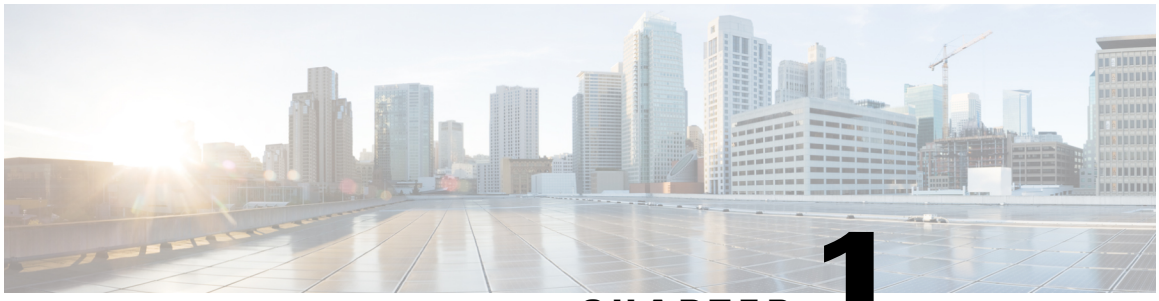
Layer 2 Configuration Guide, Cisco IOS XE Release (ASR 903)

First Published: 0,

Last Modified: 0,

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS



CHAPTER 1

Configuring Ethernet Dataplane Loopback

Ethernet data plane loopback provides a means for remotely testing the throughput of an Ethernet port.

New and Changed Information

Table 1: New and Changed Features

Feature	Description	Changed in Release	Where Documented
Ethernet data plane loopback. QoS for Ethernet loopback	This feature provides a means for remotely testing the throughput of an Ethernet port on the Cisco ASR 903 router.	Cisco IOS XE Release 3.11	Information on Ethernet Data Plane Loopback, on page 2 QoS Support for Ethernet Data Plane Loopback, on page 2

Prerequisites for Ethernet Data Plane Loopback

- Ethernet loopback sessions are supported only of EFPs (service instances, Ethernet flow points, EVCs).
- Dot1q tags must be configured while configuring Ethernet loopback sessions on EFPs. However, loopback sessions can be configured using dot1q/QinQ, even if the underlying EFP has the dot1q/QinQ range configured.

- Internal loopback sessions configured must be within the 1 GB reserved bandwidth.

Restrictions for Ethernet Data Plane Loopback

- Data plane loopback on routed port infrastructure is *not* supported.
- Etype, src-mac, or llc-oui based loopback traffic filtering is *not* supported.
- Port-level QoS is not bypassed. The egress port shaper cannot be bypassed.
- Port shaper on the ingress port in both external and internal loopback cannot be bypassed.
- Ethernet loopback is not supported on a range of dot1q tags.
- Internal and external loopbacks cannot be configured under EFP with encapsulation default or encapsulation untagged.
- Only one Ethernet loopback (terminal or facility) session can be active on an EFP at any instance.
- Egress span on the port and internal loopback on an EFP on the same port cannot be configured at the same time.
- Egress ACL is not supported on the EFP.

Information on Ethernet Data Plane Loopback

The Ethernet data plane loopback feature provides a means for remotely testing the throughput of an Ethernet port. You can verify the maximum rate of frame transmission with no frame loss. This feature allows for bidirectional or unidirectional throughput measurement, and on-demand/out-of-service (intrusive) operation during service turn-up. Two types of Ethernet loopback is supported:

- Facility loopback (external)—Traffic loopback occurs at the Ingress interface. Traffic does not flow into the router for loopback.
- Terminal loopback (internal)—Traffic loopback occurs at the Egress interface. Traffic loopback occurs after the traffic flows into the router to the other interface.

QoS Support for Ethernet Data Plane Loopback

- Ingress QoS is bypassed in external loopback on service instances.
- Internal loopack sequence is as follows:
  - Ingress QoS
  - Egress QoS (egress port), but the ingress port shaper will also take effect.

How to Configure Ethernet Data Plane Loopback

Enabling Ethernet Data Plane Loopback

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface gigabitethernet** *slot/subslot/port*
4. **service instance number ethernet** [**name**]
5. **encapsulation**{**dot1q**|**second-dot1q**}
6. **bridge-domain** *bridge-id*
7. **ethernet loopback permit** {**external**|**permit**}
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface gigabitethernet** *slot/subslot/port* **Example:** `Router (config)# interface gigabitEthernet 0/2/1`	Specifies an interface and enters interface configuration mode. • *slot/subslot/port*—The location of the interface.
Step 4	**service instance number ethernet** [**name**] **Example:** `Router(config-if)# service instance 1 ethernet`	Configure an EFP (service instance) and enter service instance configuration) mode. • **number**—Specifies the EFP identifier, an integer from 1 to 4000. • (Optional) **ethernet name**—Name of a previously configured EVC. You do not need to use an EVC name in a service instance.
Step 5	**encapsulation**{**dot1q**|**second-dot1q**}	Configure encapsulation type for the service instance.

	Command or Action	Purpose
	Example: `Router(config-if-srv)# encapsulation dot1q 120`	• **dot1q—**Configure 802.1Q encapsulation. • **second-dot1q—**Configures double-tagged 802.1Q encapsulation. Matching criteria to be used to map QinQ frames ingress on an interface to the appropriate EFP.
Step 6	**bridge-domain** *bridge-id* **Example:** `Router(config-if-srv)# bridge-domain 120`	*bridge-id***—**Specifies the identifier for the bridge domain instance.
Step 7	**ethernet loopback permit** {**external**|**permit**} **Example:** `Router(config-if-srv)# ethernet loopback permit external`	Configures Ethernet permit external or internal loopback on a interface. External loopback allows loopback of traffic from wire. This command is supported under a service instance. • **external—**Indicates facility loopback. • **internal—**Indicates terminal loopback.
Step 8	**end** **Example:** `Router# end`	Returns to privileged EXEC mode.

Starting an Ethernet Data Plane Loopback Session

Note By default the session would be running for 300 seconds unless explicitly specified by the user and automatically stopped after the session time expiry.

SUMMARY STEPS

1. **enable**
2. **ethernet loopback start local interface** *interface-id*{**service instance** *id*}{**external** |**internal** }{**dot1q** *vlan-id*}[**second-dot1q** *inner-vlan-id*][**cos** *cos-value*][**destination mac-address** *mac-address*][**timeout** {*seconds* |**none**}]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	Enter your password if prompted.
Step 2	**ethernet loopback start local interface** *interface-id*{**service instance** *id*}{**external** |**internal** }{**dot1q** *vlan-id*}[**second-dot1q** *inner-vlan-id*][**cos** *cos-value*][**destination mac-address** *mac-address*][**timeout** {*seconds* |**none**}]	Starts Ethernet external or internal loopback on the interface for a specific service. • *interface-id*—Specifies the interface. • **service instance***id*—Specifies the service instance. • **external**—Indicates facility loopback. • **internal**—Indicates terminal loopback. • **dot1q***vlan-id*—Specifies the s-tag of the packets to be loopbacked. If the filter option is not specified, all of the packets with all VLANs are eligible to be loopbacked. • (Optional) **second-dot1q***inner-vlan-id*—Specifies the c-tag of the packets to be loopbacked. If the filter option is not specified, all of the packets with all inner VLANs are eligible to be loopbacked • (Optional) **cos***cos-value*—Specifies the 802.1p/cos of the packets to be loopbacked. If the filter option is not specified, all of the packets with “Any” cos are eligible to be loopbacked. • (Optional) **destination mac-address***mac-address*—Specifies the destination mac address of the packets to be loopbacked. If the filter option is not specified, all of the packets with “Any” destination mac are eligible to be loopbacked. • (Optional) **timeout***seconds*—Sets a loopback timeout period. The range is from 1 to 90000 seconds (25 hours). The default is 300 seconds. • (Optional) **timeout***none*—Sets the loopback to no timeout.

Configuration Examples

Example: Configuring External Loopback

This example shows how to configure external (facility) loopback.

```
Router(config)# interface gigabitEthernet 0/2/1
Router(config-if)# service instance 1 ethernet
Router(config-if-srv)# encapsulation dot1q 120
Router(config-if-srv)# bridge-domain 120
Router(config-if-srv)# ethernet loopback permit external
```

This example shows external (facility) loopback on the Gigabit Ethernet 0/4/1 interface:

```
interface GigabitEthernet0/4/1
 no ip address
 negotiation auto
 service instance 10 ethernet
  encapsulation dot1q 10
  rewrite ingress tag pop 1 symmetric
  bridge-domain 10
  ethernet loopback permit external ===? For facility loopback
 !
end
```

This example below shows how to start external (facility) loopback on the router. A warning message is displayed. Type **yes** to continue.

```
Router# ethernet loopback start local interface gigabitEthernet 0/4/1 service instance 10
external dot1q 10 cos 1
 destination mac-address 0000.0000.0001 timeout none

This is an intrusive loopback and the packets matched with the service will not  be able
to pass through.
Continue? (yes/[no]): yes
```

Example: Configuring Terminal Loopback

This example shows internal (terminal) loopback on Gigabit Ethernet 0/4/1 interface:

```
interface TenGigabitEthernet0/0/0
 no ip address
service instance 10 ethernet
  encapsulation dot1q 10
  rewrite ingress tag pop 1 symmetric
  bridge-domain 10
  ethernet loopback permit internal  ===? For Terminal Loopback
 !
end
```

Verifying Ethernet Data Plane Loopback

Example: Verifying Ethernet Dataplane Loopback

Use the **show ethernet loopback** {**active** | **permitted**} [**interface** *interface numbe*r] command.

- The following example displays the loopback capabilities per interface. The output shows internal (terminal) loopback has been permitted on Ten Gigabit Ethernet 0/0/0 interface and external (facility) loopback has been permitted on Gigabit Ethernet 0/4/1 interface.

```
Router# show ethernet loopback permitted

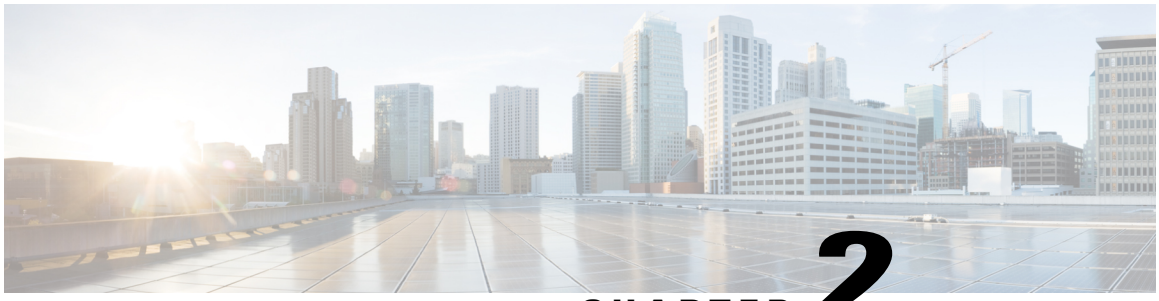
--------------------------------------------------------------------------------
Interface                                 SrvcInst Direction
Dot1q/Dot1ad(s)                           Second-Dot1q(s)
--------------------------------------------------------------------------------
Te0/0/0                                   10                              Internal
10
Gi0/4/1                                   10                              External
10
```

- This example shows all active sessions on the router.

```
Router# show ethernet loopback active

============================================================
Loopback Session ID     : 1
Interface                        : GigabitEthernet0/4/1
Service Instance            :10
Direction                        : External
Time out(sec)                 : none
Status                            : on
Start time                       : 10:31:09.539 IST Mon Aug 26 2013
Time left                         : N/A
Dot1q/Dot1ad(s)             : 10
Second-dot1q(s)             :
Source Mac Address       : Any
Destination Mac Address : 0000.0000.0001
Ether Type                       : Any
Class of service               : 1
Llc-oui                             : Any


Total Active Session(s): 1
Total Internal Session(s): 0
Total External Session(s): 1
```



CHAPTER 2

Configuring Switched Port Analyzer on the Cisco ASR 903 Router

This document describes how to configure local Switched Port Analyzer (SPAN) and remote SPAN (RSPAN) on the Cisco ASR 903 router.

New and Changed Information

Table 2: New and Changed Features

Feature	Description	Changed in Release	Where Documented
Remote SPAN	This feature is used for remote monitoring of multiple devices at source port, source Vlan levels in the Layer2 network.	Cisco IOS XE Release 3.11	• RSPAN Session, on page 12 • Configuring RSPAN Source Session, on page 19 • Configuring RSPAN Destination Session, on page 21

Feature	Description	Changed in Release	Where Documented
Local SPAN	This feature is used for monitoring the traffic on the local port of the router.	Cisco IOS XE Release 3.6	• Local SPAN Session, on page 11 • Configuring Sources and Destinations for Local SPAN, on page 17

Prerequisites for Configuring Local Span and RSPAN

Local Span

- Use a network analyzer to monitor interfaces.

RSPAN

- MAC learning should be disabled using the mac-address-table limit *[rspan vlan/bd]* maximum num action limit command before configuring the RSPAN Vlan.
- RSPAN Vlan must be dedicated and entire Layer 2 devices in the network must be aware of the Vlan.
- RSPAN source and destinations switches separated by the VPLS pseudowire must be aware of the RSPAN Vlan / brige domain (BD).
- Pseudowire must be dedicated for RSPAN traffic.
- The RSPAN destination session is not required when the destination switch is connected to source switch through Layer2 VPN. Thus, in the destination switch, the destination port must configured with the service instance with encapsulation as RSPAN Vlan/BD and bridge domain as RSPAN Vlan/BD and the MAC address learning should be disabled on RSPAN BD/Vlan.

Restrictions for Local Span and RSPAN

Local Span

- Local SPAN is only supported on physical ports.
- Combined Egress local SPAN bandwidth supported is 1 GB.
- Local SPAN is not supported on logical interfaces such as Vlans or EFPs.
- Up to 15 active local SPAN sessions (ingress and egress) are supported. The router supports up to 15 ingress sessions and up to 12 egress sessions.

- Only one local SPAN destination interface is supported. You cannot configure a local SPAN destination interface to receive ingress traffic.
- Outgoing Cisco Discovery Protocol (CDP) and Bridge Protocol Data Unit (BPDU) packets are not replicated.
- When enabled, local SPAN uses any previously entered configuration.
- When you specify source interfaces and do not specify a traffic direction (Tx, Rx, or both), both is used by default.
- Local SPAN destinations never participate in any spanning tree instance. Local SPAN includes BPDUs in the monitored traffic, so any BPDUs seen on the local SPAN destination are from the local SPAN source.
- Local SPAN sessions with overlapping sets of local SPAN source interfaces or VLANs are not supported.

RSPAN

- RSPAN Vlan/BD is not used for data traffic.
- The maximum number of supported RSPAN sessions are 15.
- Only one source port is supported per RSPAN.
- Source ranges (vlan range or port range) is not supported.
- Vlan filtering is not supported.
- If two RSPAN configurations sessions are configured on two RSPAN BDs associated to the same Trunk EFP, the traffic from the first session flows to the second session after it is configured.
- RSPAN destination configuration for Layer2 pseudowire is not supported.

Understanding Local SPAN and RSPAN

Information About Local SPAN Session and RSPAN Session

Local SPAN Session

A local Switched Port Analyzer (SPAN) session is an association of a destination interface with a set of source interfaces. You configure local SPAN sessions using parameters that specify the type of network traffic to monitor. Local SPAN sessions allow you to monitor traffic on one or more interfaces and to send either ingress traffic, egress traffic, or both to one destination interface.

Local SPAN sessions do not interfere with the normal operation of the switch. You can enable or disable SPAN sessions with command-line interface (CLI) commands. When enabled, a local SPAN session might become active or inactive based on various events or actions, and this would be indicated by a syslog message. The **show monitor session span session number** command displays the operational status of a SPAN session.

A local SPAN session remains inactive after system power-up until the destination interface is operational.

The following configuration guidelines apply when configuring local SPAN on the Cisco ASR 903 Router:

- When enabled, local SPAN uses any previously entered configuration.
- Use the **no monitor session** *session number* command with no other parameters to clear the local SPAN session number.

Local SPAN Traffic

Network traffic, including multicast, can be monitored using SPAN. Multicast packet monitoring is enabled by default. In some SPAN configurations, multiple copies of the same source packet are sent to the SPAN destination interface. For example, a bidirectional (both ingress and egress) SPAN session is configured for sources a1 and a2 to a destination interface d1. If a packet enters the switch through a1 and gets switched to a2, both incoming and outgoing packets are sent to destination interface d1; both packets would be the same (unless a Layer-3 rewrite had occurred, in which case the packets would be different).

RSPAN Session

An RSPAN source session is an association of source ports or Vlans across your network with an RSPAN Vlan. The RSPAN Vlan/BD on the router is the destination RSPAN session.

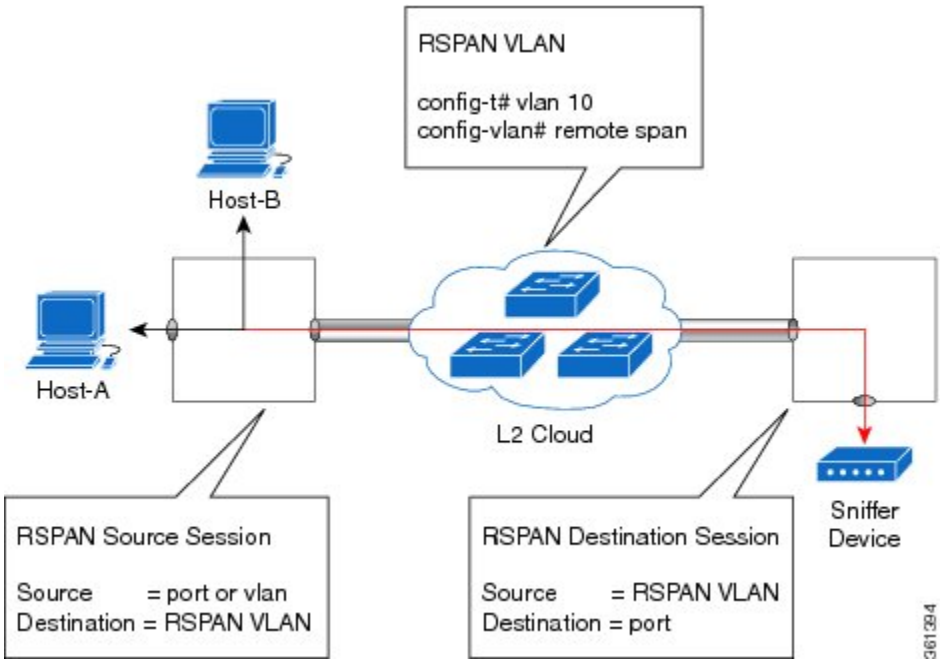
RSPAN Traffic

RSPAN supports source ports and source Vlans in the source switch and destination as RSPAN Vlan/BD.

The figure below shows the original traffic from the Host A to Host B via the source ports or Vlans on Switch A. The source ports or Vlans of Switch A is mirrored to Switch B using RSPAN Vlan 10. The traffic for each RSPAN session is carried over a user-specified RSPAN Vlan that is dedicated for that RSPAN session in all participating devices. The traffic from the source ports or Vlans are mirrored into the RSPAN Vlan and forwarded over Trunk or the EVC bridge domain (BD) ports carrying the RSPAN Vlan to a destination session monitoring the RSPAN Vlan.

Each RSPAN source must have either ports or Vlans as RSPAN sources. On RSPAN destination, the RSPAN Vlan is monitored and mirrored to the destination physical port connected to the sniffer device.

Figure 1: RSPAN Traffic



RSPAN allows remote monitoring of traffic where the source and destination switches are connected by L2VPN networks

The RSPAN source is either ports or Vlans as in a traditional RSPAN. However, the SPAN source and destination devices are connected through a L2 pseudowire associated with the RSPAN Vlan over an MPLS/IP network. The L2 pseudowire is dedicated for only RSPAN traffic. The mirrored traffic from the source port or Vlan is carried over the pseudowire associated with the RSPAN Vlan towards the destination side. On the destination side, a port belonging to the RSPAN Vlan or EVC BD is connected to sniffer device.

Destination Interface

A destination interface, also called a monitor interface, is a switched interface to which SPAN or RSPAN sends packets for analysis. You can have only one destination interface for SPAN sessions.

An interface configured as a destination interface cannot be configured as a source interface. Specifying a trunk interface as a SPAN or RSPAN destination interface stops trunking on the interface.

Source Interface

A source interface is an interface monitored for network traffic analysis. An interface configured as a destination interface cannot be configured as a source interface.

Traffic Directions

Ingress SPAN (Rx) copies network traffic received by the source interfaces for analysis at the destination interface. Egress SPAN (Tx) copies network traffic transmitted from the source interfaces to the destination interface. Specifying the configuration option both copies network traffic received and transmitted by the source interfaces to the destination interface.

The following table lists the supported traffic types for RSPAN.

Table 3: RSPAN Traffic

Source	Ingress Mirror (Rx)	Egress Mirror (Tx)	Both
Layer2 or Layer3	Supported	Supported	Supported
VLAN	Supported	Not supported	Not supported
EFP	Not supported	Not supported	Not supported
Pseudowire	Not supported	Not supported	Not supported

The following table lists the supported **rewrite** traffic for RSPAN on the EFP, Trunk with the associated RSPAN bridge domains.

Table 4: Rewrite Traffic for RSPAN BD

Rewrite Operations	Source	EFP/Trunk associated with RSPAN BD
no-rewrite	Pop1, Pop2, Push1	Only Pop1

The following tables lists the format of the spanned packets at the destination port for both Ingress and Egress RSPAN. The tables lists the formats of untagged, single, and double tagged source packets for EFPs under source port configured with **rewrite** operations (no-rewrite, pop1, pop2 and push1).

Table 5: Destination Port Ingress and Egress Spanned Traffic for EVC RSPAN BD

	Ingress Traffic	Egress Traffic
(Untagged Traffic) - Source port rewrite	**RSPAN Vlan (BD) rewrite pop1 tag symmetric**	**RSPAN Vlan (BD) rewritepop1 tag symmetric**
no-rewrite	RSPAN BD tag + packet	RSPAN BD tag + packet
pop1 tag	NA	NA
pop2 tag	NA	NA

	Ingress Traffic	Egress Traffic
push1 tag	NA	NA
(Single Traffic)-Source port rewrite	**RSPAN Vlan (BD) rewrite pop1 tag symmetric**	**RSPAN Vlan (BD) rewrite pop1 tag symmetric**
no-rewrite	RSPAN BD tag + source-outer-tag + packet	RSPAN BD tag + source-outer-tag + packet
pop1 tag		
pop2 tag		NA
push1 tag		RSPAN BD tag + source-outer-tag + packet
(Double traffic) - Source port rewrite	**RSPAN Vlan (BD) rewrite pop1 tag symmetric**	**RSPAN Vlan (BD) rewrite pop1 tag symmetric**
no-rewrite	RSPAN BD tag + source-outer-tag + source-inner-tag + packet	RSPAN BD tag + Source-inner-tag + packet
pop1 tag		
pop2 tag		
push1 tag		

Table 6: Destination Port Ingress and Egress Spanned Traffic for TEFP RSPAN BD

	Ingress Traffic	Egress Traffic
(Untagged traffic)- Source port rewrite	**RSPAN Vlan (BD) rewrite pop1 tag symmetric**	**RSPAN Vlan (BD) rewrite pop1 tag symmetric**
no-rewrite	RSPAN BD tag + packet	RSPAN BD tag + packet
pop1 tag	NA	NA
pop2 tag	NA	NA
push1 tag	NA	NA
(Single traffic)-Source port rewrite	**RSPAN Vlan (BD) rewrite pop1 tag symmetric**	**RSPAN Vlan (BD) rewrite pop1 tag symmetric**

	Ingress Traffic	Egress Traffic
no-rewrite	RSPAN BD tag + source-outertag + packet	RSPAN BD tag + source-outertag + packet
pop1 tag		
pop2 tag		NA
push1 tag		RSPAN BD tag + source-outertag + packet
(Double traffic) -Source port rewrite	**RSPAN Vlan (BD) rewrite pop1 tag symmetric**	**RSPAN Vlan (BD) rewrite pop1 tag symmetric**
no-rewrite	RSPAN BD tag + source-outertag + source-innertag+ packet	RSPAN BD tag + source-outertag + source-innertag + packet
pop1 tag		
pop2 tag		
push1 tag		

Table 7: Destination Port Ingress and Egress Spanned Traffic for RSPAN BD with VPLS Pseudowire

	Ingress Traffic	Egress Traffic
(Untagged traffic) - Source port rewrite	**RSPAN Vlan (BD) rewrite pop1 tag symmetric**	**RSPAN Vlan (BD) rewrite pop1 tag symmetric**
no-rewrite	RSPAN BD tag + packet	RSPAN BD tag + packet
pop1 tag	NA	NA
pop2 tag	NA	NA
push1 tag	NA	NA
(Single traffic)- Source port rewrite	**RSPAN Vlan (BD) rewrite pop1 tag symmetric**	**RSPAN Vlan (BD) rewrite pop1 tag symmetric**
no-rewrite	RSPAN BD tag + source-outer-tag + packet	RSPAN BD tag + source-outer-tag + packet
pop1 tag		
pop2 tag	NA	NA
push1 tag	RSPAN BD tag + source-outer-tag + packet	RSPAN BD tag + source-outer-tag + packet

	Ingress Traffic	Egress Traffic
(Double traffic)-Source port rewrite	**RSPAN Vlan (BD) rewrite pop1 tag symmetric**	**RSPAN Vlan (BD) rewrite pop1 tag symmetric**
no-rewrite	RSPAN BD tag + source-outer-tag + source-inner-tag + packet	RSPAN BD tag + source-outer-tag + source-inner-tag + packet
pop1 tag		
pop2 tag		
push1 tag		

Configuring Local SPAN and RSPAN

Configuring Sources and Destinations for Local SPAN

To configure sources and destinations for a SPAN session:

SUMMARY STEPS

1. **configure terminal**
2. **monitor session** {*session_number*} **type local**
3. **source interface** *interface_type slot/subslot/port* **[, | - | rx | tx | both]**
4. **destination interface** *interface_type slot/subslot/port* **[, | - | rx | tx | both]**
5. **no shutdown**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 2	**monitor session** {*session_number*} **type local** **Example:** `Router(config)# monitor session 1 type local`	Specifies the local SPAN session number and enters the local monitoring configuration mode. • *session_number*—Indicates the monitor session. The valid range is 1 through 15.
Step 3	**source interface** *interface_type slot/subslot/port* **[,	-	rx	tx	both]**	Specifies the source interface and the traffic direction:

	Command or Action	Purpose
	Example: `Router(config-mon-local)# source interface gigabitethernet 0/2/1 rx`	• *interface_type*—Specifies the Gigabit Ethernet or Ten Gigabit Ethernet interface. ◦ *slot/subslot/port*—The location of the interface. • ","—List of interfaces • "–"—Range of interfaces • rx—Ingress local SPAN • tx—Egress local SPAN • both
Step 4	**destination interface** *interface_type slot/subslot/port* **[, | - | rx | tx | both]** **Example:** `Router(config-mon-local)# destination interface gigabitethernet 0/2/4`	Specifies the destination interface that sends both ingress and egress local spanned traffic from source port to the prober or sniffer. • *interface_type*—Specifies the Gigabit Ethernet or Ten Gigabit Ethernet interface. ◦ *slot/subslot/port*—The location of the interface. • ","—List of interfaces • "–"—Range of interfaces • rx—Ingress local SPAN • tx—Egress local SPAN both
Step 5	**no shutdown** **Example:** `Router(config-mon-local)# no shutdown`	Enables the local SPAN session.

Removing Sources or Destinations from a Local SPAN Session

To remove sources or destinations from a local SPAN session, use the following commands beginning in EXEC mode:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **configure terminal**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**configure terminal** **Example:** `Router(config)# no monitor session 2`	Clears existing SPAN configuration for a session.

Configuring RSPAN Source Session

To configure the source for a RSPAN session:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **monitor session** *RSPAN_source_session_number* **type rspan-source**
4. **source** {*single_interface* slot/subslot/port| *single_vlan* [**rx** | **tx** | **both**]
5. **destination remote vlan** *rspan_vlan_ID*
6. **no shutdown**
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**monitor session** *RSPAN_source_session_number* **type rspan-source** **Example:** `Router(config)# monitor session 1 type rspan-source`	Configures an RSPAN source session number and enters RSPAN source session configuration mode for the session. • *RSPAN_source_session_number*—Valid sessions are 1 to 80. • **rspan-source**—Enters the RSPAN source-session configuration mode.
Step 4	**source** {*single_interface* slot/subslot/port| *single_vlan* [**rx** | **tx** | **both**] **Example:** `Router(config-mon-rspan-src)# monitor session 1 source interface gigabitethernet 0/2/1 tx`	Specifies the RSPAN session number, the source interfaces and the traffic direction to be monitored. • *single_interface*—Specifies the Gigabit Ethernet or Ten Gigabit Ethernet interface. ◦ *slot/subslot/port*—The location of the interface. • *single_vlan*—Specifies the single VLAN. • **both**—(Optional) Monitors the received and the transmitted traffic. • **rx**—(Optional) Monitors the received traffic only. • **tx**—(Optional) Monitors the transmitted traffic only.
Step 5	**destination remote vlan** *rspan_vlan_ID* **Example:** `Router(config-mon-rspan-src)# destination remote vlan2`	Associates the RSPAN source session number session number with the RSPAN VLAN. • *rspan_vlan_ID*—Specifies the Vlan ID.
Step 6	**no shutdown** **Example:** `Router(config-mon-rspan-src)# no shutdown`	Restarts the interface.
Step 7	**end** **Example:** `Router(config-mon-rspan-src)# end`	Exists the configuration.

Configuring RSPAN Destination Session

To configure the destination for a RSPAN session for remote Vlan:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **monitor session** *RSPAN_destination_session_number* **type rspan-destination**
4. **source remote vlan** *rspan_vlan_ID*
5. **destination** {*single_interface slot/subslot/port}*
6. **no shutdown**
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**monitor session** *RSPAN_destination_session_number* **type rspan-destination** **Example:** `Router(config)# monitor session 1 type rspan-destination`	Configures a RPAN session. • *RSPAN_destination_session_number*—Valid sessions are 1 to 80. • **rspan-destination**—Enters the RSPAN destination-session configuration mode.
Step 4	**source remote vlan** *rspan_vlan_ID* **Example:** `Router(config-mon-rspan-dst)# source remote vlan2`	Associates the RSPAN destination session number RSPAN VLAN. • *rspan_vlan_ID*—Specifies the Vlan ID
Step 5	**destination** {*single_interface slot/subslot/port}* **Example:** `Router(config-mon-rspan-dst)# destination interface gigabitethernet 0/1/0`	Associates the RSPAN destination session number with the destination port. • *single_interface* —Specifies the Gigabit Ethernet or Ten Gigabit Ethernet interface. ◦ *slot/subslot/port*—The location of the interface.

	Command or Action	Purpose
Step 6	**no shutdown** **Example:** `Router(config-mon-rspan-dst)# no shutdown`	Restarts the interface
Step 7	**end** **Example:** `Router(config-mon-rspan-dst)# end`	Exists the configuration

Removing Sources or Destinations from a RSPAN Session

To remove sources or destinations from a RSPAN session:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **no monitor session** {*session_number*} **{source | destination}** {*single_interface slot/subslot/port | single_vlan*}**[, | - | rx | tx | both]**
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**no monitor session** {*session_number*} **{source	destination}** {*single_interface slot/subslot/port	single_vlan*}**[,	-	rx	tx	both]** **Example:** `Router(config)# no monitor session 1`	Specifies the RSPAN session number, the source interfaces and the traffic direction to be monitored. • *session_number*—Valid sessions are 1 and 2. • **source**—Enters source interfaces.

	Command or Action	Purpose
	`source interface gigabitethernet 0/2/1 tx`	• *single_interface*—Specifies the Gigabit Ethernet or Ten Gigabit Ethernet interface. ◦ *slot/subslot/port*—The location of the interface. • *single_vlan*—Specifices the Vlan. • **both**—(Optional) Monitors the received and the transmitted traffic. • **rx**—(Optional) Monitors the received traffic only. • **tx**—(Optional) Monitors the transmitted traffic only.
Step 4	**end** **Example:** `Router(config)# end`	Exits configuration mode.

Sample Configurations

The following sections contain configuration examples for SPAN and RSPAN on the Cisco ASR 903 Router.

Configuration Example: Local SPAN

The following example shows how to configure local SPAN session 8 to monitor bidirectional traffic from source interface Gigabit Ethernet interface 0/2/1:

```
Router(config)# monitor session 8 type local
Router(config)# source interface gigabitethernet 0/2/1
```

Configuration Example: Removing Sources or Destinations from a Local SPAN Session

This following example shows how to remove a local SPAN session:

```
Router(config)# no monitor session 8
```

Configuration Example: RSPAN Source

The following example shows how RSPAN session 2 to monitor bidirectional traffic from source interface Gigabit Ethernet 0/0/1:

```
Router(config)# monitor session 2 type RSPAN-source
Router(config-mon-RSPAN-src)# source interface gigabitEthernet0/0/1 [tx |rx|both]
Router(config-mon-RSPAN-src)# destination remote VLAN 100
Router(config-mon-RSPAN-src)# no shutdown
Router(config-mon-RSPAN-src)# end
```

The following example shows how RSPAN session 3 to monitor bidirectional traffic from source Vlan 20:

```
Router(config)# monitor session 3 type RSPAN-source
Router(config-mon-RSPAN-src)# source VLAN 20 rx
Router(config-mon-RSPAN-src)# destination remote VLAN 100
Router(config-mon-RSPAN-src)# no shutdown
Router(config-mon-RSPAN-src)# end
```

Configuration Example: RSPAN Destination

The following example shows how to configure interface Gigabit Ethernet 0/0/1 as the destination for RSPAN session 2:

```
Router(config)# monitor session 2 type RSPAN-destination
Router(config-mon-RSPAN-dst)# source remote VLAN 100
Router(config-mon-RSPAN-dst)# destination interface gigabitEthernet 0/1/0
Router(config-mon-RSPAN-dst)# end
```

Verifying Local SPAN and RSPAN

Use the **show monitor session** command to view the sessions configured.

- The following example shows the RSPAN source session with Gigabit Ethernet interface 0/0/1 as source:

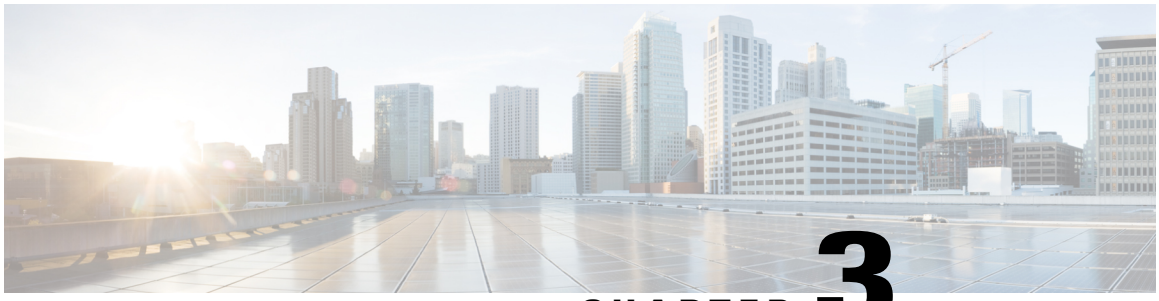
```
Router# show monitor session 2
Session 2
---------
Type                  : Remote Source Session
Status                : Admin Enabled
Source Ports          :
    Both              : Gi0/0/1
MTU                   : 1464
```

- The following example shows the RSPAN source session with Vlan 20 as source:

```
Router# show monitor session 3
Session 3
---------
Type                  : Remote Source Session
Status                : Admin Enabled
Source VLANs          :
    RX Only           : 20
MTU                   : 1464
```

- The following example shows the RSPAN destination session with Gigabit Ethernet interface 0/0/1 as source:

```
Router# show monitor session 2
Session 2
---------
Type                   : Remote Destination Session
Status                 : Admin Enabled
Destination Ports      : Gi0/0/1
MTU                    : 1464
```



CHAPTER 3

Configuration of MAC Limiting on the Cisco ASR 903 Router

This document describes how to configure MAC limiting on the Cisco ASR 903 Router.

Restrictions and Usage Guidelines

MAC limiting is supported on the following interface types:

- You can apply MAC limiting only to bridge-domains.
- MAC limiting is supported for dynamic MAC addresses.

Configuring MAC Limiting

Mac address limiting per bridge-domain restricts the number of MAC addresses that the router learns in bridge-domain on an EFP, pseudowire or switchport.

Note Local connect feature is not supported on the Cisco ASR 903 router. However, to simulate a local connect scenario, configure the connecting EFPs on the same bridge domain and disable the mac-learning on the bridge domain by setting the MAC limit to 0. Use the **mac-address-table limit bdomain** *num* **maximum** *0* **action limit** command to disable mac-learning on the router.

When the total number of addresses in a bridge-domain exceeds the maximum number, the router takes a violation action. You can enable the following actions:

- Warning—The router sends a syslog message and takes no further action. The router continues learning new MAC addresses and forwarding traffic.

- Limit—The router sends a syslog message and generates a trap; MAC learning is disabled on the bridge-domain until the recovery mechanism activates. Flooding of frames with new MAC addresses continues; to disable flooding, use the flood keyword. Flooding continues once the total number of MAC entries drops below the threshold value. This option applies only when you configure the limit keyword.

Note The threshold value must be 80% of the maximum value configured for the recovery mechanism.

- Shutdown—If the number of addresses exceeds the maximum (MAX) value, the router sends a syslog message and moves the bridge-domain (bdomain) to a disabled state. To restore the bridge-domain, disable and re-enable the mac-limiting feature.

Before You Begin

SUMMARY STEPS

1. **configure terminal**
2. **mac-address-table limit [bridge-domain id] [maximum num] [action {warning | limit | shutdown}] [flood]**
3. **end**
4. **show mac-address-table limit [bridge-domain id]**
5. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**mac-address-table limit [bridge-domain id] [maximum num] [action {warning | limit | shutdown}] [flood]**	Sets the specific limit and any optional actions to be imposed at the bridge-domain level. The default **maximum** value is 500.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show mac-address-table limit [bridge-domain id]**	Displays the information about the MAC-address table.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Example of Enabling Per-Bridge-Domain MAC Limiting

This example shows how to enable per-bridge-domain MAC limiting. The first instance of the mac-address-table limit command enables MAC limiting. The second instance of the command sets the limit and any optional actions to be imposed at the bridge-domain level.

- ```
  Router# enable
  Router# configure terminal
  Router(config)# mac-address-table limit
  Router(config)# mac-address-table limit bridge-domain 10 maximum 100 action limit flood
  Router(config)# end

  Router#show mac-address-table limit bdomain 10
    bdomain       action      flood       maximum     Total entries     Current state
  -------------+----------+------------+------------+---------------+---------------
     10           limit      Disable        100            0             Within Limit
  ```
  ```