Network Management Configuration Guide, Cisco Catalyst IE9300 Rugged Series Switches

First Published: 2022-04-26

Last Modified: 2023-11-20

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

Full Cisco Trademarks with Software License

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions, and services, visit Cisco DevNet.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

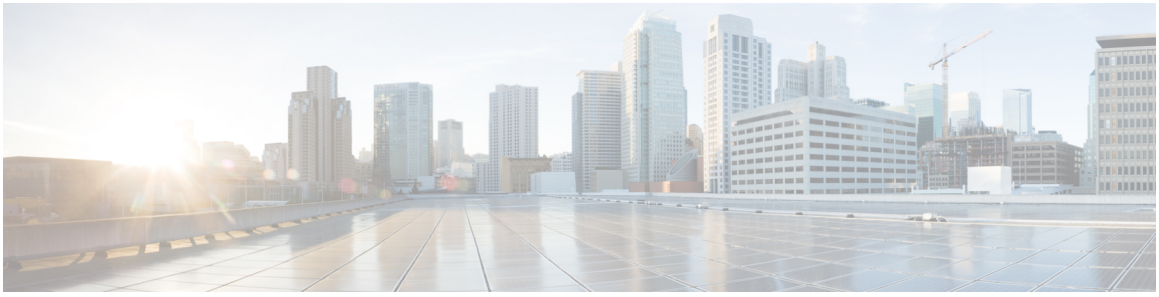
Cisco Bug Search Tool (BST) is a gateway to the Cisco bug-tracking system, which maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. The BST provides you with detailed defect information about your products and software.

Documentation Feedback

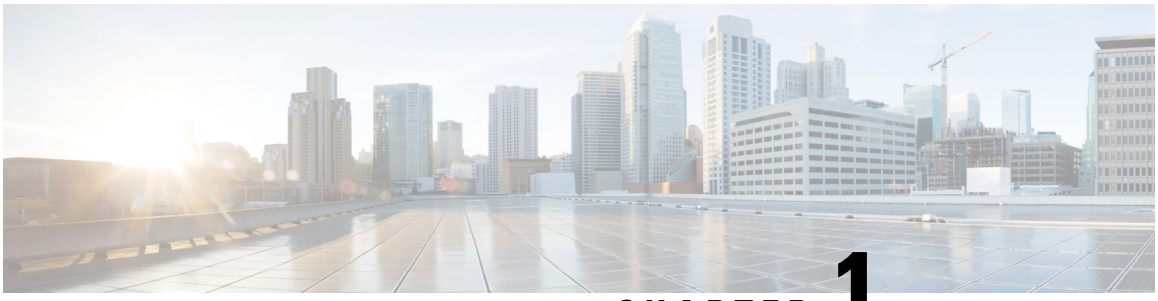
To provide feedback about Cisco technical documentation, use the feedback form available in the right pane of every online document.

Bias Free Language

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.



CONTENTS



CHAPTER 1

ERSPAN

ERSPAN

The Cisco Encapsulated Remote Switched Port Analyzer (ERSPAN) feature allows you to monitor traffic on ports or VLANs, and send the monitored traffic to destination ports over a Layer 3 (IP) network using Generic Routing Encapsulation (GRE) encapsulation. ERSPAN sends traffic to a network analyzer, such as a Switch Probe device or a Remote Monitoring (RMON) probe. ERSPAN supports source ports, source VLANs, and destination ports on different devices, which help remote monitoring of multiple devices across a network.

ERSPAN supports encapsulated packets of up to 9180 bytes. ERSPAN consists of an ERSPAN source session, routable ERSPAN GRE-encapsulated traffic, and an ERSPAN destination session.

You can configure an ERSPAN source session, an ERSPAN destination session, or both on a device. A device on which only an ERSPAN source session is configured is called an ERSPAN source device. A device on which only an ERSPAN destination session is configured is called an ERSPAN termination device. A device can act as both; an ERSPAN source device and a termination device.

Over-subscription of traffic can lead to a drop in management traffic on the destination device. To avoid over-subscription, ensure that the destination session is configured and is working on the destination device, before configuring a source session on the source device.

For a source port or a source VLAN, the ERSPAN can monitor the ingress, egress, or both ingress and egress traffic. By default, ERSPAN monitors all traffic, including multicast, and Bridge Protocol Data Unit (BPDU) frames.

A device supports up to 66 sessions. A maximum of eight source sessions can be configured and the remaining sessions can be configured as RSPAN destinations sessions. A source session can be a local SPAN source session or an RSPAN source session or an ERSPAN source session.

An ERSPAN source session is defined by the following parameters:

- A session ID.
- ERSPAN flow ID.

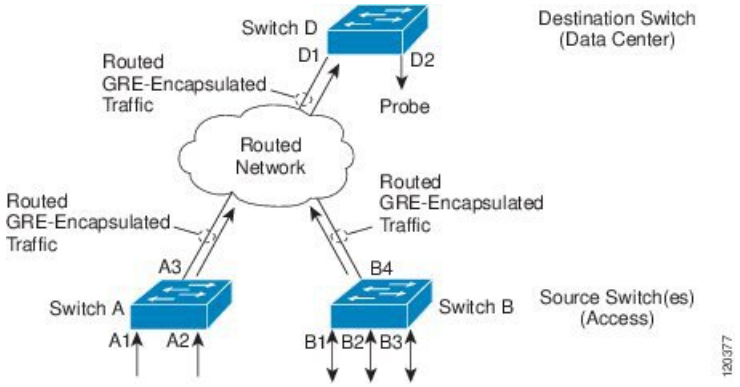
- List of source ports or source VLANs that are monitored by the session.
- Optional attributes, such as, IP type of service (ToS) and IP Time to Live (TTL), related to the Generic Routing Encapsulation (GRE) envelope.
- The destination and origin IP addresses. These are used as the destination and source IP addresses of the GRE envelope for the captured traffic, respectively.

Note

- ERSPAN source sessions do not copy ERSPAN GRE-encapsulated traffic from source ports. Each ERSPAN source session can have either ports or VLANs as sources, but not both.
- IPv4 delivery and transport headers are supported; including Type-II and Type-III headers.

  Port channel and switch virtual interface (SVI) are supported.

Figure 1: ERSPAN Configuration



Information About Configuring ERSPAN

The following sections provide information about configuring ERSPAN.

Restrictions for Configuring ERSPAN

The following restrictions apply for this feature:

- Truncation is supported only on IPv4 spanned packets and not on Layer 2 packets without an IP header.
- An ERSPAN destination interface can be part of only one session. The same destination interface cannot be configured for multiple ERSPANs/SPANs.
- You can configure either a list of ports or a list of VLANs as a source, but cannot configure both for a given session.
- Filter IP/MAC/VLAN access-group and filter SGT cannot be configured at the same time.

- When a session is configured through the ERSPAN CLI, the session ID and the session type cannot be changed. To change them, you must use the **no** form of the commands to remove the session and then reconfigure it.
- ERSPAN source sessions do not copy locally-sourced RSPAN VLAN traffic from source trunk ports that carry RSPAN VLANs.
- ERSPAN source sessions do not copy locally-sourced ERSPAN Generic routing encapsulation (GRE)-encapsulated traffic from source ports.
- Disabling the **ip routing** command for IPv4 connections stops ERSPAN traffic flow to the destination port.

ERSPAN Sources

The Cisco ERSPAN feature supports the following sources:

- Source ports: A source port that is monitored for traffic analysis. Source ports in any VLAN can be configured and trunk ports can be configured as source ports along with nontrunk source ports.
- Source VLANs: A VLAN that is monitored for traffic analysis.

ERSPAN Destination Ports

A destination port is a Layer 2 or Layer 3 port to which ERSPAN source sends traffic for analysis.

When you configure a port as a destination port, it can no longer receive any traffic. The port is dedicated for use only by the ERSPAN feature. An ERSPAN destination port does not forward any traffic except that required for the ERSPAN session. You can configure trunk ports as destination ports, which allows destination trunk ports to transmit encapsulated traffic.

SGT-Based ERSPAN

A Security Group Tag (SGT) is a 16-bit value that the Cisco Identity Services Engine (ISE) assigns to the user or endpoint session upon login. The network infrastructure views the SGT as another attribute to assign to the session and inserts the Layer 2 tag to all traffic from that session. A platform can support a maximum of 50 SGT policies per session.

On an existing flow-based SPAN (FSPAN) or VLAN filter session, SGT filtering configurations are not allowed.

Prerequisites for Configuring ERSPAN

Apply the Access control list (ACL) filter before sending the monitored traffic on to the tunnel.

How to Configure ERSPAN

You can use the commands given here to troubleshoot issues related to Encapsulated Remote Switched Port Analyzer (ERSPAN) and to capture and display network traffic in real-time on specific network device interfaces.

- debug monitor erspan
- debug monitor capture

The following sections provide information about how to configure ERSPAN.

Configuring an ERSPAN Source Session

The ERSPAN source session defines the session configuration parameters and the ports or VLANs to be monitored. To define an IPv4 ERSPAN source session, complete the following procedure:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **monitor session** *span-session-number* **type erspan-source**
4. **description** *string*
5. [**no**] **header-type 3**
6. **source** {**interface** *interface-type interface-number* | **vlan** *vlan-id*} [**,** | **-** | **both** | **rx** | **tx**]
7. **filter** {**ip access-group** {*standard-access-list* | *expanded-access-list* | *acl-name* } | **mac access-group** *acl-name* | **sgt** *sgt-ID* [**,** | **-**] | **vlan** *vlan-ID* [**,** | **-**]}
8. **destination**
9. **erspan-id** *erspan-flow-id*
10. **ip address** *ip-address*
11. **ip dscp** *dscp-value*
12. **ip ttl** *ttl-value*
13. **mtu** *mtu-size*
14. **origin ip-address** *ip-address*
15. **vrf** *vrf-id*
16. **exit**
17. **no shutdown**
18. **end**

DETAILED STEPS

Procedure

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

	Command or Action	Purpose
	Example: `Device> enable`	Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**monitor session** *span-session-number* **type erspan-source** **Example:** `Device(config)# monitor session 1 type erspan-source`	Defines an ERSPAN source session using the session ID and the session type, and enters ERSPAN monitor source session configuration mode. • The *span-session-number* argument range is from 1 to 66. The same session number cannot be used more than once. • The session IDs for source sessions or destination sessions are in the same global ID space, so each session ID is globally unique for both session types. • The session ID (configured by the *span-session-number* argument) and the session type (configured by the **erspan-source** keyword) cannot be changed once entered. Use the **no** form of this command to remove the session and then re-create the session, with a new session ID or a new session type.
Step 4	**description** *string* **Example:** `Device(config-mon-erspan-src)# description source1`	(Optional) Describes the ERSPAN source session. • The *string* argument can be up to 240 characters and cannot contain special characters or spaces.
Step 5	[**no**] **header-type 3** **Example:** `Device(config-mon-erspan-src)# header-type 3`	(Optional) Configures a switch to Type-III ERSPAN header. The default type is Type-II ERSPAN header.
Step 6	**source** {**interface** *interface-type interface-number* | **vlan** *vlan-id*} [**,** | **-** | **both** | **rx** | **tx**] **Example:** `Device(config-mon-erspan-src)# source interface fastethernet 0/1 rx`	Configures the source interface or the VLAN, and the traffic direction to be monitored.
Step 7	**filter** {**ip access-group** {*standard-access-list* | *expanded-access-list* | *acl-name* } | **mac access-group** *acl-name* | **sgt** *sgt-ID* [**,** | **-**] | **vlan** *vlan-ID* [**,** | **-**]} **Example:** `Switch(config-mon-erspan-src)# filter vlan 3`	(Optional) Configures source VLAN filtering when the ERSPAN source is a trunk port. **Note** You cannot include source VLANs and filter VLANs in the same session.

	Command or Action	Purpose
Step 8	**destination** **Example:** `Device(config-mon-erspan-src)# destination`	Enters ERSPAN source session destination configuration mode.
Step 9	**erspan-id** *erspan-flow-id* **Example:** `Device(config-mon-erspan-src-dst)# erspan-id 100`	Configures the ID used by source and destination sessions to identify the ERSPAN traffic, which must also be entered in the ERSPAN destination session configuration.
Step 10	**ip address** *ip-address* **Example:** `Device(config-mon-erspan-src-dst)# ip address 10.1.0.2`	Configures the IP address that is used as the destination of the ERSPAN traffic.
Step 11	**ip dscp** *dscp-value* **Example:** `Device(config-mon-erspan-src-dst)# ip dscp 10`	(Optional) Enables the use of IP differentiated services code point (DSCP) for packets that originate from a circuit emulation (CEM) channel.
Step 12	**ip ttl** *ttl-value* **Example:** `Device(config-mon-erspan-src-dst)# ip ttl 32`	(Optional) Configures the IP TTL value of packets in the ERSPAN traffic.
Step 13	**mtu** *mtu-size* **Example:** `Device(config-mon-erspan-src-dst)# mtu 512`	Configures the MTU size for truncation. Any ERSPAN packet that is larger than the configured MTU size is truncated to the configured size. The MTU size range is 176 to 9000 bytes. The default value is 9000 bytes.
Step 14	**origin ip-address** *ip-address* **Example:** `Device(config-mon-erspan-src-dst)# origin ip address 10.10.0.1`	Configures the IP address used as the source of the ERSPAN traffic.
Step 15	**vrf** *vrf-id* **Example:** `Device(config-mon-erspan-src-dst)# vrf 1`	(Optional) Configures the VRF name to use instead of the global routing table.
Step 16	**exit** **Example:** `Device(config-mon-erspan-src-dst)# exit`	Exits ERSPAN source session destination configuration mode, and returns to ERSPAN source session configuration mode.
Step 17	**no shutdown** **Example:** `Device(config-mon-erspan-src)# no shutdown`	Enables the configured sessions on an interface.
Step 18	**end** **Example:**	Exits ERSPAN source session configuration mode, and returns to privileged EXEC mode.

	Command or Action	Purpose
	`Device(config-mon-erspan-src)# end`	

Configuring an ERSPAN Destination Session

The ERSPAN destination session defines the session configuration parameters and the ports that receive the monitored traffic. To define an IPv4 ERSPAN destination session, complete the following procedure:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **monitor session** *session-number* **type erspan-destination**
4. **description** *string*
5. **destination interface** *interface-type interface-number*
6. **source**
7. **erspan-id** *erspan-flow-id*
8. **ip address** *ip-address* [**force**]
9. **vrf** *vrf-id*
10. **no shutdown**
11. **end**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**monitor session** *session-number* **type erspan-destination** **Example:** `Device(config)# monitor session 1 type erspan-destination`	Defines an ERSPAN destination session using the session ID and the session type, and enters ERSPAN monitor destination session configuration mode. • The *session-number* argument range is from 1 – 66. The session number must be unique and cannot be used more than once. • The session IDs for source sessions or destination sessions are in the same global ID space, so each session ID is globally unique for both session types.

	Command or Action	Purpose
		• The session ID (configured by the *session-number* argument) and the session type (configured by the **erspan-destination**) cannot be changed once entered. Use the **no** form of this command to remove the session, and then recreate the session with a new session ID or a new session type.
Step 4	**description** *string* **Example:** `Device(config-mon-erspan-dst)# description source1`	(Optional) Describes the ERSPAN destination session. • The *string* argument can be up to 240 characters in length and cannot contain special characters or spaces.
Step 5	**destination interface** *interface-type interface-number* **Example:** `Device(config-mon-erspan-dst)# destination interface GigabitEthernet1/0/1`	Associates the ERSPAN destination session number with source ports, and selects the traffic direction to be monitored.
Step 6	**source** **Example:** `Device(config-mon-erspan-dst)# source`	Enters ERSPAN destination session source configuration mode.
Step 7	**erspan-id** *erspan-flow-id* **Example:** `Device(config-mon-erspan-dst-src)# erspan-id 100`	Configures the ID used by source and destination sessions to identify the ERSPAN traffic, which must also be entered in the ERSPAN source session configuration.
Step 8	**ip address** *ip-address* [**force**] **Example:** `Device(config-mon-erspan-dst-src)# ip address 10.1.0.2`	Configures the IP address that is used as the destination of the ERSPAN traffic. • This IP address must be an address on a local interface or loopback interface, and match the address on the destination switch. • The **ip address** *ip-address* **force** command changes the destination IP address for all ERSPAN destination sessions.
Step 9	**vrf** *vrf-id* **Example:** `Device(config-mon-erspan-dst-src)# vrf 1`	(Optional) Configures the VRF name to use instead of the global routing table.
Step 10	**no shutdown** **Example:** `Device(config-mon-erspan-dst-src)# no shutdown`	Enables the configured sessions on an interface.
Step 11	**end** **Example:** `Device(config-mon-erspan-dst-src)# end`	Exits ERSPAN destination session source configuration mode, and returns to privileged EXEC mode.

Configuration Examples for ERSPAN

The following sections provide configuration examples for ERSPAN.

Example: Configuring an ERSPAN Source Session

The following example shows how to configure an ERSPAN source session:

```
Device> enable
Device# configure terminal
Device(config)# monitor session 1 type erspan-source
Device(config-mon-erspan-src)# description source1
Device(config-mon-erspan-src)# source interface GigabitEthernet 1/0/1 rx
Device(config-mon-erspan-src)# source interface GigabitEthernet 1/0/4 - 8 tx
Device(config-mon-erspan-src)# source interface GigabitEthernet 1/0/3
Device(config-mon-erspan-src)# destination
Device(config-mon-erspan-src-dst)# erspan-id 100
Device(config-mon-erspan-src-dst)# ip address 10.1.0.2
Device(config-mon-erspan-src-dst)# ip dscp 10
Device(config-mon-erspan-src-dst)# ip ttl 32
Device(config-mon-erspan-src-dst)# mtu 512
Device(config-mon-erspan-src-dst)# origin ip address 10.10.0.1
Device(config-mon-erspan-src-dst)# vrf monitoring
Device(config-mon-erspan-src-dst)# exit
Device(config-mon-erspan-src)# no shutdown
Device(config-mon-erspan-src)# end
```

Example: Configuring an ERSPAN Destination Session

The following example shows how to configure an ERSPAN destination session:

```
Device(config)# monitor session 1 type erspan-destination
Device(config-mon-erspan-dst)# destination interface GigabitEthernet1/0/11
Device(config-mon-erspan-dst)# destination interface GigabitEthernet1/0/1
Device(config-mon-erspan-dst)# source
Device(config-mon-erspan-dst-src)# erspan-id 100
Device(config-mon-erspan-dst-src)# ip address 10.1.0.2
```

The following example shows how to configure a source VRF for an ERSPAN destination session:

```
Device(config)# monitor session 1 type erspan-destination
Device(config-mon-erspan-dst)# destination interface GigabitEthernet1/0/11
Device(config-mon-erspan-dst)# destination interface GigabitEthernet1/0/1
Device(config-mon-erspan-dst)# source
Device(config-mon-erspan-dst-src)# erspan-id 100
Device(config-mon-erspan-dst-src)# ip address 10.1.0.2
Device(config-mon-erspan-dst-src)# vrf 1
```

Verifying ERSPAN

To verify the ERSPAN configuration, use the following commands:

The following is sample output from the **show monitor session** command:

```
Device# show monitor session 53

Session 53
----------
Type                    : ERSPAN Source Session
Status                  : Admin Enabled
Source Ports            :
MTU                     : 9000
```

The following is sample output from the **show platform software monitor session** command:

```
Device# show platform software monitor session 53

Span Session 53 (FED Session 0):
Type: ERSPAN Source
Prev type: Unknown
Ingress Src Ports:
Egress Src Ports:
Ingress Local Src Ports: (null)
Egress Local Src Ports: (null)
Destination Ports:
Ingress Src Vlans:
Egress Src Vlans:
Ingress Up Src Vlans: (null)
Egress Up Src Vlans: (null)
Src Trunk filter Vlans:
RSPAN dst vlan: 0
RSPAN src vlan: 0
RSPAN src vlan sav: 0
Dest port encap = 0x0000
Dest port ingress encap = 0x0000
Dest port ingress vlan = 0x0
SrcSess: 1 DstSess: 0 DstPortCfgd: 0 RspnDstCfg: 0 RspnSrcVld: 0
DstCliCfg: 0 DstPrtInit: 0 PsLclCfgd: 0
Flags: 0x00000000
Remote dest port: 0 Dest port group: 0
FSPAN disabled
FSPAN not notified
ERSPAN Id : 0
ERSPAN Org Ip: 0.0.0.0
ERSPAN Dst Ip: 0.0.0.0
ERSPAN Ip Ttl: 255
ERSPAN DSCP : 0
ERSPAN MTU : 1500 >>>>
ERSPAN VRFID : 0
ERSPAN State : Disabled
ERSPAN Tun id: 61
ERSPAN header-type: 2
ERSPAN SGT :
```

The following is sample output from the **show monitor session erspan-source detail** command:

```
Device# show monitor session erspan-source detail

Type                    : ERSPAN Source Session
Status                  : Admin Enabled
Description             : -
Source Ports            :
    RX Only             : None
    TX Only             : None
    Both                : None
Source Subinterfaces    :
    RX Only             : None
```

```
    TX Only              : None
    Both                 : None
Source VLANs             :
    RX Only              : None
    TX Only              : None
    Both                 : None
Source Drop-cause        : None
Source EFPs              :
    RX Only              : None
    TX Only              : None
    Both                 : None
Source RSPAN VLAN        : None
Destination Ports        : None
Filter VLANs             : None
Filter SGT               : None
Dest RSPAN VLAN          : None
IP Access-group          : None
MAC Access-group         : None
IPv6 Access-group        : None
Filter access-group  :None
smac for wan interface   : None
dmac for wan interface   : None
Destination IP Address   : 192.0.2.1
Destination IPv6 Address : None
Destination IP VRF       : None
MTU                      : 1500
Destination ERSPAN ID    : 251
Origin IP Address        : 10.10.10.216
Origin IPv6 Address      : None
IP QOS PREC              : 0
IPv6 Flow Label          : None
IP TTL                   : 255
ERSPAN header-type       : 3
```

The following output from the **show capability feature monitor erspan-source** command displays information about the configured ERSPAN source sessions:

```
Device# show capability feature monitor erspan-source

ERSPAN Source Session:ERSPAN Source Session Supported: TRUE
No of Rx ERSPAN source session: 8
No of Tx ERSPAN source session: 8
ERSPAN Header Type supported: II and III
ACL filter Supported: TRUE
SGT filter Supported: TRUE
Fragmentation Supported: TRUE
Truncation Supported: FALSE
Sequence number Supported: FALSE
QOS Supported: TRUE
```

The following output from the **show capability feature monitor erspan-destination** command displays all the configured global built-in templates:

```
Device# show capability feature monitor erspan-destination

ERSPAN Destination Session:ERSPAN Destination Session Supported: TRUE
Maximum No of ERSPAN destination session: 8
ERSPAN Header Type supported: II and III
```

Additional References

RFCs

Standard/RFC	Title
RFC 2784	Generic Routing Encapsulation (GRE)

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

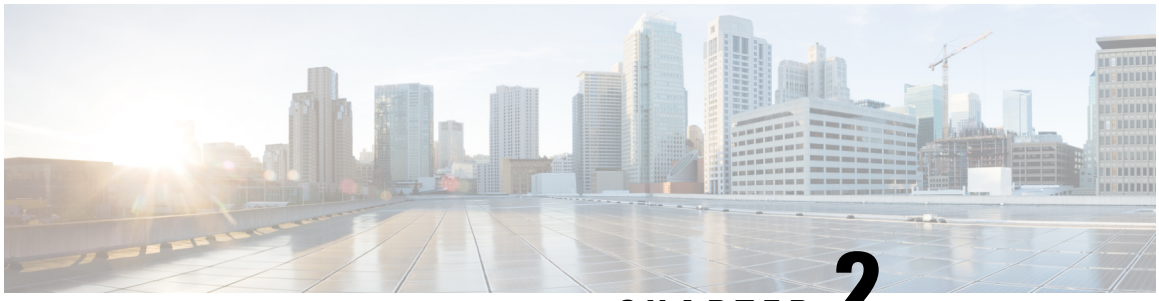
Feature History for Configuring ERSPAN

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1: Feature Information for Configuring ERSPAN

Feature Name	Releases	Feature Information
ERSPAN	Cisco IOS XE Cupertino 17.7.1	This feature was introduced for Cisco Catalyst IE9300 Rugged Series Switches.



CHAPTER 2

Configuring Swap Drive

Swapping the External Drive

Swap Drive and Disaster Recovery

The swap drive feature enables you to replace a failed switch quickly and easily. You simply move an external secure digital (SD) card or USB drive with a backup of the original switch to the new. After you turn on the new switch, it comes up with the same image and configuration as the original switch.

The swap drive feature is available for Cisco Catalyst IE9300 Rugged Series Switches beginning in Cisco IOS XE Cupertino 17.9.1. Each Cisco Catalyst IE9300 Rugged Series Switch has a secure digital (SD) cardslot and a USB-A port. See the *Cisco Catalyst IE9300 Rugged Series Switch Hardware Installation Guide* on Cisco.com for information about the switch SD cardslot and USB port.

In order to restore the settings to the new switch, you must have previously synchronized the original switch with the SD card or USB drive. Although you can run synchronization at any time manually, we recommend that you configure synchronization to occur automatically at set times.

When you request synchronization—either manually or automatically—the switch checks for any discrepancies between the internal flash drive on the switch and the SD card.

When an SD card is formatted on the switch, the card is formatted with the Disk Operating System Filing System (DOSFS), a platform-independent industry-standard file system that is supported on various Cisco switches and routers. The switch does not support third-party SD cards or SD High Capacity (SDHC) cards

If the write-protect switch on the SD card is in the lock position, the switch can read data on the card and use files on the SD card during the boot process, but cannot write updates and files to the card.

You can use a USB 2.0 drive as you would use an SD card for the swap drive feature.

Note For the swap drive feature to work, Cisco IOS XE Cupertino 17.9.1. must be installed on both the original switch and the replacement switch.

How Swap Drive Works

Swap drive consists of two main stages: backup of the original switch and recovery of the image and configuration on the new switch.

Backup duplicates the entire system in the external SD card or USB drive. You trigger backup by entering a CLI command, either to do a one-time sync or to set up automatic periodic syncs. If the switch has already been backed up, only changes since the last backup are duplicated in the external drive.

Restore occurs automatically, when you insert the external drive in the new switch and then power on the switch. The new switch looks for an SD card and scans it to see if an image and configuration are present. If they are present, the switch then copies them to internal flash and comes up with the image and configuration of the original system.

If an SD card isn't present or doesn't have the original switch's image and configuration, the switch then looks for and scans the USB drive. If they are present on the USB drive, the switch comes up with the original switch's image and configuration. If the image and configuration are not present on any external media, the system asks the user whether to continue with the initial configuration on the new switch.

For swap drive instructions, see Swap the External Drive; for a list of CLI commands, see Swap Drive CLI Commands. Both sections are in this guide.

Swap the External Drive

You remove the SD drive from the failed switch, and insert it into the new switch, then power on the new switch. A new switch is a switch without a startup configuration file. This is the case if the new switch has never been deployed before.

Before you begin

Cable the new switch correctly and make sure that it is powered off before you transfer the SD card or USB drive.

Procedure

Step 1 On the failed switch, remove the SD card or USB drive.

Note The SD card and USB drive are hot-swappable, but do not remove it from the switch while sdflash write is in progress.

Step 2 On the new switch, ensure that the SD card or USB drive is oriented properly, and then press it into the slot on the switch until it is seated.

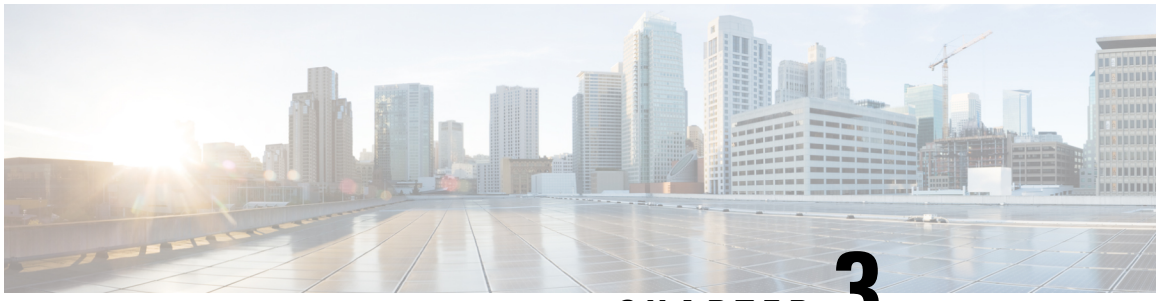
Step 3 Power on the new switch.
The image and configuration of the failed switch are transferred to the new one.

Swap Drive CLI Commands

The following table lists the CLI commands for the swap drive feature.

Note Perform all **auto sync** commands in configuration mode.

Command	Description
• **sync sdflash:** • **sync usbflash1:**	Syncs the switch image and configuration files from internal flash to the SD or USB drive.
• **sync sdflash: ios-image** • **sync usbflash1: ios-image**	Syncs the switch image from the internal flash to the SD or USB drive.
• **sync sdflash:skip config** • **sync usbflash1: skip config**	Syncs the switch image from the internal flash to the SD or USB drive but does not sync the configuration.
• **sync sdflash:skip ios-image** • **sync usbflash1: skip ios-image**	Syncs the configuration files om the internal flash to the SD or USB drive but does not sync the image.
sync restore-bundle	Copies the bundle image in the new switch instead of installing it during restore.
[no] auto sync enable	Enables or disables the auto sync feature. **Note** Auto sync is disabled by default. Unless you enable it, you cannot use other options for the feature.
auto sync config [usbflash1|sdflash]:	Sets the configuration to run during the sync.
[no] auto sync run time: [hh:mm:ss]	The time when sync is performed. The default is 00:00:00.
show sync status	Displays the last sync time and status. **Note** If a type-6 password is configured, the status shows the configuration as out of sync with the message that type-6 passwords are not synced.
show auto sync configuration	Displays all the configuration settings.
show auto sync status	Displays the last auto sync time and status.



CHAPTER 3

VLAN Mapping

VLAN Mapping

In a typical deployment of VLAN mapping, you want the service provider to provide a transparent switching infrastructure that includes customers' switches at the remote location as a part of the local site. This allows customers to use the same VLAN ID space and run Layer 2 control protocols seamlessly across the provider network. In such scenarios, we recommend that service providers do not impose their VLAN IDs on their customers.

One way to establish translated VLAN IDs (S-VLANs) is to map customer VLANs to service-provider VLANs (called VLAN ID mapping) on trunk ports connected to a customer network. Packets entering the port are mapped to a service provider VLAN (S-VLAN) based on the port number and the packet's original customer VLAN-ID (C-VLAN).

Service providers's internal assignments might conflict with a customer's VLAN. To isolate customer traffic, a service provider could decide to map a specific VLAN into another one while the traffic is in its cloud.

Switch Support

VLAN Mapping is supported on all models of Cisco Catalyst IE9300 Rugged Series Switches. The feature is available with a Network Essentials or Network Advantage license.

Deployment Example

All forwarding operations on the switch are performed using S-VLAN and not C-VLAN information because the VLAN ID is mapped to the S-VLAN on ingress.

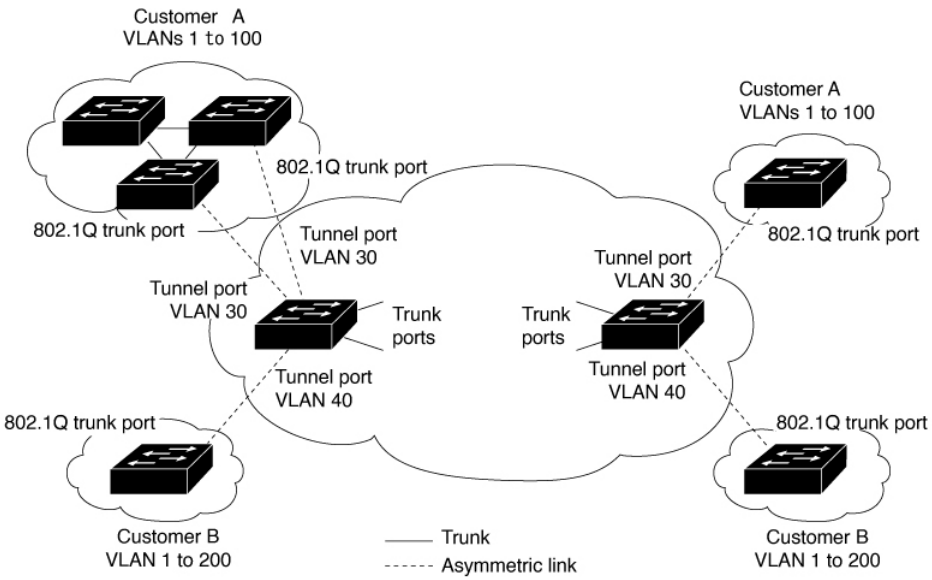
Note When you configure features on a port configured for VLAN mapping, you always use the S-VLAN rather than the customer VLAN-ID (C-VLAN). One-to-one VLAN mapping is not supported at this time.

On an interface configured for VLAN mapping, the specified C-VLAN packets are mapped to the specified S-VLAN when they enter the port. Symmetrical mapping to the customer C-VLAN occurs when packets exit the port.

The switch supports the following types of VLAN mapping on trunk ports:

Mapping Customer VLANs to Service-Provider VLANs

Figure 2: QnQ Topology



The preceding illustration shows a topology where Customer A and Customer B use the same VLANs in multiple sites on different sides of a service-provider network. You map the customer VLAN IDs to service-provider VLAN IDs for packet travel across the service-provider backbone. The customer VLAN IDs are retrieved at the other side of the service-provider backbone for use in the other customer site. Configure the same set of VLAN mappings at a customer-connected port on each side of the service-provider network.

Selective QnQ

Selective QnQ maps the specified customer VLANs entering the UNI to the specified S-VLAN ID. The S-VLAN ID is added to the incoming unmodified C-VLAN and the packet travels the service provider network double-tagged. At the egress, the S-VLAN ID is removed and the customer VLAN-ID is retained on the packet. By default, packets that do not match the specified customer VLANs are dropped.

QnQ on a Trunk Port

QnQ on a trunk port maps all the customer VLANs entering the UNI to the specified S-VLAN ID. Similar to Selective QnQ, the packet is double-tagged and at the egress, the S-VLAN ID is removed.

Configuration Guidelines for VLAN Mapping

Note By default, no VLAN mapping is configured.

Guidelines include the following:

- If the VLAN mapping is enabled on an EtherChannel, the configuration does not apply to all member ports of the EtherChannel bundle and applies only to the EtherChannel interface.
- If the VLAN mapping is enabled on an EtherChannel and a conflicting mapping is enabled on a member port, then the port is removed from the EtherChannel.
- The member port of an EtherChannel is removed from the EtherChannel bundle if the mode of the port is changed to anything other than 'trunk' mode.
- To process control traffic consistently, either enable Layer 2 protocol tunneling (recommended), as follows:

```
!
Device(config)# interface Gig 1/0/1
Device(config-if)# switchport mode access
Device(config-if)# l2protocol-tunnel stp
Device(config-if)# end
```

  or insert a BPDU filter for spanning tree, as follows:

```
Current configuration : 153 bytes
!
Device(config)# interface Gig 1/0/1
Device(config-if)# switchport mode trunk
Device(config-if)# switchport vlan mapping 10 20
Device(config-if)# spanning-tree bpdufilter enable
Device(config-if)# end
```

- Default native VLANs, user-configured native VLANs, and reserved VLANs (range 1002-1005) cannot be used for VLAN mapping.
- PVLAN support is not available when VLAN mapping is configured.

Configuration Guidelines for Selective QnQ

- S-VLAN should be created and present in the allowed VLAN list of the trunk port where Selective QnQ is configured.
- When Selective QnQ is configured, the device supports Layer 2 protocol tunneling for CDP, STP, LLDP, and VTP.
- IP routing is not supported on Selective QnQ enabled ports.
- IPSG is not supported on Selective QnQ enabled ports.

Configuration Guidelines for QnQ on a Trunk port

- S-VLAN should be created and present in the allowed VLAN list of the trunk port where QnQ on a trunk port is configured.
- When QnQ on a trunk port is configured, the device supports Layer 2 protocol tunneling for CDP, STP, LLDP, and VTP.
- Ingress and egress SPAN, and RSPAN are supported on trunk ports with QnQ enabled.
- When QnQ is enabled, the SPAN filtering can be enabled to monitor only the traffic on the mapped VLAN, that is, S-VLANs.
- IGMP snooping is not supported on the C-VLAN.

Configuring VLAN Mapping

The following sections provide information about configuring VLAN mapping:

Configure Selective QnQ on a Trunk Port

To configure VLAN mapping for selective QnQ on a trunk port, complete the following steps:

Note You cannot configure one-to-one mapping and selective QnQ on the same interface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *interface-id*
4. **switchport mode trunk**
5. **switchport vlan mapping** *vlan-id* **dot1q-tunnel** *outer vlan-id*
6. **switchport vlan mapping default dot1q-tunnel** *vlan-id*
7. **exit**
8. **spanning-tree bpdufilter enable**
9. **end**
10. **show interfaces** *interface-id* **vlan mapping**
11. **copy running-config startup-config**

DETAILED STEPS

Procedure

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

	Command or Action	Purpose
	Example: `Device> enable`	Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *interface-id* **Example:** `Device(config)# interface gigabitethernet1/0/1`	Enters interface configuration mode for the interface connected to the service-provider network. You can enter a physical interface or an EtherChannel port channel.
Step 4	**switchport mode trunk** **Example:** `Device(config-if)# switchport mode trunk`	Configures the interface as a trunk port.
Step 5	**switchport vlan mapping** *vlan-id* **dot1q-tunnel** *outer vlan-id* **Example:** `Device(config-if)# switchport vlan mapping 16 dot1q-tunnel 64`	Enters the VLAN IDs to be mapped: • vlan-id : The customer VLAN ID (C-VLAN) entering the switch from the customer network. The range is from 1 to 4094. You can enter a string of VLAN-IDs. • outer-vlan-id: The outer VLAN ID (S-VLAN) of the service provider network. The range is from 1 to 4094. Use the no form of this command to remove the VLAN mapping configuration. Entering the **no switchport vlan mapping all** command deletes all mapping configurations.
Step 6	**switchport vlan mapping default dot1q-tunnel** *vlan-id* **Example:** `Device(config-if)# switchport vlan mapping default dot1q-tunnel 22`	Specifies that all unmapped packets on the port are forwarded with the specified S-VLAN. By default, packets that do not match the mapped VLANs, are dropped. Untagged traffic are forwarded without dropping.
Step 7	**exit** **Example:** `Device(config-if)# exit`	Returns to global configuration mode.
Step 8	**spanning-tree bpdufilter enable** **Example:** `Device(config)# spanning-tree bpdufilter enable`	Inserts a BPDU filter for spanning tree. **Note** To process control traffic consistently, either enable Layer 2 protocol tunneling (recommended) or insert a BPDU filter for spanning tree.
Step 9	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

	Command or Action	Purpose
Step 10	**show interfaces** *interface-id* **vlan mapping** **Example:** `Device# show interfaces gigabitethernet1/0/1 vlan mapping`	Verifies the configuration.
Step 11	**copy running-config startup-config** **Example:** `Device# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Example

This example shows how to configure selective QnQ mapping on the port so that traffic with a C-VLAN ID of 2 to 5 enters the switch with an S-VLAN ID of 100. By default, the traffic of any other VLAN ID is dropped.

```
Device(config)# interface GigabitEthernet1/0/1
Device(config-if)# switchport vlan mapping 2-5 dot1q-tunnel 100
Device(config-if)# exit
```

This example shows how to configure selective QnQ mapping on the port so that traffic with a C-VLAN ID of 2 to 5 enters the switch with an S-VLAN ID of 100. The traffic of any other VLAN ID is forwarded with the S-VLAN ID of 200.

```
Device(config)# interface GigabiEthernet1/0/1
Device(config-if)# switchport vlan mapping 2-5 dot1q-tunnel 100
Device(config-if)# switchport vlan mapping default dot1q-tunnel 200
Device(config-if)# exit

Device# show vlan mapping
Total no of vlan mappings configured: 5
Interface Hu1/0/50:
VLANs on wire                   Translated VLAN     Operation
------------------------------  ---------------     --------------
2-5                                  100            selective QinQ
*                                    200            default Q
```

Configure QnQ on a Trunk Port

To configure VLAN mapping for QnQ on a trunk port, perform this task:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *interface-id*
4. **switchport mode trunk**
5. **switchport vlan mapping default dot1q-tunnel** *vlan-id*
6. **exit**
7. **spanning-tree bpdufilter enable**

8. **end**
9. **show interfaces** *interface-id* **vlan mapping**
10. **copy running-config startup-config**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *interface-id* **Example:** `Device(config)# interface gigabitethernet1/0/1`	Enters interface configuration mode for the interface connected to the service-provider network. You can enter a physical interface or an EtherChannel port channel.
Step 4	**switchport mode trunk** **Example:** `Device(config-if)# switchport mode trunk`	Configures the interface as a trunk port.
Step 5	**switchport vlan mapping default dot1q-tunnel** *vlan-id* **Example:** `Device(config-if)# switchport vlan mapping default dot1q-tunnel 16`	Specifies that all unmapped C-VLAN packets on the port are forwarded with the specified S-VLAN.
Step 6	**exit** **Example:** `Device(config-if)# exit`	Returns to global configuration mode.
Step 7	**spanning-tree bpdufilter enable** **Example:** `Device(config)# spanning-tree bpdufilter enable`	Inserts a BPDU filter for spanning tree. **Note** To process control traffic consistently, either enable Layer 2 protocol tunneling (recommended) or insert a BPDU filter for spanning tree.
Step 8	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.
Step 9	**show interfaces** *interface-id* **vlan mapping** **Example:**	Verifies the configuration.

	Command or Action	Purpose
	`Device# show interfaces gigabitethernet1/0/1 vlan mapping`	
Step 10	**copy running-config startup-config** **Example:** `Device# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Example

This example shows how to configure QnQ mapping on the port so that traffic of any VLAN ID is forwarded with the S-VLAN ID of 200.

```
Device(config)# interface gigabiethernet1/0/1
Device(config-if)# switchport vlan mapping default dot1q-tunnel 200
Device(config-if)# exit
```

Feature History for VLAN Mapping

This table provides release and related information for features explained in this chapter. These features are available on all releases subsequent to the one they were introduced in, unless noted otherwise.

Release	Feature	Feature Information
Cisco IOS XE 17.13.1	Selective QnQ	Support for features was introduced.
	QnQ on a trunk port	