICMP Details
Redirects    : Disabled
Unreachables : Number - 100                     Time (seconds)   - 10
TTL Expired  : Number - 100                     Time (seconds)   - 10
===============================================================================
*A:ALA-12#
```

Table 118: Output fields: IP interface

Label	Description
If Name	The IP interface name.
Admin State	Down — The IP interface is administratively disabled. Up — The IP interface is administratively enabled.
Oper State	Down — The IP interface is operationally disabled. Up — The IP interface is operationally disabled.
IP Addr/mask	The IP address and subnet mask length of the IP interface. Not Assigned — Indicates no IP address has been assigned to the IP interface.
Address Type	Primary — The IP address for the IP interface is the Primary address on the IP interface. Secondary — The IP address for the IP interface is a Secondary address on the IP interface.
IGP Inhibit	Disabled — The secondary IP address on the interface is recognized as a local interface by the IGP. Enabled — The secondary IP address on the interface is not recognized as a local interface by the IGP.
Broadcast Address	All-ones — The broadcast format on the IP interface is all ones. Host-ones — The broadcast format on the IP interface is host ones.

Label	Description
If Index	The interface index of the IP router interface.
If Type	Network — The IP interface is a network/core IP interface. Service — The IP interface is a service IP interface.
Port Id	The port ID of the IP interface.
Egress Filter	The egress IP filter policy ID associated with the IP interface. none — Indicates no egress filter policy is associated with the interface.
Ingress Filter	The ingress IP filter policy ID associated with the IP interface. none — Indicates no ingress filter policy is associated with the interface.
QoS Policy	The QoS policy ID associated with the IP interface.
SNTP Broadcast	False — Receipt of SNTP broadcasts on the IP interface is disabled. True — Receipt of SNTP broadcasts on the IP interface is enabled.
MAC Address	The MAC address of the IP interface.
Arp Timeout	The ARP timeout for the interface, in seconds, which is the time an ARP entry is maintained in the ARP cache without being refreshed.
ICMP Mask Reply	False — The IP interface does not reply to a received ICMP mask request. True — The IP interface replies to a received ICMP mask request.
Redirects	Specifies the maximum number of ICMP redirect messages the IP interface issues in a specific period of time (Time (seconds)). Disabled — Indicates the IP interface does not generate ICMP redirect messages.
Unreachables	Specifies the maximum number of ICMP destination unreachable messages the IP interface issues in a specific period of time. Disabled — Indicates the IP interface does not generate ICMP destination unreachable messages.
TTL Expired	The maximum number (Number) of ICMP TTL expired messages the IP interface issues in a specific period of time (Time (seconds)).

Label	Description
	Disabled — Indicates the IP interface does not generate ICMP TTL expired messages.

Sample output — standard

```
*A:7210SAS>show>router interface i1 detail
===============================================================================
Interface Table (Router: Base)
===============================================================================

-------------------------------------------------------------------------------
Interface
-------------------------------------------------------------------------------
If Name      : i1
Admin State  : Up                                Oper (v4/v6)     : Down/--
Protocols    : None

IP Addr/mask : Not Assigned
-------------------------------------------------------------------------------
Details
-------------------------------------------------------------------------------
Description  : (Not Specified)
If Index     : 2                                 Virt. If Index   : 2
Last Oper Chg: 03/07/2001 01:47:29               Global If Index  : 127
Port Id      : 1/1/1
TOS Marking  : Trusted                           If Type          : Network
Egress Filter: none                              Ingress Filter   : none
Egr IPv6 Flt : none                              Ingr IPv6 Flt    : none
SNTP B.Cast  : False                             QoS Policy       : 2
Queue-group  : None
MAC Address  : 00:25:ba:0d:27:32                 Arp Timeout      : 14400
IP Oper MTU  : 9198
LdpSyncTimer : None                              Strip-Label      : Disabled
uRPF Chk     : disabled
uRPF Fail By*: 0                                 uRPF Chk Fail Pk*: 0

ICMP Details
Redirects    : Number - 100                      Time (seconds)   - 10
Unreachables : Number - 100                      Time (seconds)   - 10
TTL Expired  : Number - 100                      Time (seconds)   - 10

===============================================================================
Meter Statistics
===============================================================================

-------------------------------------------------------------------------------
                         Packets                 Octets
-------------------------------------------------------------------------------
Ingress Meter 1 (Unicast)
For. InProf           : 0                        0
For. OutProf          : 0                        0
Ingress Meter 9 (Multipoint)
For. InProf           : 0                        0
For. OutProf          : 0                        0
===============================================================================
===============================================================================
* indicates that the corresponding row element may have been truncated.
*A:7210SAS>show>router#
```

Table 119: Output fields: IP interface standard

Label	Description
Interface-Name	The IP interface name.
Type	n/a — No IP address has been assigned to the IP interface, so the IP address type is not applicable. Pri — The IP address for the IP interface is the Primary address on the IP interface. Sec — The IP address for the IP interface is a secondary address on the IP interface.
IP-Address	The IP address and subnet mask length of the IP interface. n/a — Indicates no IP address has been assigned to the IP interface.
Adm	Down — The IP interface is administratively disabled. Up — The IP interface is administratively enabled.
Opr	Down — The IP interface is operationally disabled. Up — The IP interface is operationally enabled.
Mode	Network — The IP interface is a network/core IP interface. Service — The IP interface is a service IP interface.

Sample output — summary

```
*A:ALA-12# show router 3 interface summary
===============================================================================
Router Summary (Interfaces)
===============================================================================
Instance  Router Name                     Interfaces    Admin-Up   Oper-Up
-------------------------------------------------------------------------------
1         Base                            7             7          5
===============================================================================
*A:ALA-12#
```

Table 120: Output fields: router IP interface summary

Label	Description
Instance	The router instance number.
Router Name	The name of the router instance.
Interfaces	The number of IP interfaces in the router instance.

mvpn

Syntax

mvpn

Context

show>router

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays multicast VPN related information. The router instance must be specified.

Output

The following output is an example of MVPN information, and Table 121: Output fields: MVPN describes the output fields.

Sample output

```
*A:Dut-y# show router 10 mvpn

===============================================================================
MVPN 10 configuration data
===============================================================================
signaling : Bgp auto-discovery : Default
UMH Selection : Highest-Ip intersite-shared : Enabled
vrf-import : N/A
vrf-export : N/A
vrf-target : unicast
C-Mcast Import RT : target:16.16.16.16:3

ipmsi : ldp
i-pmsi P2MP AdmSt : Up

spmsi : ldp
s-pmsi P2MP AdmSt : Up
max-p2mp-spmsi : 251
data-delay-interval: 3 seconds
enable-asm-mdt : N/A
data-threshold : 224.0.0.0/4 --> 1 kbps

===============================================================================
*A:Dut-y#
```

Table 121: Output fields: MVPN

Label	Description
signaling	Displays the signaling type.
UMH Selection	Displays the UMH selection method.

Label	Description
vrf-import	Displays the VRF import policy in use.
vrf-export	Displays the VRF export policy in use.
vrf-target	Displays the VRF target.
C-Mcast Import RT	Displays the c-multicast import router PE system address or loopback address. This address is common for all VPNs on the PE.
ipmsi	Displays the signaling protocol used to setup the I-PMSI tree transport tunnel.
i-pmsi P2MP AdmSt	Displays I-PMSI P2MP administrative state.
spmsi	Displays signaling protocol used to setup the S-PMSI tree transport tunnel.
s-pmsi P2MP AdmSt	Displays the S-PMSI P2MP administrative state.
max-p2mp-spmsi	Displays the maximum number of P2MP S-PMSIs.
data-delay-interval	Displays the interval, in seconds, before a PE router connected to the source switches traffic from the inclusive provider tunnel to the selective provider tunnel.
enable-asm-mdt	Displays whether ASM MDT is enabled.
data-threshold	Displays the data threshold.

mvpn-list

Syntax

mvpn-list [**type** *type*] [**auto-discovery** *auto-discovery*] [**signalling** *signalling*] [**group** *group*]

Context

show>router

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays multicast VPN list-related information. The router instance must be specified.

Parameters

type

Specifies the MVPN type.

Values pim, rsvp, ldp

auto-discovery

Specifies the auto-discovery mode.

Values none, default, mdt-safi

signalling

Specifies the signaling type.

Values bgp, pim

group

Specifies the group address.

Values grp-address

Output

The following output is an example of multicast VPN list information, and Table 122: Output fields: MVPN list describes the output fields.

Sample output

```
*A:Dut-y# show router mvpn-list

===============================================================================
MVPN List
===============================================================================
VprnID Sig A-D iPmsi/sPmsi GroupAddr/Lsp-Template (S,G)/(*,G)
-------------------------------------------------------------------------------
10 Bgp Default Mldp/Mldp N/A 512/0
20 Bgp Default Mldp/Mldp N/A 512/0
30 Bgp Default None/None N/A 0/0
-------------------------------------------------------------------------------
Total PIM I-PMSI tunnels : 0
Total RSVP I-PMSI tunnels : 0
Total MLDP I-PMSI tunnels : 2
Total PIM TX S-PMSI tunnels : 0
Total RSVP TX S-PMSI tunnels : 0
Total MLDP TX S-PMSI tunnels : 502
Total PIM RX S-PMSI tunnels : 0
Total RSVP RX S-PMSI tunnels : 0
Total MLDP RX S-PMSI tunnels : 0
Total (S,G) : 1024
Total (*,G) : 0
Total Mvpns : 3
Sig = Signal Pim-a = pim-asm Pim-s = pim-ssm A-D = Auto-Discovery
===============================================================================
*A:Dut-y#
```

Table 122: Output fields: MVPN list

Label	Description
Total PIM I-PMSI tunnels	Displays the total number of PIM I-PMSI tunnels.
Total RSVP I-PMSI tunnels	Displays the total number of RSVP I-PMSI tunnels.
Total MLDP I-PMSI tunnels	Displays the total number of MLDP I-PMSI tunnels.
Total PIM TX I-PMSI tunnels	Displays the total number of PIM I-PMSI transmit tunnels.
Total RSVP TX I-PMSI tunnels	Displays the total number of RSVP I-PMSI transmit tunnels.
Total MLDP TX I-PMSI tunnels	Displays the total number of MLDP I-PMSI transmit tunnels.
Total PIM RX I-PMSI tunnels	Displays the total number of PIM I-PMSI receive tunnels.
Total RSVP RX I-PMSI tunnels	Displays the total number of RSVP I-PMSI receive tunnels.
Total MLDP RX I-PMSI tunnels	Displays the total number of MLDP I-PMSI receive tunnels.
Total (S,G)	Displays the total number of (S,G) multicast groups.
Total (*,G)	Displays the total number of (*,G) multicast groups.
Total Mvpns	Displays the total number of MVPNs.

route-table

Syntax

route-table [*ip-prefix* [*lmask*] [**longer**] | [**protocol** *protocol*] | [**summary**]]

Context

show>router

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays the active routes in the routing table.

If no command line arguments are specified, all routes are displayed, sorted by prefix.

Parameters

***ip-prefix*[/*mask*]**

Displays routes only matching the specified *ip-prefix* and optional *mask*.

longer

Displays routes matching the *ip-prefix*/*mask* and routes with longer masks.

protocol *protocol*

Displays routes learned from the specified protocol.

Values bgp, isis, local, ospf, rip, static, aggregate

summary

Displays route table summary information.

Output

The following output is an example of route table information, and Table 123: Output fields: route table describes the output fields.

Sample output

```
*A:ALA-12# show router 3 route-table
===============================================================================
Route Table
===============================================================================
Dest Address       Next Hop        Type    Protocol    Age       Metric  Pref
-------------------------------------------------------------------------------
10.10.0.1/32       10.10.13.1      Remote  OSPF        65844     1001    10
10.10.0.2/32       10.10.13.1      Remote  OSPF        65844     2001    10
10.10.0.3/32       0.0.0.0         Local   Local       1329261   0       0
10.10.0.4/32       10.10.34.4      Remote  OSPF        3523      1001    10
10.10.0.5/32       10.10.35.5      Remote  OSPF        1084022   1001    10
10.10.12.0/24      10.10.13.1      Remote  OSPF        65844     2000    10
10.10.13.0/24      0.0.0.0         Local   Local       65859     0       0
10.10.15.0/24      10.10.13.1      Remote  OSPF        58836     2000    10
10.10.24.0/24      10.10.34.4      Remote  OSPF        3523      2000    10
10.10.25.0/24      10.10.35.5      Remote  OSPF        399059    2000    10
10.10.34.0/24      0.0.0.0         Local   Local       3543      0       0
10.10.35.0/24      0.0.0.0         Local   Local       1329259   0       0
10.10.45.0/24      10.10.34.4      Remote  OSPF        3523      2000    10
10.200.0.0/16      0.0.0.0         Local   Local       4513      0       0
192.168.0.0/20     0.0.0.0         Local   Local       1329264   0       0
192.168.254.0/24   0.0.0.0         Remote  Static      11        1       5
-------------------------------------------------------------------------------
*A:ALA-12#


*A:ALA-12# show router 3 route-table 10.10.0.4
===============================================================================
Route Table
===============================================================================
Dest Address       Next Hop        Type    Protocol    Age       Metric  Pref
-------------------------------------------------------------------------------
```

```
10.10.0.4/32       10.10.34.4      Remote  OSPF        3523      1001    10
-------------------------------------------------------------------------------
*A:ALA-12#


*A:ALA-12# show router 3 route-table 10.10.0.4/32 longer
===============================================================================
Route Table
===============================================================================
Dest Address       Next Hop        Type    Protocol    Age       Metric  Pref
-------------------------------------------------------------------------------
10.10.0.4/32       10.10.34.4      Remote  OSPF        3523      1001    10
-------------------------------------------------------------------------------
No. of Routes: 1
===============================================================================
+ : indicates that the route matches on a longer prefix
*A:ALA-12#


*A:ALA-12# show router 3 route-table protocol ospf
===============================================================================
Route Table
===============================================================================
Dest Address       Next Hop        Type    Protocol    Age       Metric  Pref
-------------------------------------------------------------------------------
10.10.0.1/32       10.10.13.1      Remote  OSPF        65844     1001    10
10.10.0.2/32       10.10.13.1      Remote  OSPF        65844     2001    10
10.10.0.4/32       10.10.34.4      Remote  OSPF        3523      1001    10
10.10.0.5/32       10.10.35.5      Remote  OSPF        1084022   1001    10
10.10.12.0/24      10.10.13.1      Remote  OSPF        65844     2000    10
10.10.15.0/24      10.10.13.1      Remote  OSPF        58836     2000    10
10.10.24.0/24      10.10.34.4      Remote  OSPF        3523      2000    10
10.10.25.0/24      10.10.35.5      Remote  OSPF        399059    2000    10
10.10.45.0/24      10.10.34.4      Remote  OSPF        3523      2000    10
-------------------------------------------------------------------------------
*A:ALA-12#


*A:ALA-12# show router 3 route-table summary
===============================================================================
Route Table Summary
===============================================================================
                              Active                  Available
-------------------------------------------------------------------------------
Static                        1                       1
Direct                        6                       6
BGP                           0                       0
OSPF                          9                       9
ISIS                          0                       0
RIP                           0                       0
Aggregate                     0                       0
-------------------------------------------------------------------------------
Total                         15                      15
===============================================================================
*A:ALA-12#
```

Table 123: Output fields: route table

Label	Description
Dest Address	The route destination address and mask.

Label	Description
Next Hop	The next-hop IP address for the route destination.
Type	Local — The route is a local route. Remote — The route is a remote route.
Protocol	The protocol through which the route was learned.
Age	The age, in seconds, for the route.
Metric	The metric value for the route.
Pref	The preference value for the route.
No. of Routes	The number of routes displayed in the list.

static-arp

Syntax

static-arp [*ip-address* | *ip-int-name* | **mac** *ieee-mac-addr*]

Context

show>router

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays the router static ARP table sorted by IP address.

If no options are present, all ARP entries are displayed.

Parameters

ip-address

Displays only static ARP entries associated with the specified IP address.

ip-int-name

Displays only static ARP entries associated with the specified IP interface name.

mac *ieee-mac-addr*

Displays only static ARP entries associated with the specified MAC address.

Output

The following output is an example of static ARP table information, and Table 124: Output fields: ARP table describes the output fields.

Sample output

```
*A:ALA-12# show router 3 static-arp
===============================================================================
ARP Table
===============================================================================
IP Address      MAC Address       Age      Type Interface
-------------------------------------------------------------------------------
10.200.0.253    00:00:5a:40:00:01 00:00:00 Sta  to-ser1
10.200.1.1      00:00:5a:01:00:33 00:00:00 Inv  to-ser1a
-------------------------------------------------------------------------------
No. of ARP Entries: 2
===============================================================================
*A:ALA-12#


*A:ALA-12# show router 3 static-arp 10.200.1.1
===============================================================================
ARP Table
===============================================================================
IP Address    MAC Address        Age     Type Interface
-------------------------------------------------------------------------------

10.200.1.1      00:00:5a:01:00:33  00:00:00 Inv   to-ser1  a

===============================================================================
*A:ALA-12#

*A:ALA-12# show router 3 static-arp to-ser1
===============================================================================
ARP Table
===============================================================================
IP Address    MAC Address       Age      Type Interface
-------------------------------------------------------------------------------
10.200.0.253  00:00:5a:40:00:01 00:00:00 Sta  to-ser1
===============================================================================
S*A:ALA-12#

*A:ALA-12# show router 3 static-arp mac 00:00:5a:40:00:01
===============================================================================
ARP Table
===============================================================================
IP Address    MAC Address       Age      Type Interface
-------------------------------------------------------------------------------
10.200.0.253  00:00:5a:40:00:01 00:00:00 Sta  to-ser1
===============================================================================
*A:ALA-12#
```

Table 124: Output fields: ARP table

Label	Description
IP Address	The IP address of the static ARP entry.
MAC Address	The MAC address of the static ARP entry.
Age	The age of the ARP entry. Static ARPs always have 00:00:00 for the age.
Type	Inv — The ARP entry is an inactive static ARP entry (invalid).

Label	Description
	Sta — The ARP entry is an active static ARP entry.
Interface	The IP interface name associated with the ARP entry.
No. of ARP Entries	The number of ARP entries displayed in the list.

static-route

Syntax

static-route [*ip-prefix Imask*] | [**preference** *preference*] | [**next-hop** *ip-addr* | **tag** *tag*] [**detail**]

Context

show>router

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays the static entries in the routing table.

If no options are present, all static routes are displayed sorted by prefix.

Parameters

ip-prefix Imask

Displays only static routes matching the specified *ip-prefix* and *mask*.

preference *preference*

Displays only static routes with the specified route preference.

Values 0 to 65535

next-hop *ip-addr*

Displays only static routes with the specified next hop IP address.

detail

Displays detailed information about the static route.

tag

Displays the tag used to add a 32-bit integer tag to the static route. The tag is used in route policies to control distribution of the route into other protocols.

Values 1 to 4294967295

Output

The following output is an example of static routing table entry information, and Table 125: Output fields: static route table describes the output fields.

Sample output

```
*A:ALA-12# show router 3 static-route
===============================================================================
Route Table
===============================================================================
IP Addr/mask       Pref Metric Type Nexthop              Interface       Active
-------------------------------------------------------------------------------
192.168.250.0/24   5    1      ID   10.200.10.1          to-ser1         Y
192.168.252.0/24   5    1      NH   10.10.0.254          n/a             N
192.168.253.0/24   5    1      NH   to-ser1              n/a             N
192.168.253.0/24   5    1      NH   10.10.0.254          n/a             N
192.168.254.0/24   4    1      BH   black-hole           n/a             Y
===============================================================================
*A:ALA-12#


*A:ALA-12# show router 3 static-route 192.168.250.0/24
===============================================================================
Route Table
===============================================================================
IP Addr/mask       Pref Metric Type Nexthop              Interface       Active
-------------------------------------------------------------------------------
192.168.250.0/24   5    1      ID   10.200.10.1          to-ser1         Y
===============================================================================
*A:ALA-12#


*A:ALA-12# show router 3 static-route preference 4
===============================================================================
Route Table
===============================================================================
IP Addr/mask       Pref Metric Type Nexthop              Interface       Active
-------------------------------------------------------------------------------
192.168.254.0/24   4    1      BH   black-hole           n/a             Y
===============================================================================
*A:ALA-12#


*A:ALA-12# show router 3 static-route next-hop 10.10.0.254
===============================================================================
Route Table
===============================================================================
IP Addr/mask       Pref Metric Type Nexthop              Interface       Active
-------------------------------------------------------------------------------
192.168.253.0/24   5    1      NH   10.10.0.254          n/a             N
===============================================================================
*A:ALA-12#

*A:Dut-B# show router static-route

===============================================================================
Static Route Table (Router: Base)  Family: IPv4
===============================================================================
Prefix                                    Tag         Met    Pref Type Act
   Next Hop                                Interface
-------------------------------------------------------------------------------
10.2.3.4/32                               0           1      5    NH   Y
   10.11.25.6
ip-10.11.25.5_base_to_cpe_static
10.11.15.0/24                             0           1      5    NH   Y
   10.11.25.6
ip-10.11.25.5_base_to_cpe_static
-------------------------------------------------------------------------------
```

```
No. of Static Routes: 2
===============================================================================


*A:Dut-B# show router static-route detail
===============================================================================
Static Route Table (Router: Base)  Family: IPv4
===============================================================================
Network          : 10.2.3.4/32
Nexthop          : 10.11.25.6
Type             : Nexthop                          Nexthop Type      : IP
Interface        : ip-10.11.25.5_base_to_cpe_stat*  Active            : Y
Metric           : 1                                Preference        : 5
Admin  State     : Up                               Tag               : 0
BFD              : disabled
CPE-check        : enabled                          State             : n/a
Target           : 10.11.18.6
Interval         : 1                                Drop Count        : 3
Log              : N
CPE Host Up Time : 0d 00:00:02
CPE Echo Req Tx  : 3                                CPE Echo Reply Rx : 3
CPE Up Trans     : 1                                CPE Down Trans    : 0
CPE TTL          : 2
-------------------------------------------------------------------------------
Network          : 10.11.15.0/24
Nexthop          : 10.11.25.6
Type             : Nexthop                          Nexthop Type      : IP
Interface        : ip-10.11.25.5_base_to_cpe_stat*  Active            : Y
Metric           : 1                                Preference        : 5
Admin  State     : Up                               Tag               : 0
BFD              : disabled
CPE-check        : disabled
-------------------------------------------------------------------------------
No. of Static Routes: 2

===============================================================================
```

Table 125: Output fields: static route table

Label	Description
IP Addr/mask	The static route destination address and mask.
Pref	The route preference value for the static route.
Metric	The route metric value for the static route.
Type	BH — The static route is a blackhole route. The next hop for this type of route is black hole. ID — The static route is an indirect route, where the next hop for this type of route is the non-directly connected next hop. NH — The route is a static route with a directly connected next hop. The next hop for this type of route is either the next-hop IP address or an egress IP interface name.
Next Hop	The next hop for the static route destination.
Interface	The egress IP interface name for the static route.

Label	Description
	n/a — indicates there is no current egress interface because the static route is inactive or a blackhole route.
Active	N — The static route is inactive; for example, the static route is disabled or the next hop IP interface is down. Y — The static route is active.
No. of Routes	The number of routes displayed in the list.

tunnel-table

Syntax

tunnel-table [*ip-address*[*/mask*] [**protocol** *protocol* | **sdp** *sdp-id*]

tunnel-table [**summary**]

Context

show>router

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays tunnel table information.

When the **auto-bind** command is used when configuring a VPRN service, it means the MP-BGP NH resolution is referring to core routing instance for IP reachability. For a VPRN service, this object specifies the lookup to be used by the routing instance, if no SDP to the destination exists.

Parameters

ip-address[/mask]

Displays the specified tunnel table destination IP address and mask.

protocol *protocol*

Displays LDP protocol information.

sdp *sdp-id*

Displays information pertaining to the specified SDP.

summary

Displays summary tunnel table information.

Output

The following output is an example of tunnel table information, and Table 126: Output fields: tunnel table describes the output fields.

Sample output

```
*A:ALA-12>config>service#  show router 3 tunnel-table summary
===============================================================================
Tunnel Table Summary (Router: Base)
===============================================================================
                            Active                  Available
-------------------------------------------------------------------------------
LDP                         1                       1
SDP                         1                       1
===============================================================================
*A:ALA-12>config>service#
```

Table 126: Output fields: tunnel table

Label	Description
Destination	The route destination address and mask.
Owner	Specifies the tunnel owner.
Encap	Specifies the tunnel encapsulation type.
Tunnel ID	Specifies the tunnel (SDP) identifier.
Pref	Specifies the route preference for routes learned from the configured peers.
Nexthop	The next hop for the route destination.
Metric	The route metric value for the route.

7.4.2.3 Clear commands

interface

Syntax

interface [*ip-int-name* | *ip-addr*] [**icmp**]

Context

clear>router

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command clears IP interface statistics.

If no IP interface is specified, either by IP interface name or IP address, the command performs the clear operation on all IP interfaces.

Parameters

ip-int-name* | *ip-addr

Specifies the IP interface name or IP interface address.

Default All IP interfaces.

icmp

Keyword that specifies to reset the ICMP statistics for the IP interfaces used for ICMP rate limit.

damping

Syntax

damping [[*ip-prefixlmask*] [**neighbor** *ip-address*]] | [**group** *name*]

Context

clear>router>bgp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command clears or resets the route damping information for received routes.

Parameters

ip-prefix/mask

Clears damping information for entries that match the IP prefix and mask length.

neighbor *ip-address*

Clears damping information for entries received from the BGP neighbor.

group *name*

Clears damping information for entries received from any BGP neighbors in the peer group.

flap-statistics

Syntax

flap-statistics [[*ip-prefixlmask*] [**neighbor** *ip-addr*]] | [**group** *group-name*] | [**regex** *reg-exp*] | [**policy** *policy-name*]

Context

clear>router>bgp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command clears route flap statistics.

Parameters

ip-prefix/mask

Clears route flap statistics for entries that match the specified IP prefix and mask length.

neighbor *ip-addr*

Clears route flap statistics for entries received from the specified BGP neighbor.

group *group-name*

Clears route flap statistics for entries received from any BGP neighbors in the specified peer group.

regex *reg-exp*

Clears route flap statistics for all entries that have the regular expression and the AS path that matches the regular expression.

policy *policy-name*

Clears route flap statistics for entries that match the specified route policy.

neighbor

Syntax

neighbor {*ip-addr* | **as** *as-number* | **external** | **all**} [**soft** | **soft-inbound** | **statistics**]

Context

clear>router>bgp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command resets the specified BGP peer or peers. This can cause existing BGP connections to be shut down and restarted.

Parameters

ip-addr

Resets the BGP neighbor with the specified IP address.

as *as-number*

Resets all BGP neighbors with the specified peer AS number.

external

Resets all EBGP neighbors.

all

Resets all BGP neighbors.

soft

Keyword to specify that the BGP neighbors reevaluate all routes in the Local-RIB against the configured export policies.

soft-inbound

Keyword to specify that the BGP neighbors reevaluate all routes in the RIB-In against the configured import policies.

statistics

Keyword that specifies the BGP neighbor statistics.

protocol

Syntax

protocol

Context

clear>router>bgp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command resets the entire BGP protocol. If the AS number was previously changed, the BGP AS number does not inherit the new value.

database

Syntax

database

Context

clear>router>rip

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command clears all routes in the RIP database.

id

Syntax

id *service-id*

Context

clear>service

clear>service>statistics

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command clears commands for a specific service.

Parameters

service-id

Specifies the ID that uniquely identifies a service.

Values 1 to 2147483648

sap

Syntax

sap *sap-id* {**all** | **counters** | **stp**}

Context

clear>service>statistics

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command clears SAP statistics for a SAP.

Parameters

sap-id

Specifies the physical port identifier portion of the SAP definition. See Common CLI command descriptions for command syntax.

spoke-sdp

Syntax

spoke-sdp *sdp-id*:*vc-id* **ingress-vc-label**

Context

clear>service>id

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command clears and resets the spoke-SDP bindings for the service.

Parameters

sdp-id

Specifies the spoke-SDP ID to be cleared and reset.

Values 1 to 17407

vc-id

Specifies the virtual circuit ID on the SDP ID to be cleared and reset.

Values 1 to 4294967295

sdp

Syntax

sdp *sdp-id* **keep-alive**

Context

clear>service>statistics

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command clears keepalive statistics associated with the SDP ID.

Parameters

sdp-id

Specifies the SDP ID for which to clear keepalive statistics.

Values 1 to 17407

counters

Syntax

counters

Context

clear>service>statistics>id

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command clears all traffic queue counters associated with the service ID.

spoke-sdp

Syntax

spoke-sdp *sdp-id*[**:***vc-id*] {**all** | **counters** | **stp**}

Context

clear>service>statistics>id

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command clears statistics for the spoke-SDP bound to the service.

Parameters

sdp-id

Specifies the spoke-SDP ID for which to clear statistics.

Values 1 to 17407

vc-id

Specifies the virtual circuit ID on the SDP ID to be reset.

Values 1 to 4294967295

all

Clears all queue statistics and STP statistics associated with the SDP.

counters

Clears all queue statistics associated with the SDP.

stp

Clears all STP statistics associated with the SDP.

stp

Syntax

stp

Context

clear>service>statistics>id

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command clears all spanning tree statistics for the service ID.

7.4.2.4 Debug commands

id

Syntax

[**no**] **id** *service-id*

Context

debug>service

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command debugs commands for a specific service.

The **no** form of this command disables debugging.

Parameters

service-id

Specifies the ID that uniquely identifies a service.

sap

Syntax

[**no**] **sap** *sap-id*

Context

debug>service>id

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command displays Subscriber Host Connectivity Verification (SHCV) events for a particular SAP.

Parameters

sap-id

Specifies the physical port identifier portion of the SAP definition. See Common CLI command descriptions for command syntax.

sap

Syntax

[**no**] **sap** *sap-id*

Context

debug>service>id

debug>service>stp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables STP debugging for a specific SAP.

The **no** form of this command disables debugging.

Parameters

sap-id

Specifies the physical port identifier portion of the SAP definition. See Common CLI command descriptions for command syntax.

sdp

Syntax

[**no**] **sdp** *sdp-id:vc-id*

Context

debug>service>id

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables STP debugging for a specific SDP.

The **no** form of this command disables debugging.

event-type

Syntax

[**no**] **event-type** {**config-change** | **svc-oper-status-change** | **sap-oper-status-change** | **sdpbind-oper-status-change**}

Context

debug>service>id

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables debugging for an event type.

The **no** form of this command disables debugging.

event-type

Syntax

[**no**] **event-type** {**config-change** | **oper-status-change**}

Context

debug>service>id>sap

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables debugging for an event type.

The **no** form of this command disables debugging.

stp

Syntax

[**no**] **stp**

Context

debug>service>id

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables the context for debugging STP.

The **no** form of this command disables debugging.

all-events

Syntax

all-events

Context

debug>service>id>stp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables STP debugging for all events.

The **no** form of this command disables debugging.

bpdu

Syntax

[**no**] **bpdu**

Context

debug>service>stp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables STP debugging for received and transmitted BPDUs.

The **no** form of this command disables debugging.

core-connectivity

Syntax

[**no**] **core-connectivity**

Context

debug>service>stp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables STP debugging for core connectivity.

The **no** form of this command disables debugging.

exception

Syntax

[**no**] **exception**

Context

debug>service>stp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables STP debugging for exceptions.

The **no** form of this command disables debugging.

fsm-state-changes

Syntax

[**no**] **fsm-state-changes**

Context

debug>service>stp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables STP debugging for FSM state changes.

The **no** form of this command disables debugging.

fsm-timers

Syntax

[**no**] **fsm-timers**

Context

debug>service>stp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables STP debugging for FSM timer changes.

The **no** form of this command disables debugging.

port-role

Syntax

[**no**] **port-role**

Context

debug>service>stp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables STP debugging for changes in port roles.

The **no** form of this command disables debugging.

port-state

Syntax

[**no**] **port-state**

Context

debug>service>stp

Platforms

Supported on all 7210 SAS platforms as described in this document

Description

This command enables STP debugging for port states.

The **no** form of this command disables debugging.

8 Common CLI command descriptions

This section provides information about Command Line Interface (CLI) syntax and command usage for common service commands.

8.1 Command descriptions

8.1.1 SAP syntax

sap

Syntax

[**no**] **sap** *sap-id*

Context

various

Platforms

Supported on all 7210 SAS platforms as described in this document

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 formats listed in the following table.

Table 127: SAP-ID formats

Type	Syntax	Example
port-id	*slot*/*mda*/*port*[.*channel*]	1/1/5
null	[*port-id* | *lag-id*]	*port-id*: 1/1/3 *lag-id*: lag-3
dot1q	[*port-id* | *lag-id*]:qtag1	*port-id*:qtag1: 1/1/3:100 *lag-id*:qtag1:lag-3:102

Type	Syntax	Example
		cp.conn-prof-id: 1/2/1:cp.2
qinq	[*port-id* | *lag-id*]:*qtag1*.*qtag2*	*port-id*:qtag1.qtag2: 1/1/3:100.10 *lag-id*:qtag1.qtag2: lag-10:

The values depend on the encapsulation type configured for the interface. The following table describes the allowed values for the port and encapsulation types.

Table 128: Encapsulation types

Port type	Encap-type	Allowed values	Comments
Ethernet	null	0	The SAP is identified by the port.
Ethernet	dot1q	0 to 4094	The SAP is identified by the 802.1Q tag on the port.[19]
Ethernet	QinQ	qtag1: 0 to 4094 qtag2: 0 to 4094	The SAP is identified by two tags on the port.[20] [21]

19 A 0 qtag1 value also accepts untagged packets on the dot1q port.

20 A 0 qtag1 value is allowed with some 7210 SAS platforms. See SAP configuration considerations for information about platforms and frame processing.

21 A 0 qtag2 value is not allowed on 7210 SAS platforms as described in this document. See SAP configuration considerations for more information about allowed SAPs and their processing behavior.

9 Appendix: DHCP management

This chapter provides information about using DHCP, including theory, supported features and configuration process overview.

9.1 DHCP principles

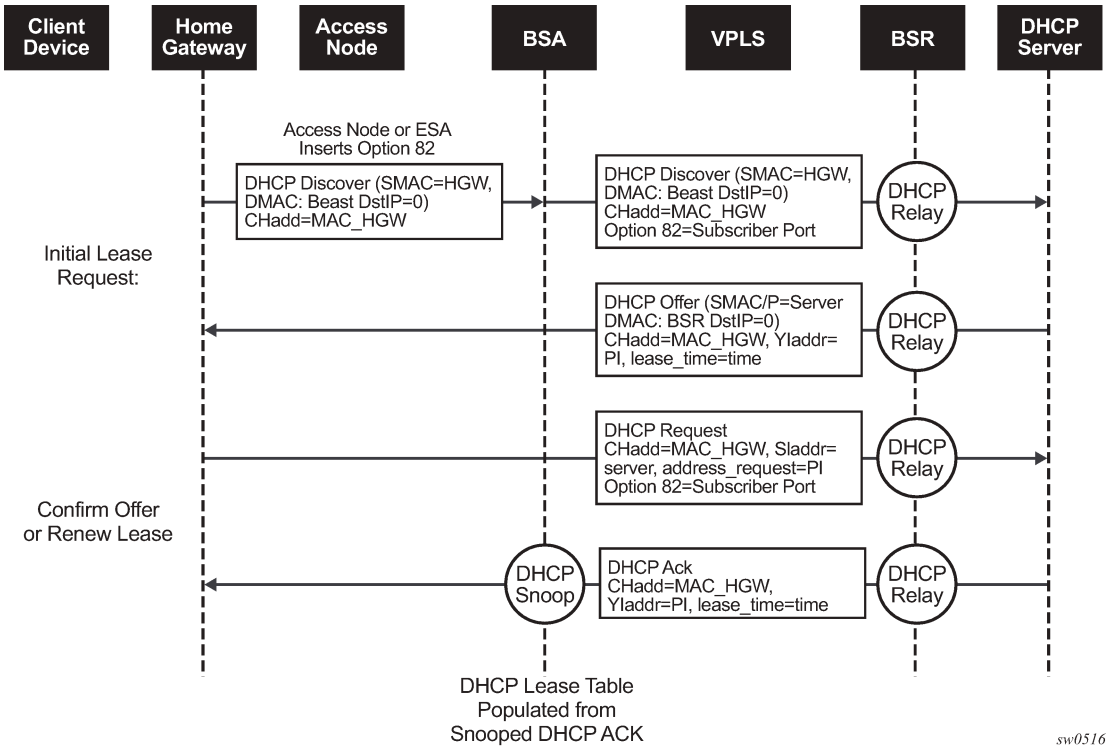
Note: DHCP relay is only supported on the 7210 SAS-R6 and 7210 SAS-R12.

In a Triple Play network, client devices (such as a routed home gateway, a session initiation protocol (SIP) phone or a set-top box) use Dynamic Host Configuration Protocol (DHCP) to dynamically obtain their IP address and other network configuration information. 7210 autoinit procedure also uses DHCP to dynamically obtain the BOF used for first-time booting of the system (along with IP address required to retrieve the BOF, the configuration file and the Timos software image from the network). DHCP is defined and shaped by several RFCs and drafts in the IETF DHC working group including the following:

- RFC 2131, Dynamic Host Configuration Protocol
- RFC 3046, DHCP Relay Agent Information Option

The DHCP operation is shown in the following figure.

Figure 80: IP address assignment with DHCP



During boot-up, the client device sends a DHCP discover message to get an IP address from the DHCP Server. The message contains:

- Destination MAC address - broadcast
- Source MAC address - MAC of client device
- Client hardware address - MAC of client device

If this message passes through a DSLAM or other access node (possibly a 7210 SAS device), typically the Relay information option (Option 82) field is added, indicating shelf, slot, port, VPI, VCI and other fields, to identify the subscriber.

DHCP relay is enabled on the first IP interface in the upstream direction. Depending on the scenario, the DSLAM, BSA or the BSR relays the discover message as a unicast packet toward the configured DHCP server. DHCP relay is configured to insert the giaddr to indicate to the DHCP server in which subnet an address should be allocated:

1. The DHCP server looks up the client MAC address and Option 82 information in its database. If the client is recognized and authorized to access the network, an IP address is assigned and a DHCP offer message returned. The BSA or BSR relays this back to the client device.
2. It is possible that the discover reached more than one DHCP server, and therefore that more than one offer was returned. The client selects one of the offered IP addresses and confirms it needs to use this in a DHCP request message, sent as unicast to the DHCP server that offered it.
3. The DHCP server confirms that the IP address is still available, updates its database to indicate it is now in use, and replies with a DHCP ACK message back to the client. The ACK also contains the Lease Time of the IP address.

9.1.1 DHCP features

9.1.1.1 Using Option 82 field

Option 82, or the relay information option is specified in RFC 3046, DHCP Relay Agent Information Option, allows the router to append some information to the DHCP request that identifies where the original DHCP request arrives from.

There are two sub-options under Option 82:

- Agent Circuit ID Sub-option (RFC 3046, section 3.1): This sub-option specifies data which must be unique to the box that is relaying the circuit.
- Remote ID Sub-option (RFC 3046 section 3.2): This sub-option identifies the host at the other end of the circuit. This value must be globally unique.

Both sub-options are supported by the Nokia 7210 SAS and can be used separately or together.

Inserting Option 82 information is supported independently of DHCP relay.

When the circuit ID sub-option field is inserted by the 7210 SAS, it can take following values:

- *sap-id* - the SAP index (only under a IES or VPRN service)
- *ifindex* - the index of the IP interface (only under a IES or VPRN service)
- *ascii-tuple* - an ASCII-encoded concatenated tuple, consisting of [system-name|serviceid| interface-name] (for VPRN or IES) or [system-name|service-id|sap-id] (for VPLS)
- *vlan-ascii-tuple* - an ASCII-encoded concatenated tuple, consisting of the ascii-tuple followed by Dot1p bits and Dot1q tags

Note that for VPRN the ifindex is unique only within a VRF. The DHCP relay function automatically prepends the VRF ID to the ifindex before relaying a DHCP Request.

When a DHCP packet is received with Option 82 information already present, the system can do one of three things. The available actions are:

- **Replace**

  On ingress the existing information-option is replaced with the information-option parameter configured on the 7210 SAS. On egress (toward the customer) the information-option is stripped (per the RFC).

- **Drop**

  The DHCP packet is dropped and a counter is incremented.

- **Keep**

  The existing information is kept on the packet and the router does not add any more information. On egress the information option is not stripped and is sent on to the downstream node.

In accordance with the RFC, the default behavior is to keep the existing information; except if the giaddr of the packet received is identical to a local IP address on the router, then the packet is dropped and an error incremented regardless of the configured action.

The maximum packet size for a DHCP relay packet is 1500 bytes. If adding the Option 82 information would cause the packet to exceed this size, the DHCP relay request is forwarded without the Option 82 information. This packet size limitation exists to ensure that there is no fragmentation on the end Ethernet segment where the DHCP server attaches.

In the downstream direction, the inserted Option 82 information should not be passed back toward the client (as per RFC 3046, DHCP Relay Agent Information Option). To enable downstream stripping of the option 82 field, DHCP snooping should be enabled on the SDP or SAP connected to the DHCP server.

9.1.1.2 Trusted and untrusted

There is a case where the relay agent could receive a request where the downstream node added Option 82 information without also adding a giaddr (giaddr of 0). In this case the default behavior is for the router to drop the DHCP request. This behavior is in line with the RFC.

The 7210 SAS supports a command trusted, which allows the router to forward the DHCP request even if it receives one with a giaddr of 0 and Option 82 information attached. This could occur with older access equipment. In this case the relay agent would modify the request's giaddr to be equal to the ingress interface. This only makes sense when the action in the information option is keep, and the service is IES or VPRN. In the case where the Option 82 information gets replaced by the relay agent, either through explicit configuration or the VPLS DHCP Relay case, the original Option 82 information is lost, and the reason for enabling the trusted option is lost.

9.1.1.3 DHCP snooping

To support DHCP based address assignment in L2 aggregation network, 7210 supports DHCP snooping. 7210 can copy packets designated to the standard UDP port for DHCP (port 67) to its control plane for inspection, this process is called DHCP snooping.

DHCP snooping can be performed in two directions:

1. From the client to the DHCP server (Discover or Request messages) to insert Option 82 information; For these applications, DHCP snooping must be enabled on the SAP toward the subscriber.
2. From the DHCP server (ACK messages), to remove the Option 82 field toward the client. For these applications, DHCP snooping must be enabled on both the SAP toward the network and the SAP toward the subscriber.

9.1.2 Common configuration guidelines

9.1.2.1 Configuration guidelines for DHCP relay and snooping

The following configuration guidelines must be followed to configure DHCP relay and snooping:

- 7210 SAS devices does not support the ARP populate based on the DHCP lease, assigned to the DHCP client
- 7210 SAS devices does not maintain the DHCP lease assigned to the client
- 7210 SAS devices do not perform IP spoofing checks and MAC spoofing checks based on the DHCP parameters assigned to the client
- MAC learning must be enabled in the VPLS service, for DHCP snooping.
- DHCP snooping is not supported for B-SAPs in B-VPLS services and I-SAPs in I-VPLS services.
- Ingress ACLs cannot be used to drop DHCP control packet.

- DHCP packets received over a SDP cannot be identified and option-82 inserted by the node cannot be removed by the node, in the downstream direction. If this behavior is not needed user should not enable DHCP snooping in the VPLS service, if the DHCP server is reachable over the SDP (either spoke-sdp or mesh-sdp).

9.1.2.2 Configuring Option 82 handling

Option 82, or "Relay Information Option" is a field in DHCP messages used to identify the subscriber. The Option 82 field can already be filled in when a DHCP message is received at the router, or it can be empty. If the field is empty, the router shoulMAC learning must be enabled in the VPLS service, for DHCP snooping.d add identifying information (circuit ID, remote ID or both). If the field is not empty, the router can decide to replace it.

The following is a sample partial BSA configuration with Option 82 adding on a VPLS service. Note that snooping must be enabled explicitly on a SAP.

Example: Partial BSA configuration — adding Option 82 to a VPLS

```
*A:7210SAS>config>service#
------------------------------------------------

vpls 2 customer 1 create
            shutdown
            stp
                shutdown
            exit
sap 1/1/12:100 create
                dhcp                    //Configuration example to add option 82
                    option
                        action replace
                        circuit-id
                        no remote-id
                    exit
                    no shutdown
                exit
            exit
            no shutdown
        exit
------------------------------------------------

*A:7210SAS>config>service#
```

The following example displays a partial BSA configuration to remove the Option 82 on a VPLS.

Example: Partial BSA configuration — removing Option 82 from a VPLS

```
vpls 2 customer 1 create
            stp
                shutdown
            exit
            sap 1/1/14:100 create      //Configuration example to remove option 82
                dhcp
                    snoop
                    no shutdown
                exit
            exit
```

10 Standards and protocol support

Note:
The information provided in this chapter is subject to change without notice and may not apply to all platforms.

Nokia assumes no responsibility for inaccuracies.

The following conventions are used in this section:

- T(A,N) indicates 7210 SAS-T in both Access-uplink mode and Network mode. Similarly, T(N) indicates 7210 SAS-T in network mode only.
- K5 indicates 7210 SAS-K 2F2T1C.
- K12 indicates 7210 SAS-K 2F4T6C.
- K30 indicates 7210 SAS-K 3SFP+ 8C.
- Sx/S-1/10GE indicates all variants of 7210 SAS-Sx 1/10GE and 7210 SAS-S 1/10GE platforms.
- Sx-10/100GE indicates only the variants of 7210 SAS-Sx 10/100GE. Sx-10/100GE QSFP28 indicates the 7210 SAS-Sx 10/100GE 64 SFP+ 4QSFP28 variant.
- Sx/S-1/10GE-VC indicates 7210 SAS-Sx 1/10GE and 7210 SAS-S 1/10GE platforms in standalone VC mode.
- R6 indicates 7210 SAS-R6.
- R12 indicates 7210 SAS-R12.
- D indicates 7210 SAS-D and 7210 SAS-D ETR. If a line item applies only to 7210 SAS-D ETR, then it is indicated as D-ETR.
- Dxp indicates 7210 SAS-Dxp-12p (2SFP+ 4F6T) 7210 SAS-Dxp-12p ETR (2SFP+ 4F6T), 7210 SAS-Dxp 16p (2SFP+ 4F10T), and 7210 SAS-Dxp-24p (2SFP+ 6F16T). If a line item applies only to a particular variant, the variant name will be called out explicitly against that item.
- This standards list is not applicable to platforms in the satellite mode of operation, as most of the features are supported on 7x50 SR platforms. For this reason, the host platforms standards compliance must be consulted for the satellite mode of operation.

10.1 BGP

draft-ietf-idr-add-paths-04, Advertisement of Multiple Paths in BGP is supported on T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

draft-ietf-sidr-origin-validation-signaling-04, BGP Prefix Origin Validation State Extended Community is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 1772, Application of the Border Gateway Protocol in the Internet is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 1997, BGP Communities Attribute is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 2385, Protection of BGP Sessions via the TCP MD5 Signature Option is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 2439, BGP Route Flap Damping is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 2545, Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing is supported on K12, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 2858, Multiprotocol Extensions for BGP-4 is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 2918, Route Refresh Capability for BGP-4 is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 3107, Carrying Label Information in BGP-4 is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 3392, Capabilities Advertisement with BGP-4 is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 4271, A Border Gateway Protocol 4 (BGP-4) is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 4360, BGP Extended Communities Attribute is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 4364, BGP/MPLS IP Virtual Private Networks (VPNs) is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 4456, BGP Route Reflection: An Alternative to Full Mesh Internal BGP (IBGP) is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

Note:
Only R6 and R12 supports RR server functionality. Rest of the platforms support only client function.

RFC 4659, BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 4684, Constrained Route Distribution for Border Gateway Protocol/MultiProtocol Label Switching (BGP/MPLS) Internet Protocol (IP) Virtual Private Networks (VPNs) is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 4760, Multiprotocol Extensions for BGP-4 is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 4798, Connecting IPv6 Islands over IPv4 MPLS Using IPv6 Provider Edge Routers (6PE) is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 4893, BGP Support for Four-octet AS Number Space is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 5004, Avoid BGP Best Path Transitions from One External to Another is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 5291, Outbound Route Filtering Capability for BGP-4 is supported on K12, K30, T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 5668, 4-Octet AS Specific BGP Extended Community is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 6811, Prefix Origin Validation is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

10.2 Ethernet

IEEE 802.1AB, Station and Media Access Control Connectivity Discovery is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

TIA-1057, LLDP for Media endpoint devices is supported on Dxp, Sx/S-1/10GE, and Sx/S-1/10GE-VC

IEEE 802.1ad, Provider Bridges is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

IEEE 802.1ag, Connectivity Fault Management is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

IEEE 802.1ah, Provider Backbone Bridges is supported on T(N)

IEEE 802.1ax, Link Aggregation is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

IEEE 802.1D, MAC Bridges is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

IEEE 802.1p, Traffic Class Expediting is supported on D, E, Dxp, K5, K12, K30, T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

IEEE 802.1Q, Virtual LANs is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

IEEE 802.1s, Multiple Spanning Trees is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

IEEE 802.1w, Rapid Reconfiguration of Spanning Tree is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

IEEE 802.1X, Port Based Network Access Control is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

IEEE 802.3ab, 1000BASE-T is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

IEEE 802.3ac, VLAN Tag is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

IEEE 802.3ad, Link Aggregation is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

IEEE 802.3ae, 10 Gb/s Ethernet is supported on Dxp, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

IEEE 802.3ah, Ethernet in the First Mile is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

IEEE 802.3ba, 40 Gb/s and 100 Gb/s Ethernet is supported on R6, R12, and Sx-10/100GE

IEEE 802.3i, Ethernet is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

IEEE 802.3u, Fast Ethernet is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

IEEE 802.3z, Gigabit Ethernet is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

IEEE 802.3af, Power Over Ethernet (PoE) is supported on Dxp, T-ETR, Mxp-ETR, and Sx/S-1/10GE

Note:
Sx/S-1/10GE only on PoE variant and Sx-1/10GE fiber variant with two fixed copper ports. Only on Dxp-16p and Dxp-24p.

IEEE 802.3at, Power Over Ethernet (PoE+) is supported on Dxp, T-ETR, Mxp-ETR, and Sx/S-1/10GE

Note:
Sx/S-1/10GE only on PoE variant and Sx-1/10GE fiber variant with two fixed copper ports. Only on Dxp-16p and Dxp-24p.

IEEE 802.3bt, Power Over Ethernet (PoE++/HPoE) is supported on Dxp

Note:
Only on Dxp-16p and Dxp-24p.

ITU-T G.8032, Ethernet Ring Protection Switching is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

ITU-T Y.1731, OAM functions and mechanisms for Ethernet based networks is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

10.3 EVPN

draft-snr-bess-evpn-proxy-arp-nd-00, Proxy-ARP/ND function in EVPN networks is supported on K12, K30, Mxp, Sx/S-1/10GE, R6, and R12

Note:
Sx/S-/10GE standalone mode only.

RFC 7432, BGP MPLS-Based Ethernet VPN is supported on K12, K30, Mxp, Sx/S-1/10GE, R6, and R12

Note:
Sx/S-/10GE standalone mode only.

draft-ietf-bess-evpn-vpws-14, Virtual Private Wire Service support in Ethernet VPN is supported on Mxp

10.4 Fast Reroute

draft-ietf-rtgwg-lfa-manageability-08, Operational management of Loop Free Alternates is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

Note:
With Segment Routing.

RFC 5286, Basic Specification for IP Fast Reroute: Loop-Free Alternates is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

Note:
With Segment Routing.

RFC 7490, Remote Loop-Free Alternate (LFA) Fast Reroute (FRR) is supported on K12, K30, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

Note:
With Segment Routing.

10.5 Internet Protocol (IP) — General

draft-grant-tacacs-02, The TACACS+ Protocol is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

draft-ietf-vrrp-unified-spec-02, Virtual Router Redundancy Protocol Version 3 for IPv4 and IPv6 is supported on Mxp

RFC 768, User Datagram Protocol is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 793, Transmission Control Protocol is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 854, TELNET Protocol Specifications is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 951, Bootstrap Protocol (BOOTP) is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 1034, Domain Names - Concepts and Facilities is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 1035, Domain Names - Implementation and Specification is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 1350, The TFTP Protocol (revision 2) is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 1534, Interoperation between DHCP and BOOTP is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 1542, Clarifications and Extensions for the Bootstrap Protocol is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 2131, Dynamic Host Configuration Protocol is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 2132, DHCP Options and BOOTP Vendor Extensions is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 2347, TFTP Option Extension is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 2348, TFTP Blocksize Option is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 2349, TFTP Timeout Interval and Transfer Size Options is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 2428, FTP Extensions for IPv6 and NATs is supported on D, Dxp, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 2865, Remote Authentication Dial In User Service (RADIUS) is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 2866, RADIUS Accounting is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 3046, DHCP Relay Agent Information Option (Option 82) is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 3596, DNS Extensions to Support IP version 6 is supported on D, Dxp, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 3768, Virtual Router Redundancy Protocol (VRRP) is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 4250, The Secure Shell (SSH) Protocol Assigned Numbers is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 4251, The Secure Shell (SSH) Protocol Architecture is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 4252, The Secure Shell (SSH) Authentication Protocol is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

Note:
All 7210 platforms support password and publickey based user authentication. 7210 SAS-D support only password based authentication.

RFC 4253, The Secure Shell (SSH) Transport Layer Protocol is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 4254, The Secure Shell (SSH) Connection Protocol is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 4632, Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 5880, Bidirectional Forwarding Detection (BFD) is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

Note:
IPv4 only on all platforms listed. IPv4 and IPv6 only on Mxp.

RFC 5881, Bidirectional Forwarding Detection (BFD) IPv4 and IPv6 (Single Hop) is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

Note:
IPv4 only on all platforms listed. IPv4 and IPv6 only on Mxp.

RFC 5883, Bidirectional Forwarding Detection (BFD) for Multihop Paths is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

Note:
IPv4 only on all platforms listed. IPv4 and IPv6 only on Mxp.

RFC 6528, Defending against Sequence Number Attacks is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 7130, Bidirectional Forwarding Detection (BFD) on Link Aggregation Group (LAG) Interfaces is supported on T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

10.6 IP — Multicast

RFC 1112, Host Extensions for IP Multicasting is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

Note:
IGMP v1, v2, v3 is supported.

RFC 2236, Internet Group Management Protocol, Version 2 is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 3306, Unicast-Prefix-based IPv6 Multicast Addresses is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 3376, Internet Group Management Protocol, Version 3 is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 3446, Anycast Rendevous Point (RP) mechanism using Protocol Independent Multicast (PIM) and Multicast Source Discovery Protocol (MSDP) is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

Note:
MSDP supported only on Sx/S-1/10GE standalone.

RFC 3618, Multicast Source Discovery Protocol (MSDP) is supported on Sx/S-1/10GE

Note:
Only in standalone mode.

RFC 4601, Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised) is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 4604, Using Internet Group Management Protocol Version 3 (IGMPv3) and Multicast Listener Discovery Protocol Version 2 (MLDv2) for Source-Specific Multicast is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

Note:
MLD not supported.

RFC 4607, Source-Specific Multicast for IP is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 4608, Source-Specific Protocol Independent Multicast in 232/8 is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 4610, Anycast-RP Using Protocol Independent Multicast (PIM) is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 5059, Bootstrap Router (BSR) Mechanism for Protocol Independent Multicast (PIM) is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 5384, The Protocol Independent Multicast (PIM) Join Attribute Format is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 6513, Multicast in MPLS/BGP IP VPNs is supported on T(N), Mxp, Sx/S-1/10GE, Sx/S-1/10GE-VC, R6, and R12

Note:
Only IPv4.

RFC 6514, BGP Encodings and Procedures for Multicast in MPLS/IP VPNs is supported on T(N), Mxp, Sx/S-1/10GE, Sx/S-1/10GE-VC, R6, and R12

Note:
Only IPv4.

RFC 6515, IPv4 and IPv6 Infrastructure Addresses in BGP Updates for Multicast VPNs is supported on T(N), Mxp, Sx/S-1/10GE, Sx/S-1/10GE-VC, R6, and R12

Note:
Only IPv4.

RFC 6625, Wildcards in Multicast VPN Auto-Discover Routes is supported on T(N), Mxp, Sx/S-1/10GE, Sx/S-1/10GE-VC, R6, and R12

Note:
Only IPv4.

RFC 6826, Multipoint LDP In-Band Signaling for Point-to-Multipoint and Multipoint-to-Multipoint Label Switched Path is supported on T(N), Mxp, Sx/S-1/10GE, Sx/S-1/10GE-VC, R6, and R12

Note:
Only IPv4.

RFC 7246, Multipoint Label Distribution Protocol In-Band Signaling in a Virtual Routing and Forwarding (VRF) Table Context is supported on T(N), Mxp, Sx/S-1/10GE, Sx/S-1/10GE-VC, R6, and R12

Note:
Only IPv4.

RFC 7385, IANA Registry for P-Multicast Service Interface (PMSI) Tunnel Type Code Points is supported on T(N), Mxp, Sx/S-1/10GE, Sx/S-1/10GE-VC, R6, and R12

Note:
Only IPv4.

10.7 IP — Version 4

RFC 791, Internet Protocol is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 792, Internet Control Message Protocol is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 826, An Ethernet Address Resolution Protocol is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 1519, Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 1812, Requirements for IPv4 Routers is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 1981, Path MTU Discovery for IP version 6 is supported on K12, K30, T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 2401, Security Architecture for Internet Protocol is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

Note:
Supported only for OSPFv3 authentication. Not supported for services.

RFC 2460, Internet Protocol, Version 6 (IPv6) Specification is supported on D, Dxp, K12, K30, T(A, N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

Note:
D, Dxp, and T(A) for Management only.

10.8 IP — Version 6

RFC 2464, Transmission of IPv6 Packets over Ethernet Networks is supported on D, Dxp, K12, K30, T(A, N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

Note:
D, Dxp, and T(A) for Management only.

RFC 3021, Using 31-Bit Prefixes on IPv4 Point-to-Point Links is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 3122, Extensions to IPv6 Neighbor Discovery for Inverse Discovery Specification is supported on K12, K30, T(A, N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 3587, IPv6 Global Unicast Address Format is supported on D, Dxp, K12, K30, T(A, N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

Note:
D, Dxp, and T(A) for Management only.

RFC 4007, IPv6 Scoped Address Architecture is supported on D, Dxp, K12, K30, T(A, N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

Note:
D, Dxp, and T(A) for Management only.

RFC 4193, Unique Local IPv6 Unicast Addresses is supported on D, Dxp, K12, K30, T(A, N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

Note:
D, Dxp, and T(A) for Management only.

RFC 4291, Internet Protocol Version 6 (IPv6) Addressing Architecture is supported on D, Dxp, K12, K30, T(A, N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

Note:
D, Dxp, and T(A) for Management only.

RFC 4443, Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification is supported on D, Dxp, K12, K30, T(A, N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

Note:
D, Dxp, and T(A) for Management only.

RFC 4861, Neighbor Discovery for IP version 6 (IPv6) is supported on D, Dxp, K12, K30, T(A, N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

Note:
D, Dxp, and T(A) for Management only.

RFC 4862, IPv6 Stateless Address Autoconfiguration (Router Only) is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 5095, Deprecation of Type 0 Routing Headers in IPv6 is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 5952, A Recommendation for IPv6 Address Text Representation is supported on D, Dxp, K12, K30, T(A, N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

Note:
D, Dxp, and T(A) for Management only.

RFC 6106, IPv6 Router Advertisement Options for DNS Configuration is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 6164, Using 127-Bit IPv6 Prefixes on Inter-Router Links is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

10.9 IPsec

RFC 2401, Security Architecture for the Internet Protocol is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

Note:
Only for use with OSPFv3 authentication. Not supported for services.

RFC 2406, IP Encapsulating Security Payload (ESP) is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

Note:
Only for use with OSPFv3 authentication. Not supported for services.

10.10 IS-IS

draft-ietf-isis-mi-02, IS-IS Multi-Instance is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

draft-ietf-isis-segment-routing-extensions-04, IS-IS Extensions for Segment Routing is supported on K12, K30, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

draft-kaplan-isis-ext-eth-02, Extended Ethernet Frame Size Support is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

ISO/IEC 10589:2002, Second Edition, Nov. 2002, Intermediate system to Intermediate system intra-domain routeing information exchange protocol for use in conjunction with the protocol for providing the connectionless-mode Network Service (ISO 8473) is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 1195, Use of OSI IS-IS for Routing in TCP/IP and Dual Environments is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 3359, Reserved Type, Length and Value (TLV) Codepoints in Intermediate System to Intermediate System is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 3719, Recommendations for Interoperable Networks using Intermediate System to Intermediate System (IS-IS) is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 3787, Recommendations for Interoperable IP Networks using Intermediate System to Intermediate System (IS-IS) is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 4971, Intermediate System to Intermediate System (IS-IS) Extensions for Advertising Router Information is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 5120, M-ISIS: Multi Topology (MT) Routing in IS-IS is supported on K12, T(N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 5130, A Policy Control Mechanism in IS-IS Using Administrative Tags is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 5301, Dynamic Hostname Exchange Mechanism for IS-IS is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 5302, Domain-wide Prefix Distribution with Two-Level IS-IS is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 5303, Three-Way Handshake for IS-IS Point-to-Point Adjacencies is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 5304, IS-IS Cryptographic Authentication is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 5305, IS-IS Extensions for Traffic Engineering TE is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 5306, Restart Signaling for IS-IS (Helper Mode) is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 5308, Routing IPv6 with IS-IS is supported on K12, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 5309, Point-to-Point Operation over LAN in Link State Routing Protocols is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 5310, IS-IS Generic Cryptographic Authentication is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 6232, Purge Originator Identification TLV for IS-IS is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 6233, IS-IS Registry Extension for Purges is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

draft-ietf-isis-mi-02, IS-IS Multi-Instance is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

Note:
K12, K30 support only a single instance and can operate in multi-instance deployment as it supports the processing of TLVs for multi-instance support.

draft-ietf-isis-segment-routing-extensions-04, IS-IS Extensions for Segment Routing is supported on K12, K30, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

10.11 Management

draft-ieft-snmpv3-update-mib-05, Management Information Base (MIB) for the Simple Network Management Protocol (SNMP) is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

draft-ietf-idr-bgp4-mib-05, Definitions of Managed Objects for the Fourth Version of Border Gateway Protocol (BGP-4) is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

draft-ietf-isis-wg-mib-06, Management Information Base for Intermediate System to Intermediate System (IS-IS) is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

draft-ietf-mboned-msdp-mib-01, Multicast Source Discovery protocol MIB is supported on Sx/S-1/10GE

Note:
Only in standalone mode.

draft-ietf-mpls-ldp-mib-07, Definitions of Managed Objects for the Multiprotocol Label Switching, Label Distribution Protocol (LDP) is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

draft-ietf-mpls-lsr-mib-06, Multiprotocol Label Switching (MPLS) Label Switching Router (LSR) Management Information Base Using SMIv2 is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

draft-ietf-mpls-te-mib-04, Multiprotocol Label Switching (MPLS) Traffic Engineering Management Information Base is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

draft-ietf-ospf-mib-update-08, OSPF Version 2 Management Information Base is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

ianaaddressfamilynumbers-mib, IANA-ADDRESS-FAMILY-NUMBERS-MIB is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

ianaiftype-mib, IANAifType-MIB is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

ianaiprouteprotocol-mib, IANA-RTPROTO-MIB is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

IEEE8021-CFM-MIB, IEEE P802.1ag(TM) CFM MIB is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

IEEE8021-PAE-MIB, IEEE 802.1X MIB is supported on D, Dxp, K5, K12, K30, T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

IEEE8023-LAG-MIB, IEEE 802.3ad MIB is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

LLDP-MIB, IEEE P802.1AB(TM) LLDP MIB is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 1157, A Simple Network Management Protocol (SNMP) is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 1215, A Convention for Defining Traps for use with the SNMP is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 1724, RIP Version 2 MIB Extension is supported on Mxp and Sx/S-1/10GE

Note:
Only in standalone mode.

RFC 2021, Remote Network Monitoring Management Information Base Version 2 using SMIv2 is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 2138, Remote Authentication Dial In User Service (RADIUS) is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 2206, RSVP Management Information Base using SMIv2 is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 2213, Integrated Services Management Information Base using SMIv2 is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 2571, An Architecture for Describing SNMP Management Frameworks is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 2572, Message Processing and Dispatching for the Simple Network Management Protocol (SNMP) is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 2573, SNMP Applications is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 2575, View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP) is supported on D, E, Dxp, K5, K12, K30, T(A,N), X, Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 2578, Structure of Management Information Version 2 (SMIv2) is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 2579, Textual Conventions for SMIv2 is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 2787, Definitions of Managed Objects for the Virtual Router Redundancy Protocol is supported on K12, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 2819, Remote Network Monitoring Management Information Base is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 2856, Textual Conventions for Additional High Capacity Data Types is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 2863, The Interfaces Group MIB is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 2864, The Inverted Stack Table Extension to the Interfaces Group MIB is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 2933, Internet Group Management Protocol MIB is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 3014, Notification Log MIB is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 3164, The BSD syslog Protocol is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 3165, Definitions of Managed Objects for the Delegation of Management Scripts is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 3231, Definitions of Managed Objects for Scheduling Management Operations is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 3273, Remote Network Monitoring Management Information Base for High Capacity Networks is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 3414, User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3) is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 3416. Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP) is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 3417, Transport Mappings for the Simple Network Management Protocol (SNMP) (SNMP over UDP over IPv4) is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 3419, Textual Conventions for Transport Addresses is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 3584, Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 3593, Textual Conventions for MIB Modules Using Performance History Based on 15 Minute Intervals is supported on Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 3635, Definitions of Managed Objects for the Ethernet-like Interface Types is supported on D, E, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 3826, The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 3877, Alarm Management Information Base (MIB) is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 4001, Textual Conventions for Internet Network Addresses is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 4022, Management Information Base for the Transmission Control Protocol (TCP) is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 4113, Management Information Base for the User Datagram Protocol (UDP) is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 4220, Traffic Engineering Link Management Information Base is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 4292, IP Forwarding Table MIB is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 4293, Management Information Base for the Internet Protocol (IP) is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 5101, Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of IP Traffic Flow Information is supported on Mxp, Sx/S-1/10GE, and R6

RFC 6241, Network Configuration Protocol (NETCONF) is supported on K5, K12, T(N), Mxp, Sx/S-1/10GE, R6, and R12

RFC 6242, Using the NETCONF Protocol over Secure Shell (SSH) is supported on K5, K12, T(N), Mxp, Sx/S-1/10GE, R6, and R12

10.12 MPLS — General

RFC 3031, Multiprotocol Label Switching Architecture is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 3032, MPLS Label Stack Encoding is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 3443, Time To Live (TTL) Processing in Multi-Protocol Label Switching (MPLS) Networks is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 4182, Removing a Restriction on the use of MPLS Explicit NULL is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 5332, MPLS Multicast Encapsulations is supported on T(N), Mxp, Sx/S-1/10GE, Sx/S-1/10GE-VC, R6, and R12

10.13 MPLS — GMPLS

draft-ietf-ccamp-rsvp-te-srlg-collect-04, RSVP-TE Extensions for Collecting SRLG Information is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

10.14 MPLS — LDP

draft-ietf-mpls-ldp-ipv6-15, Updates to LDP for IPv6 is supported on Mxp

draft-pdutta-mpls-ldp-adj-capability-00, LDP Adjacency Capabilities is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

draft-pdutta-mpls-ldp-v2-00, LDP Version 2 is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

draft-pdutta-mpls-tldp-hello-reduce-04, Targeted LDP Hello Reduction is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 3037, LDP Applicability is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 3478, Graceful Restart Mechanism for Label Distribution Protocol (Helper Mode) is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 5036, LDP Specification is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 5283, LDP Extension for Inter-Area Label Switched Paths (LSPs) is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 5443, LDP IGP Synchronization is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 5561, LDP Capabilities is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 6388, Label Distribution Protocol Extensions for Point-to-Multipoint and Multipoint-to-Multipoint Label Switched Paths is supported on T(N), Mxp, Sx/S-1/10GE, Sx/S-1/10GE-VC, R6, and R12

Note:
P2MP LSPs only.

10.15 MPLS — MPLS-TP

RFC 5586, MPLS Generic Associated Channel is supported on T(N), R6, and R12

RFC 5921, A Framework for MPLS in Transport Networks is supported on T(N), R6, and R12

RFC 5960, MPLS Transport Profile Data Plane Architecture is supported on T(N), R6, and R12

RFC 6370, MPLS Transport Profile (MPLS-TP) Identifiers is supported on T(N), R6, and R12

RFC 6378, MPLS Transport Profile (MPLS-TP) Linear Protection is supported on T(N), R6, and R12

RFC 6426, MPLS On-Demand Connectivity and Route Tracing is supported on T(N), R6, and R12

RFC 6428, Proactive Connectivity Verification, Continuity Check and Remote Defect indication for MPLS Transport Profile is supported on T(N), R6, and R12

RFC 6478, Pseudowire Status for Static Pseudowires is supported on T(N), R6, and R12

RFC 7213, MPLS Transport Profile (MPLS-TP) Next-Hop Ethernet Addressing is supported on T(N), R6, and R12

10.16 MPLS — OAM

RFC 6424, Mechanism for Performing Label Switched Path Ping (LSP Ping) over MPLS Tunnels is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 6425, Detecting Data Plane Failures in Point-to-Multipoint Multiprotocol Label Switching (MPLS) - Extensions to LSP Ping is supported on T(N), Mxp, R6, and R12

10.17 MPLS — RSVP-TE

RFC 2702, Requirements for Traffic Engineering over MPLS is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 2747, RSVP Cryptographic Authentication is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 2961, RSVP Refresh Overhead Reduction Extensions is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 3097, RSVP Cryptographic Authentication -- Updated Message Type Value is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 3209, RSVP-TE: Extensions to RSVP for LSP Tunnels is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 3477, Signalling Unnumbered Links in Resource ReSerVation Protocol - Traffic Engineering (RSVP-TE) is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 4090, Fast Reroute Extensions to RSVP-TE for LSP Tunnels is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 4561, Definition of a Record Route Object (RRO) Node-Id Sub-Object is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 4875, Extensions to Resource Reservation Protocol - Traffic Engineering (RSVP-TE) for Point-to-Multipoint TE Label Switched Paths (LSPs) is supported on T(N), Mxp, Sx/S-1/10GE, Sx/S-1/10GE-VC, R6, and R12

RFC 4950, ICMP Extensions for Multiprotocol Label Switching is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 5817, Graceful Shutdown in MPLS and Generalized MPLS Traffic Engineering Networks is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

10.18 OSPF

draft-ietf-ospf-prefix-link-attr-06, OSPFv2 Prefix/Link Attribute Advertisement is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

draft-ietf-ospf-segment-routing-extensions-04, OSPF Extensions for Segment Routing is supported on K12, K30, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 1765, OSPF Database Overflow is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 2328, OSPF Version 2 is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 3101, The OSPF Not-So-Stubby Area (NSSA) Option is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 3509, Alternative Implementations of OSPF Area Border Routers is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 3623, Graceful OSPF Restart Graceful OSPF Restart (Helper Mode) is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 3630, Traffic Engineering (TE) Extensions to OSPF Version 2 is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 4222, Prioritized Treatment of Specific OSPF Version 2 Packets and Congestion Avoidance is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 4552, Authentication/Confidentiality for OSPFv3 is supported on K12, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 4576, Using a Link State Advertisement (LSA) Options Bit to Prevent Looping in BGP/MPLS IP Virtual Private Networks (VPNs) is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 4577, OSPF as the Provider/Customer Edge Protocol for BGP/MPLS IP Virtual Private Networks (VPNs) is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 4970, Extensions to OSPF for Advertising Optional Router Capabilities is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 5185, OSPF Multi-Area Adjacency is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 5187, OSPFv3 Graceful Restart (Helper Mode) is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

RFC 5243, OSPF Database Exchange Summary List Optimization is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 5250, The OSPF Opaque LSA Option is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 5309, Point-to-Point Operation over LAN in Link State Routing Protocols is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 5340, OSPF for IPv6 is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 5838, Support of Address Families in OSPFv3 is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 6987, OSPF Stub Router Advertisement is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

draft-ietf-ospf-prefix-link-attr-06, OSPFv2 Prefix/Link Attribute Advertisement is supported on K12, K30, Mxp, Sx/S-1/10GE, R6, and R12

draft-ietf-ospf-segment-routing-extensions-04, OSPF Extensions for Segment Routing is supported on K12, K30, Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

10.19 Pseudowire

draft-ietf-l2vpn-vpws-iw-oam-04, OAM Procedures for VPWS Interworking is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 3916, Requirements for Pseudo- Wire Emulation Edge-to-Edge (PWE3) is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 3985, Pseudo Wire Emulation Edge-to-Edge (PWE3) is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 4385, Pseudo Wire Emulation Edge-to-Edge (PWE3) Control Word for Use over an MPLS PSN is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 4446, IANA Allocations for Pseudowire Edge to Edge Emulation (PWE3) is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 4447, Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP) is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 4448, Encapsulation Methods for Transport of Ethernet over MPLS Networks is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 5659, An Architecture for Multi-Segment Pseudowire Emulation Edge-to-Edge is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 6073, Segmented Pseudowire is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 6310, Pseudowire (PW) Operations, Administration, and Maintenance (OAM) Message Mapping is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 6391, Flow-Aware Transport of Pseudowires over an MPLS Packet Switched Network is supported on K12, K30, Mxp, R6, and R12

RFC 6718, Pseudowire Redundancy is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 6870, Pseudowire Preferential Forwarding Status bit is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 7023, MPLS and Ethernet Operations, Administration, and Maintenance (OAM) Interworking is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 7267, Dynamic Placement of Multi-Segment Pseudowires is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

10.20 Quality of Service

RFC 2430, A Provider Architecture for Differentiated Services and Traffic Engineering (PASTE) is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 2474, Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 2598, An Expedited Forwarding PHB is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 3140, Per Hop Behavior Identification Codes is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 3260, New Terminology and Clarifications for Diffserv is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

10.21 RIP

RFC 1058, Routing Information Protocol is supported on Mxp and Sx/S-1/10GE

Note:
Only in standalone mode.

RFC 2082, RIP-2 MD5 Authentication is supported on Mxp and Sx/S-1/10GE

Note:
Only in standalone mode.

RFC 2453, RIP Version 2 is supported on Mxp and Sx/S-1/10GE

Note:
Only in standalone mode.

10.22 Timing

GR-1244-CORE, Clocks for the Synchronized Network: Common Generic Criteria, Issue 3, May 2005 is supported on D-ETR, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

Note:
For Dxp, the support only includes the Dxp-12p ETR, Dxp-16p, and Dxp-24p.

GR-253-CORE, SONET Transport Systems: Common Generic Criteria. Issue 3, September 2000 is supported on D-ETR, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

Note:
For Dxp, the support only includes the Dxp-12p ETR, Dxp-16p, and Dxp-24p.

IEEE 1588-2008, IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems is supported on D-ETR, Dxp, K5, K12, K30, T(A,N), Mxp, Sx-1/10GE, Sx-10/100GE, R6, and R12

Note:
For Dxp, IEEE default profile is supported only includes the Dxp-12p ETR, Dxp-16p, Dxp-24p. Sx-10/100GE does not support IEEE default profile.

ITU-T G.781, Synchronization layer functions, issued 09/2008 is supported on D-ETR, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

Note:
For Dxp, the support only includes the Dxp-12p ETR, Dxp-16p, and Dxp-24p.

ITU-T G.813, Timing characteristics of SDH equipment slave clocks (SEC), issued 03/2003 is supported on D-ETR, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

Note:
For Dxp, the support only includes the Dxp-12p ETR, Dxp-16p, and Dxp-24p.

ITU-T G.8261, Timing and synchronization aspects in packet networks, issued 04/2008 is supported on D-ETR, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

Note:
For Dxp, the support only includes the Dxp-12p ETR, Dxp-16p, and Dxp-24p.

ITU-T G.8262, Timing characteristics of synchronous Ethernet equipment slave clock (EEC), issued 08/2007 is supported on D-ETR, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

Note:
For Dxp, the support only includes the Dxp-12p ETR, Dxp-16p, and Dxp-24p.

ITU-T G.8264, Distribution of timing information through packet networks, issued 10/2008 is supported on D-ETR, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, R6, and R12

Note:
For Dxp, the support only includes the Dxp-12p ETR, Dxp-16p, and Dxp-24p.

ITU-T G.8265.1, Precision time protocol telecom profile for frequency synchronization, issued 10/2010 is supported on D-ETR, K5, K12, K30, T(A,N), Mxp, Sx-1/10GE, R6, and R12

ITU-T G.8275.1, Precision time protocol telecom profile for phase/time synchronization with full timing support from the network, issued 07/2014 is supported on Dxp, K12, K30, T(A,N), Mxp, Sx-1/10GE, Sx-10/100GE, R6, and R12

Note:
For 7210 SAS-Sx 10/100GE, the support only includes the Sx 10/100GE QSFP28 variant. For Dxp, the support only includes the Dxp-12p ETR, Dxp-16p, and Dxp-24p.

IEC/IEEE 61850-9-3-2016, Communication networks and systems for power utility automation - Part 9-3: Precision time protocol profile for power utility automation is supported on Dxp-16p and Dxp-24p

IEEE C37.238-2017 - IEEE Standard Profile for Use of IEEE 1588 Precision Time Protocol in Power System Applications is supported on Dxp-16p and Dxp-24p

RFC 5905, Network Time Protocol Version 4: Protocol and Algorithms Specification is supported on D, Dxp, K5, K12, K30, T(A,N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

10.23 VPLS

RFC 4761, Virtual Private LAN Service (VPLS) Using BGP for Auto-Discovery and Signaling is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

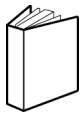
Note:
On 7210 platforms, only BGP-AD is suported with TLDP signalling for PW. No BGP signalling is supported for PW establishment.

RFC 4762, Virtual Private LAN Service (VPLS) Using Label Distribution Protocol (LDP) Signaling is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 5501, Requirements for Multicast Support in Virtual Private LAN Services is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

RFC 6074, Provisioning, Auto-Discovery, and Signaling in Layer 2 Virtual Private Networks (L2VPNs) is supported on K12, K30, T(N), Mxp, Sx/S-1/10GE, Sx-10/100GE, Sx/S-1/10GE-VC, R6, and R12

Customer document and product support



Customer documentation

Customer documentation welcome page

Technical support

Product support portal

Documentation feedback

Customer documentation feedback