LAN Switching Configuration Guide, Cisco IOS XE Release 2

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

Configuring ERSPAN

This module describes how to configure Encapsulated Remote Switched Port Analyzer (ERSPAN). ERSPAN sessions allow you to monitor traffic on one or more ports, or one or more VLANs, and send the monitored traffic to one or more destination ports.

Note The Configuring ERSPAN feature is not supported on Layer 2 switching interfaces.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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.

Restrictions for Configuring ERSPAN

- The maximum number of ERSPAN sessions on a Cisco ASR 1000 Series Router is 1024. A Cisco ASR 1000 Series Router can be used as an ERSPAN source device on which only source sessions are configured, an ERSPAN destination device on which only destination sessions are configured, or an ERSPAN source and destination device on which both source and destination sessions are configured. However, the total session number cannot exceed the maximum session number of 1024.
- The maximum port number for each ERSPAN session is 128.
- ERSPAN on Cisco ASR 1000 Series Routers supports Fast Ethernet, Gigabit Ethernet, TenGigabit Ethernet, and port-channel interfaces as source ports for a source session.

- ERSPAN users on Cisco ASR 1000 Series Routers can configure a list of ports as source or a list of VLANs as source, but cannot configure both for a given session.
- When a session is configured through the ERSPAN configuration CLI, the session ID and the session type cannot be changed. In order to change them, you must first use the **no** form of the configuration command to remove the session and then reconfigure the session.
- The **monitor session** *span-session-number* **type local** command is not supported on Cisco ASR 1000 Series Routers.
- Filter VLAN option is not functional in ERSPAN monitoring session on WAN interfaces.

Information About Configuring ERSPAN

ERSPAN Overview

ERSPAN sessions allow you to monitor traffic on one or more ports, or one or more VLANs, and send the monitored traffic to one or more destination ports. ERSPAN sends traffic to a network analyzer such as a SwitchProbe device or other Remote Monitoring (RMON) probe. ERSPAN supports source ports, source VLANs, and destination ports on different routers, which provides remote monitoring of multiple routers across your network (see the figure below).

ERSPAN consists of an ERSPAN source session, routable ERSPAN generic routing encapsulation (GRE) encapsulated traffic, and an ERSPAN destination session.

You can configure an ERSPAN source session and an ERSPAN destination session, or both, on a Cisco ASR 1000 Series Aggregation Services Router. A device that has only an ERSPAN source session configured is called an ERSPAN source device, and a device that has only an ERSPAN destination session configured is called an ERSPAN termination device. A Cisco ASR 1000 Series Router can act as both an ERSPAN source device and termination device. Also, an ERSPAN session can be terminated with a destination session on the same Cisco ASR 1000 Series Router.

An ERSPAN source session is defined by the following:

- A session ID
- A list of source ports or source VLANs to be monitored by the session
- The destination and the origin IP addresses, which are used as the destination and source IP addresses of the GRE envelope for the captured traffic, respectively
- An ERSPAN flow ID
- Optional attributes related to the GRE envelope such as IP type of service (TOS) and IP Time to Live (TTL)

For a source port or a source VLAN, the ERSPAN can monitor ingress, egress, or both ingress and egress traffic.

An ERSPAN destination session is defined by the following:

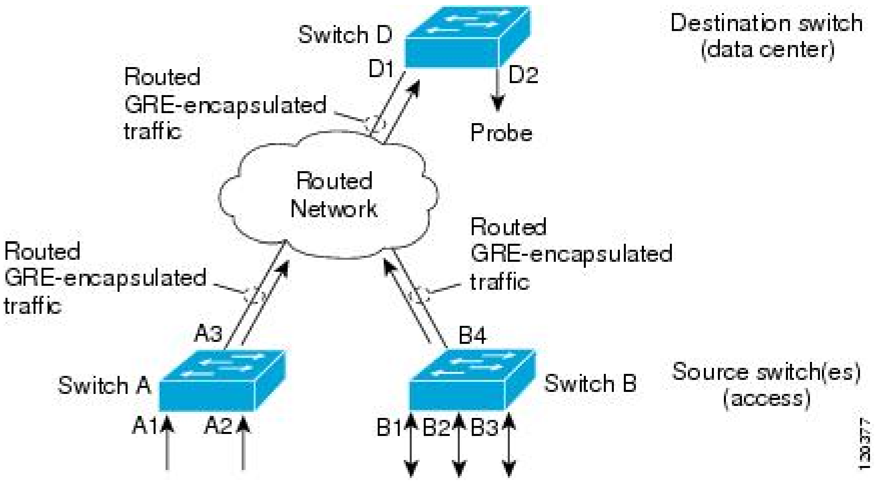
- A session ID
- A list of destination ports

- The source IP address, which is the same as the destination IP address of the corresponding source session
- The ERSPAN flow ID, which is used to match the destination session with the source session

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.

The ERSPAN source sessions copy traffic from the source ports or source VLANs and forwards the traffic using routable GRE-encapsulated packets to the ERSPAN destination session. The ERSPAN destination session switches the traffic to the destination ports.

Figure 1 ERSPAN Configuration



Monitored Traffic

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

ERSPAN Sources

The Cisco ERSPAN feature supports the following sources:

- Source ports—A source port is a port monitored for traffic analysis. You can configure source ports in any VLAN, and trunk ports can be configured as source ports along with nontrunk source ports.
- Source VLANs—A source VLAN is a VLAN monitored for traffic analysis.

  - The **tunnel** keyword was added to the **source interface** command.
  - Support was added for the following types of tunnel interfaces as source ports for a source session:
    - GRE
    - IPinIP
    - IPv6
    - IPv6 over IP tunnel
    - mGRE
    - SVTI

Note GRE, mGRE, SVTI, and IPinIP tunnel interfaces support monitoring of both IPsec-protected and non-IPsec-protected tunnel packets. Monitoring allows you to see the clear-text tunnel packet after IPsec decryption if that tunnel is IPsec protected.

The following limitations apply to the enhancements introduced in Cisco IOS XE Release 3.4S:

- Only monitoring of non-IPsec-protected tunnel packets is supported on IPv6 and IPv6 over IP tunnel interfaces.
- The enhancements apply only to ERSPAN source sessions, not to ERSPAN destination sessions.

ERSPAN has the following behavior in Cisco IOS XE Release 3.4S:

- The tunnel interface is removed from the ERSPAN database at all levels when the tunnel interface is deleted. If you want to create the same tunnel again, you must manually configure it in source monitor sessions in order to keep monitoring the tunnel traffic.
- The Layer 2 Ethernet header is feature generated with both source and destination MAC addresses set to zero.

ERSPAN Destination Ports

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

When you configure a port as a destination port, it can no longer receive any traffic. When you configure a port as a destination port, 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.

Using ERSPAN as Local SPAN

To use ERSPAN to monitor traffic through one or more ports, or one or more VLANs, you must create an ERSPAN source session and an ERSPAN destination session.

There is no restriction on whether these two sessions are created on the same router or not. If the two sessions are created on two different routers, the monitoring traffic will be forwarded from the source to the destination by ERSPAN. However, if the two sessions are created on the same router, the data flow takes place inside the router, which is similar to that of local SPAN.

The following factors are applicable while using ERSPAN as local SPAN:

- Both sessions have the same ERSPAN ID.
- Both sessions have the same IP address. This IP address is the router’s own IP address; that is, the loopback IP address or the IP address configured on any port.

Configuring ERSPAN WAN Source Support

The ERSPAN monitors and captures traffic over Ethernet ports and virtual LANs (VLANs). ERSPAN replicates the original frame and encapsulates the replicated frame inside an IP or generic routing encapsulation (GRE) packet by adding Fabric Interface Asic (FIA) entries on the WAN interface. The frame header of the replicated packet is modified for capturing. After encapsulation, ERSPAN sends the IP or GRE packet through an IP network to a device on the network. This device sends the original frame to an analyzing device that is directly connected to the network device.

How to Configure ERSPAN

ERSPAN uses separate source and destination sessions. You configure the source and destination sessions on different routers. The following sections describe how to configure ERSPAN sessions:

- Configuring an ERSPAN Source Session, page 5
- Configuring an ERSPAN Destination Session, page 8

Configuring an ERSPAN Source Session

Perform this task to configure an ERSPAN source session. The ERSPAN source session defines the session configuration parameters and the ports or VLANs to be monitored.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **monitor session** *span-session-number* **type** {**erspan-destination** | **erspan-source**}
4. **description** *string*
5. **source interface** {*if-single* | *if-list* | *if-range* | *if-mixed*} [**rx** | **tx** | **both**]
6. **source vlan** {*id-single* | *id-list* | *id-range* | *id-mixed*} [**rx** | **tx** | **both**]
7. **filter vlan** {*id-single* | *id-list* | *id-range* | *id-mixed*}
8. **destination**
9. **erspan-id** *erspan-flow-id*
10. **ip address** *ip-address*
11. **ip prec** *prec-value*
12. **ip dscp** *dscp-value*
13. **ip ttl** *ttl-value*
14. **origin ip address** *ip-address* [**force**]
15. **vrf** *vrf-id*
16. **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** *span-session-number* **type** {**erspan-destination** | **erspan-source**}
	Example:
	`Router(config)# monitor session 1 type erspan-destination`
		Defines an ERSPAN destination 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 1024. 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-destination** or **erspan-source** keyword) cannot be changed once entered. Use the **no** form of the command to remove the session and then re-create the session through the command with a new session ID or a new session type.

Step 4	**description** *string* **Example:** `Router(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	**source interface** {*if-single* | *if-list* | *if-range* | *if-mixed*} [**rx** | **tx** | **both**] **Example:** `Router(config-mon-erspan-src)# source interface GigabitEthernet1/0/1 rx`	Associates the ERSPAN source session number with the source ports, and selects the traffic direction to be monitored.
Step 6	**source vlan** {*id-single* | *id-list* | *id-range* | *id-mixed*} [**rx** | **tx** | **both**] **Example:** `Router(config-mon-erspan-src)# source vlan 1`	(Optional) Associates the ERSPAN source session number with the VLANs, and selects the traffic direction to be monitored. • You cannot mix source VLANs and filter VLANs within a session. You can have source VLANs or filter VLANs, but not both at the same time.

	Command or Action	Purpose

Step 7	**filter vlan** {*id-single* | *id-list* | *id-range* | *id-mixed*}
	Example:
	`Router(config-mon-erspan-src)# filter vlan 1`
		(Optional) Configures source VLAN filtering when the ERSPAN source is a trunk port.
		• You cannot mix source VLANs and filter VLANs within a session. You can have source VLANs or filter VLANs, but not both at the same time.

Step 8	**destination** **Example:** `Router(config-mon-erspan-src)# destination`	Enters ERSPAN source session destination configuration mode.
Step 9	**erspan-id** *erspan-flow-id* **Example:** `Router(config-mon-erspan-src-dst)# erspan-id 100`	Configures the ID number used by the 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:** `Router(config-mon-erspan-src-dst)# ip address 10.10.0.1`	Configures the IP address used as the source of the ERSPAN traffic.
Step 11	**ip prec** *prec-value* **Example:** `Router(config-mon-erspan-src-dst)# ip prec 5`	(Optional) Configures the IP precedence value of the packets in the ERSPAN traffic. • You can optionally use either the **ip prec** command or the **ip dscp** command, but not both.
Step 12	**ip dscp** *dscp-value* **Example:** `Router(config-mon-erspan-src-dst)# ip dscp`	(Optional) Enables the use of IP differentiated services code point (DSCP) for packets that originate from a circuit emulation (CEM) channel. • You can optionally use either the **ip prec** command or the **ip dscp** command, but not both.
Step 13	**ip ttl** *ttl-value* **Example:** `Router(config-mon-erspan-src-dst)# ip ttl 32`	(Optional) Configures the IP time-to-live (TTL) value of the packets in the ERSPAN traffic.

	Command or Action	Purpose
Step 14	**origin ip address** *ip-address* [**force**] **Example:** `Router(config-mon-erspan-src-dst)# origin ip address 10.1.0.1`	Configures the IP address used as the source of the ERSPAN traffic.
Step 15	**vrf** *vrf-id* **Example:** `Router(config-mon-erspan-src-dst)# vrf 1`	(Optional) Configures the VRF name to use instead of the global routing table.

Step 16	**end**
	Example:
	`Router(config-mon-erspan-src-dst)# end`
		Exits ERSPAN source session destination configuration mode, and returns to privileged EXEC mode.

Configuring an ERSPAN Destination Session

Perform this task to configure an ERSPAN destination session. The ERSPAN destination session defines the session configuration parameters and the ports that will receive the monitored traffic.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **monitor session** *session-number* **type** {**erspan-destination** | **erspan-source**}
4. **description** *string*
5. **destination interface** {*if-single* | *if-list* | *if-range* | *if-mixed*} [**rx** | **tx** | **both**]
6. **source**
7. **erspan-id** *erspan-flow-id*
8. **ip address** *ip-address*
9. **vrf** *vrf-id*
10. **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** *session-number* **type** {**erspan-destination** | **erspan-source**}
	Example:
	`Router(config)# monitor session 1 type erspan-source`
		Defines an ERSPAN source session using the session ID and the session type, and enters the command in ERSPAN monitor source session configuration mode.
		The *session-number* argument range is from 1 to 1024. 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 *session number* argument) and the session type (configured by the **erspan-destination** or **erspan-source** keyword) cannot be changed once entered. Use the **no** form of the command to remove the session and then re-create the session through the command with a new session ID or a new session type.

Step 4	**description** *string* **Example:** `Router(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	**destination interface** {*if-single* | *if-list* | *if-range* | *if-mixed*} [**rx** | **tx** | **both**] **Example:** `Router(config-mon-erspan-src)# destination interface GigabitEthernet1/0/1 rx`	Associates the ERSPAN source session number with the source ports, and selects the traffic direction to be monitored.

	Command or Action	Purpose
Step 6	**source** **Example:** `Router(config-mon-erspan-src)# source`	Enters ERSPAN destination session source configuration mode.
Step 7	**erspan-id** *erspan-flow-id* **Example:** `Router(config-mon-erspan-src-dst)# erspan-id 100`	Configures the ID number used by the source and destination sessions to identify the ERSPAN traffic, which must also be entered in the ERSPAN destination session configuration.
Step 8	**ip address** *ip-address* **Example:** `Router(config-mon-erspan-src-dst)# ip address 10.10.0.1`	Configures the IP address used as the source of the ERSPAN traffic.
Step 9	**vrf** *vrf-id* **Example:** `Router(config-mon-erspan-src-dst)# vrf 1`	(Optional) Configures the VRF name to use instead of the global routing table.

Step 10	**end**
	Example:
	`Router(config-mon-erspan-src-dst)# end`
		Exits ERSPAN destination session source configuration mode, and returns to privileged EXEC mode.

Configuration Examples for ERSPAN

Example: Configuring an ERSPAN Source Session

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

```
monitor session 1 type erspan-source
 source interface GigabitEthernet1/0/1 rx
 source interface GigabitEthernet1/0/4 - 8 tx
 source interface GigabitEthernet1/0/3
 destination
  erspan-id 100
  ip address 10.10.0.1
  ip prec 5
  ip ttl 32
  origin ip address 10.1.0.1
```

Example: Configuring an ERSPAN Destination Session

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

```
monitor session 2 type erspan-destination
 destination interface GigabitEthernet1/3/2
 destination interface GigabitEthernet2/2/0
 source
  erspan-id 100
  ip address 10.10.0.1
```

Additional References

The following sections provide references related to the ERSPAN feature.

Related Documents

Related Topic	Document Title
LAN Switching commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	Cisco IOS LAN Switching Command Reference
Cisco IOS commands	Cisco IOS Master Commands List, All Releases

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS XE software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported by this feature, and support for existing standards has not been modified by this feature.	--

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

Feature Information 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
Encapsulated Remote SPAN	Cisco IOS XE Release 2.1	ERSPAN sessions allow you to monitor traffic on one or more ports, or one or more VLANs, and send the monitored traffic to one or more destination ports. The following section provides information about this feature. The following commands were modified by this feature: **description**, **destination**, **erspan-id**, **filter**, **ip dscp**, **ip prec**, **ip ttl, monitor permit-list**, **monitor session**, **origin ip address**, **show monitor permit-list**, **source**, **switchport**, **switchport mode trunk**, **switchport nonegotiate**, **switchport trunk encapsulation**, **vrf**.
ERSPAN WAN Source	Cisco IOS XE Release 3.5S	ERSPAN monitors and captures traffic over Ethernet ports and virtual LANs (VLANs). The following section provides information about this feature. The following command was introduced by this feature:**source interface**.

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.

Configuring Routing Between VLANs with IEEE 802.1Q Encapsulation

This chapter describes the required and optional tasks for configuring routing between VLANs with IEEE 802.1Q encapsulation.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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.

Restrictions for Configuring Routing Between VLANs with IEEE 802.1Q Encapsulation

Shared port adapters (SPAs) on Cisco ASR 1000 Series Aggregation Services Router have a limit of 8,000 TCAM entries, which limits the number of VLANs you can create on a single SPA.

Information About Configuring Routing Between VLANs with IEEE 802.1Q Encapsulation

Configuring Routing Between VLANs with IEEE 802.1Q Encapsulation

The IEEE 802.1Q protocol is used to interconnect multiple switches and routers, and for defining VLAN topologies. The IEEE 802.1Q standard is extremely restrictive to untagged frames. The standard provides only a per-port VLANs solution for untagged frames. For example, assigning untagged frames to VLANs takes into consideration only the port from which they have been received. Each port has a parameter called a *permanent virtual identification* (Native VLAN) that specifies the VLAN assigned to receive untagged frames.

The main characteristics of IEEE 802.1Q are as follows:

- Assigns frames to VLANs by filtering.
- The standard assumes the presence of a single spanning tree and of an explicit tagging scheme with one-level tagging.

How to Configure Routing Between VLANs with IEEE 802.1Q Encapsulation

Configuring IP Routing over IEEE 802.1Q

IP routing over IEEE 802.1Q extends IP routing capabilities to include support for routing IP frame types in VLAN configurations using the IEEE 802.1Q encapsulation.

To route IP over IEEE 802.1Q between VLANs, you need to customize the subinterface to create the environment in which it will be used. Perform the tasks described in the following sections in the order in which they appear:

Enabling IP Routing

IP routing is automatically enabled in the Cisco IOS XE software for routers. To reenable IP routing if it has been disabled, perform the following steps.

Once you have IP routing enabled on the router, you can customize the characteristics to suit your environment. If necessary, refer to the IP configuration chapters in the *Cisco IOS XE IP Routing Protocols Configuration Guide* , Release 2, for guidelines on configuring IP.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip routing**
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	**ip routing** **Example:** `Router(config)# ip routing`	Enables IP routing on the router.

Step 4	**end**
	Example:
	`Router(config)# exit`
		Exits privileged EXEC mode.

Defining the VLAN Encapsulation Format

To define the encapsulation format as IEEE 802.1Q, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface gigabitethernet** *card* / *spaslot* / *port* **.** *subinterface-number*
4. **encapsulation dot1q** *vlanid*
5. **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** *card* / *spaslot* / *port* **.** *subinterface-number* **Example:** `Router(config)# interface gigabitethernet 0/0/0.101`	Specifies the subinterface on which IEEE 802.1Q will be used, and enters interface configuration mode.
Step 4	**encapsulation dot1q** *vlanid* **Example:** `Router(config-subif)# encapsulation dot1q 101`	Defines the encapsulation format as IEEE 802.1Q (**dot1q**), and specifies the VLAN identifier

Step 5	**end**
	Example:
	`Router(config-subif)# end`
		Exits subinterface configuration mode.

Assigning an IP Address to Network Interface

An interface can have one primary IP address. To assign a primary IP address and a network mask to a network interface, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface gigabitethernet** *card* / *spaslot* / *port* **.** *subinterface-number*
4. **ip address** *ip-address mask*
5. **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** *card* / *spaslot* / *port* **.** *subinterface-number* **Example:** `Router(config)# interface gigabitethernet 0/0/0.101`	Specifies the subinterface on which IEEE 802.1Q will be used, and enters interface configuration mode.
Step 4	**ip address** *ip-address mask* **Example:** `Router(config-subif)# ip address 10.0.0.0 255.0.0.0`	Sets a primary IP address for an interface. • Enter the primary IP address for an interface. **Note** A mask identifies the bits that denote the network number in an IP address. When you use the mask to subnet a network, the mask is then referred to as a subnet mask.

Step 5	**end**
	Example:
	`Router(config-subif)# end`
		Exits subinterface configuration mode.

Monitoring and Maintaining VLAN Subinterfaces

To indicate whether a VLAN is a native VLAN, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **show vlans**
3. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show vlans** **Example:** `Router# show vlans`	Displays VLAN information.

Step 3	**end**
	Example:
	`Router# end`
		Exits privileged EXEC mode.

Configuration Examples for Configuring Routing Between VLANs with IEEE 802.1Q Encapsulation

- Configuring IP Routing over IEEE 802.1Q Example, page 20

Configuring IP Routing over IEEE 802.1Q Example

This configuration example shows IP being routed on VLAN 101:

```
!
ip routing
!
interface gigabitethernet 4/1/1.101
  encapsulation dot1q 101
  ip addr 10.0.0.0 255.0.0.0
!
```

Additional References

The following sections provide references related to the Configuring Routing Between VLANs with IEEE 802.1Q Encapsulation feature.

Related Documents

Related Topic	Document Title
LAN Switching commands	*Cisco IOS LAN Switching Command Reference*
Cisco IOS commands	Cisco IOS Master Commands List, All Releases

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS XE software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	--

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Configuring Routing Between VLANs with IEEE 802.1Q Encapsulation

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 2 Feature Information for Configuring Routing Between VLANs with IEEE 802.1Q Encapsulation

Feature Name	Releases	Feature Information
Configuring Routing Between VLANs with IEEE 802.1Q Encapsulation	Cisco IOS XE Release 2.1	This feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

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.

IEEE 802.1Q-in-Q VLAN Tag Termination

Encapsulating IEEE 802.1Q VLAN tags within 802.1Q enables service providers to use a single VLAN to support customers who have multiple VLANs. The IEEE 802.1Q-in-Q VLAN Tag Termination feature on the subinterface level preserves VLAN IDs and keeps traffic in different customer VLANs segregated.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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.

Information About IEEE 802.1Q-in-Q VLAN Tag Termination

IEEE 802.1Q-in-Q VLAN Tag Termination on Subinterfaces

IEEE 802.1Q-in-Q VLAN Tag Termination simply adds another layer of IEEE 802.1Q tag (called “metro tag” or “PE-VLAN”) to the 802.1Q tagged packets that enter the network. The purpose is to expand the VLAN space by tagging the tagged packets, thus producing a “double-tagged” frame. The expanded VLAN space allows the service provider to provide certain services, such as Internet access on specific VLANs for specific customers, and yet still allows the service provider to provide other types of services for their other customers on other VLANs.

Generally the service provider’s customers require a range of VLANs to handle multiple applications. Service providers can allow their customers to use this feature to safely assign their own VLAN IDs on subinterfaces because these subinterface VLAN IDs are encapsulated within a service-provider designated

VLAN ID for that customer. Therefore there is no overlap of VLAN IDs among customers, nor does traffic from different customers become mixed. The double-tagged frame is “terminated” or assigned on a subinterface with an expanded **encapsulation dot1q** command that specifies the two VLAN ID tags (outer VLAN ID and inner VLAN ID) terminated on the subinterface (see the figure below).

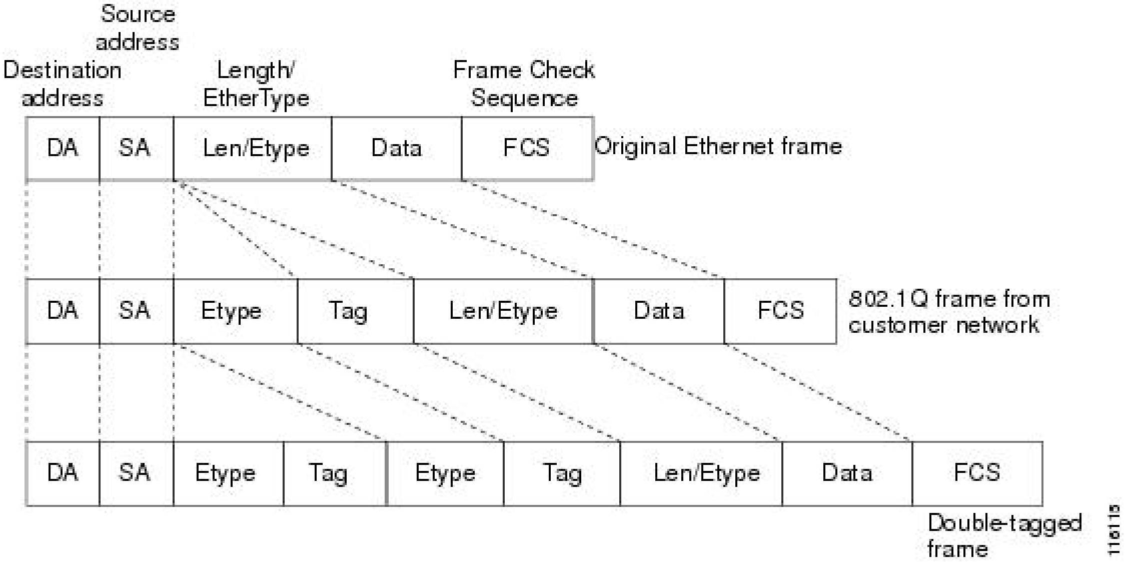
IEEE 802.1Q-in-Q VLAN Tag Termination is generally supported on whichever Cisco IOS XE features or protocols are supported on the subinterface. The only restriction is whether you assign ambiguous or unambiguous subinterfaces for the inner VLAN ID. See the Unambiguous and Ambiguous Subinterfaces section.

The primary benefit for the service provider is reduced number of VLANs supported for the same number of customers. Other benefits of this feature include:

- PPPoE scalability. By expanding the available VLAN space from 4096 to approximately 16.8 million (4096 times 4096), the number of PPPoE sessions that can be terminated on a given interface is multiplied.
- When deploying Gigabyte Ethernet DSL Access Multiplexer (DSLAM) in wholesale model, you can assign the inner VLAN ID to represent the end-customer virtual circuit (VC) and assign the outer VLAN ID to represent the service provider ID.

Whereas switches require IEEE 802.1Q tunnels on interfaces to carry double-tagged traffic, routers need only encapsulate Q-in-Q VLAN tags within another level of 802.1Q tags in order for the packets to arrive at the correct destination.

Figure 2 Untagged, 802.1Q-Tagged, and Double-Tagged Ethernet Frames



Unambiguous and Ambiguous Subinterfaces

The **encapsulation dot1q** command is used to configure Q-in-Q termination on a subinterface. The command accepts an Outer VLAN ID and one or more Inner VLAN IDs. The outer VLAN ID always has a specific value, while inner VLAN ID can either be a specific value or a range of values.

A subinterface that is configured with a single Inner VLAN ID is called an unambiguous Q-in-Q subinterface. In the following example, Q-in-Q traffic with an Outer VLAN ID of 101 and an Inner VLAN ID of 1001 is mapped to the Gigabit Ethernet 1/1/0.100 subinterface:

```
Router(config)# interface gigabitEehernet1/1/0.100
Router(config-subif)# encapsulation dot1q 101 second-dot1q 1001
```

A subinterface that is configured with multiple Inner VLAN IDs is called an ambiguous Q-in-Q subinterface. By allowing multiple Inner VLAN IDs to be grouped together, ambiguous Q-in-Q subinterfaces allow for a smaller configuration, improved memory usage and better scalability.

In the following example, Q-in-Q traffic with an Outer VLAN ID of 101 and Inner VLAN IDs anywhere in the 2001-2100 and 3001-3100 range is mapped to the Gigabit Ethernet 1/1/0.101 subinterface:

```
Router(config)# interface gigabitethernet1/1/0.101
Router(config-subif)# encapsulation dot1q 101 second-dot1q 2001-2100,3001-3100
```

Ambiguous subinterfaces can also use the **any**keyword to specify the inner VLAN ID.

See the Configuration Examples for IEEE 802.1Q-in-Q VLAN Tag Termination section for an example of how VLAN IDs are assigned to subinterfaces, and for a detailed example of how the **any** keyword is used on ambiguous subinterfaces.

Only PPPoE is supported on ambiguous subinterfaces. Standard IP routing is not supported on ambiguous subinterfaces.

How to Configure IEEE 802.1Q-in-Q VLAN Tag Termination

- Configuring the Interfaces for IEEE 802.1Q-in-Q VLAN Tag Termination, page 25
- Verifying the IEEE 802.1Q-in-Q VLAN Tag Termination, page 28

Configuring the Interfaces for IEEE 802.1Q-in-Q VLAN Tag Termination

Perform this task to configure the main interface used for the Q-in-Q double tagging and to configure the subinterfaces. An optional step in this task shows you how to configure the EtherType field to be 0x9100 for the outer VLAN tag, if that is required. After the subinterface is defined, the 802.1Q encapsulation is configured to use the double tagging.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **dot1q tunneling ethertype** *ethertype*
5. **interface** *type number* **.** *subinterface-number*
6. **encapsulation dot1q** *vlan-id* **second-dot1q** {**any** | *vlan-id* | *vlan-id* **-** *vlan-id* [*vlan-id* **-** *vlan-id*]}
7. **pppoe enable** [**group** *group-name*] [**max-sessions** *max-sessions-number*]
8. **exit**
9. Repeat Step 5 to configure another subinterface.
10. Repeat Step 6 and Step 7 to specify the VLAN tags to be terminated on the subinterface.
11. **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** *type number* **Example:** `Router(config)# interface gigabitethernet 1/0/0`	Configures an interface and enters interface configuration mode.
Step 4	**dot1q tunneling ethertype** *ethertype* **Example:** `Router(config-if)# dot1q tunneling ethertype 0x9100`	(Optional) Defines the Ethertype field type used by peer devices when implementing Q-in-Q VLAN tagging.
Step 5	**interface** *type number* **.** *subinterface-number* **Example:** `Router(config-if)# interface gigabitethernet 1/0/0.1`	Configures a subinterface and enters subinterface configuration mode.

Step 6	**encapsulation dot1q** *vlan-id* **second-dot1q** {**any** | *vlan-id* | *vlan-id* **-** *vlan-id* [*vlan-id* **-** *vlan-id*]}
	Example:
	`Router(config-subif)# encapsulation dot1q 100 second-dot1q 200`
		(Required) Enables the 802.1Q encapsulation of traffic on a specified subinterface in a VLAN.
		• Use the **second-dot1q** keyword and the *vlan-id*argument to specify the VLAN tags to be terminated on the subinterface.
		• In this example, an unambiguous Q-in-Q subinterface is configured because only one inner VLAN ID is specified.
		• Q-in-Q frames with an outer VLAN ID of 100 and an inner VLAN ID of 200 will be terminated.

	Command or Action	Purpose
Step 7	**pppoe enable** [**group** *group-name*] [**max-sessions** *max-sessions-number*] **Example:** `Router(config-subif)# pppoe enable group vpn1`	Enables PPPoE sessions on a subinterface. The example specifies that the PPPoE profile, vpn1, will be used by PPPoE sessions on the subinterface.
Step 8	**exit** **Example:** `Router(config-subif)# exit`	Exits subinterface configuration mode and returns to interface configuration mode. • Repeat this step one more time to exit interface configuration mode.
Step 9	Repeat Step 5 to configure another subinterface. **Example:** `Router(config-if)# interface gigabitethernet 1/0/0.2`	(Optional) Configures a subinterface and enters subinterface configuration mode.

Step 10	Repeat Step 6 and Step 7 to specify the VLAN tags to be terminated on the subinterface.
	Example:
	`Router(config-subif)# encapsulation dot1q 100 second-dot1q 100-199,201-600`
	Example:
	Example:
	`Router(config-subif)# pppoe enable group vpn1`
	Example:
		Step 6 enables the 802.1Q encapsulation of traffic on a specified subinterface in a VLAN.
		• Use the **second-dot1q** keyword and the *vlan-id*argument to specify the VLAN tags to be terminated on the subinterface.
		• In the example, an ambiguous Q-in-Q subinterface is configured because a range of inner VLAN IDs is specified.
		• Q-in-Q frames with an outer VLAN ID of 100 and an inner VLAN ID in the range of 100 to 199 or 201 to 600 will be terminated.
		Step 7 enables PPPoE sessions on the subinterface. The example specifies that the PPPoE profile, vpn1, will be used by PPPoE sessions on the subinterface.

Step 11	**end**
	Example:
	`Router(config-subif)# end`
		Exits subinterface configuration mode and returns to privileged EXEC mode.

Verifying the IEEE 802.1Q-in-Q VLAN Tag Termination

Perform this optional task to verify the configuration of the IEEE 802.1Q-in-Q VLAN Tag Termination feature.

SUMMARY STEPS

1. **enable**
2. **show running-config**
3. **show vlans dot1q** [**internal** *interface-type interface-number* **.***subinterface-number*[**detail**] | **second-dot1q** *inner-id* **any**]] [**detail]**

DETAILED STEPS

Step 1 **enable**

Enables privileged EXEC mode. Enter your password if prompted.

Example:

```
Router> enable
```

Step 2 **show running-config**

Use this command to show the currently running configuration on the device. You can use delimiting characters to display only the relevant parts of the configuration.

Example:

```
Router# show running-config
```

Step 3 **show vlans dot1q** [**internal** *interface-type interface-number* **.***subinterface-number*[**detail**] | **second-dot1q** *inner-id* **any**]] [**detail]**

Use this command to show the statistics for all the 802.1Q VLAN IDs. In this example, only the outer VLAN ID is displayed.

Example:

```
Router# show vlans dot1q
Total statistics for 802.1Q VLAN 1:
   441 packets, 85825 bytes input
   1028 packets, 69082 bytes output
Total statistics for 802.1Q VLAN 101:
   5173 packets, 510384 bytes input
   3042 packets, 369567 bytes output
Total statistics for 802.1Q VLAN 201:
   1012 packets, 119254 bytes input
   1018 packets, 120393 bytes output
Total statistics for 802.1Q VLAN 301:
   3163 packets, 265272 bytes input
   1011 packets, 120750 bytes output
Total statistics for 802.1Q VLAN 401:
   1012 packets, 119254 bytes input
   1010 packets, 119108 bytes output
```

Configuration Examples for IEEE 802.1Q-in-Q VLAN Tag Termination

Configuring any Keyword on Subinterfaces for IEEE 802.1Q-in-Q VLAN Tag Termination Example

Some ambiguous subinterfaces can use the **any** keyword for the inner VLAN ID specification. The **any** keyword represents any inner VLAN ID that is not explicitly configured on any other interface. In the following example, seven subinterfaces are configured with various outer and inner VLAN IDs.

Note The **any** keyword can be configured on only one subinterface of a specified physical interface and outer VLAN ID.

```
interface GigabitEthernet1/0/0.1
 encapsulation dot1q 100 second-dot1q 100
interface GigabitEthernet1/0/0.2
 encapsulation dot1q 100 second-dot1q 200
interface GigabitEthernet1/0/0.3
 encapsulation dot1q 100 second-dot1q 300-400,500-600
interface GigabitEthernet1/0/0.4
 encapsulation dot1q 100 second-dot1q any
interface GigabitEthernet1/0/0.5
 encapsulation dot1q 200 second-dot1q 50
interface GigabitEthernet1/0/0.6
 encapsulation dot1q 200 second-dot1q 1000-2000,3000-4000
interface GigabitEthernet1/0/0.7
 encapsulation dot1q 200 second-dot1q any
```

The table below shows which subinterfaces are mapped to different values of the outer and inner VLAN ID on Q-in-Q frames that come in on Gigabit Ethernet interface 1/0/0.

Table 3 Subinterfaces Mapped to Outer and Inner VLAN IDs for GE Interface 1/0/0

Outer VLAN ID	Inner VLAN ID	Subinterface mapped to
100	1 through 99	GigabitEthernet1/0/0.4
100	100	GigabitEthernet1/0/0.1
100	101 through 199	GigabitEthernet1/0/0.4
100	200	GigabitEthernet1/0/0.2
100	201 through 299	GigabitEthernet1/0/0.4

Outer VLAN ID	Inner VLAN ID	Subinterface mapped to
100	300 through 400	GigabitEthernet1/0/0.3
100	401 through 499	GigabitEthernet1/0/0.4
100	500 through 600	GigabitEthernet1/0/0.3
100	601 through 4095	GigabitEthernet1/0/0.4
200	1 through 49	GigabitEthernet1/0/0.7
200	50	GigabitEthernet1/0/0.5
200	51 through 999	GigabitEthernet1/0/0.7
200	1000 through 2000	GigabitEthernet1/0/0.6
200	2001 through 2999	GigabitEthernet1/0/0.7
200	3000 through 4000	GigabitEthernet1/0/0.6
200	4001 through 4095	GigabitEthernet1/0/0.7

A new subinterface is now configured:

```
interface GigabitEthernet1/0/0.8
 encapsulation dot1q 200 second-dot1q 200-600,900-999
```

The table below shows the changes made to the table for the outer VLAN ID of 200. Notice that subinterface 1/0/0.7 configured with the **any** keyword now has new inner VLAN ID mappings.

Table 4 Subinterfaces Mapped to Outer and Inner VLAN IDs for GE Interface 1/0/0--Changes Resulting from Configuring GE Subinterface 1/0/0.8

Outer VLAN ID	Inner VLAN ID	Subinterface mapped to
200	1 through 49	GigabitEthernet1/0/0.7
200	50	GigabitEthernet1/0/0.5
200	51 through 199	GigabitEthernet1/0/0.7
200	200 through 600	GigabitEthernet1/0/0.8
200	601 through 899	GigabitEthernet1/0/0.7
200	900 through 999	GigabitEthernet1/0/0.8
200	1000 through 2000	GigabitEthernet1/0/0.6
200	2001 through 2999	GigabitEthernet1/0/0.7
200	3000 through 4000	GigabitEthernet1/0/0.6
200	4001 through 4095	GigabitEthernet1/0/0.7

Additional References

The following sections provide references related to the IEEE 802.1Q-in-Q VLAN Tag Termination feature.

Related Documents

Related Topic	Document Title
Related commands	*Cisco IOS LAN Switching Command Reference*

Standards

Standards	Title
IEEE 802.1Q	--

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS XE software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
No new or modified RFCs are supported by this feature, and support for existing standards has not been modified by this feature.	--

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/techsupport

Feature Information for IEEE 802.1Q-in-Q VLAN Tag Termination

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 5 Feature Information for IEEE 802.1Q-in-Q VLAN Tag Termination

Feature Name	Releases	Feature Information
IEEE 802.1Q-in-Q VLAN Tag Termination	Cisco IOS XE Release 2.1	This feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers. The following commands have been modified for this feature: **dot1q tunneling ethertype**, **encapsulation dot1q**, and **show vlans dot1q**

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.

VLAN Mapping to Gigabit EtherChannel Member Links

The VLAN Mapping to Gigabit EtherChannel (GEC) Member Links feature allows you to configure static assignment of user traffic as identified by a VLAN ID to a given member link of a GEC bundle. You can manually assign VLAN subinterfaces to a primary and secondary link. This feature includes load balancing to downstream equipment, regardless of vendor equipment capabilities, and provides failover protection by redirecting traffic to the secondary member link if the primary link fails. Member links are supported with up to 16 bundles per chassis.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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.

Prerequisites for VLAN Mapping to GEC Member Links

- Per-VLAN load balancing must be globally enabled.
- Each VLAN must have IEEE 802.1Q encapsulation configured.
- One primary and one secondary link must be associated with each VLAN.

Restrictions for VLAN Mapping to GEC Member Links

- TenGigabit Ethernet is not supported as a member link in VLAN mapping.

The following restrictions are applicable for IPv6 load balancing on GEC links:

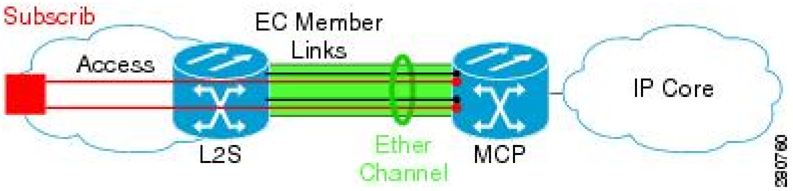
- IPv6 traffic distribution is enabled only on port channels with flow load balancing.
- Multiprotocol Label Switching (MPLS) Traffic Engineering (TE) is not supported on port channels.
- The port-channel QinQ subinterface is not supported.

Information About VLAN Mapping of GEC Member Links

VLAN-to-Port Channel Member Link Mapping

The figure below illustrates the traffic flow for the VLAN-to-port channel mapping.

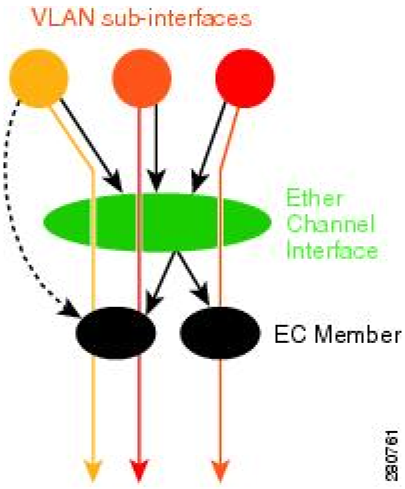
Figure 3 VLAN-to-Port Channel Mapping



The black lines represent the physical 1 GigabitEthernet interfaces connecting the MCP router with the Layer 2 (L2) switch. These interfaces are bundled together in port-channels, shown in green.

In the figure below, subscriber VLAN subinterfaces, shown in shades of orange and red, are configured as Layer 3 (L3) interfaces on top of the EtherChannel interfaces. Mapping of the VLAN to the member link (shown with the dotted black arrow) is done through configuration and downloaded in the dataplane so that outgoing VLA traffic (shown with orange and red arrows) is sent over the associated active primary or secondary member link. The QoS configuration in this model is applied at the VLAN subinterface and member link interface level, implying that QoS queues are created at both levels.

Figure 4 Mapping of VLAN to Member Links



VLAN-Manual Load Balancing

When load balancing is configured for GEC links, traffic flows are mapped to different buckets as dictated by the load balancing algorithm. For each EtherChannel configured, a set of 16 buckets are created. The EtherChannel module decides how buckets are distributed across member links. Each bucket has an active link associated with it that represents the interface to be used for all flows that are mapped to the same bucket.

All packets to be forwarded over the same VLAN subinterface are considered to be part of the same flow that is mapped to one bucket. Each bucket is associated with a primary-secondary pair, and the buckets point to the active interface in the pair. Only one of the pair is active at a time. Multiple VLAN flows can be mapped to the same bucket if their (primary, secondary) mapping is the same.

The buckets are created when VLAN manual load balancing is enabled. When VLAN load balancing is removed, the buckets are deleted. All port channels use either VLAN manual load balancing or dynamic flow-based load balancing. For information about flow-based load balancing, see the module Flow-Based Per Port-Channel Load Balancing.

VLAN Primary and Secondary Link Association

For port-channel traffic distribution, a member link has a configured state, primary or secondary, and an operational state, active or standby. The primary link is also active when the interface is up. If the primary interface is down, the interface is in primary standby state while the secondary interface is in secondary active state. If the primary link is up, the secondary link is in secondary standby, even if the interface is operationally up.

A primary and a secondary member link are each associated with each routed VLAN configured on a port-channel main interface. When forwarding traffic for this VLAN, the primary interface is used as the outgoing interface when this interface is up, the secondary interface, if operational, is used when the primary interface is down.

If not all the conditions for per-VLAN traffic distribution are met, the mapping is not downloaded in the forwarding plane. Otherwise, the dataplane is updated with this mapping.

The table below describes the primary and secondary link configuration status and the resulting function of each configuration.

Table 6 VLAN Primary and Secondary Link Mapping Status

Primary Status	Secondary Status	Description
Configured	Configured	Both primary and secondary links are specified with the **encapsulation dot1q** command. `encapsulation dot1Q` *vlan-id* `primary` *interface-number* `secondary` *interface-number*
Defaulted	Defaulted	Neither a primary nor secondary link is specified. `encapsulation dot1Q` *vlan-id* In a stable system, defaults for both primary and secondary links are selected in the same way for all VLANs. The first link up that is added to the EC is selected as primary, and the second link up as secondary. If there are no links up, the primary and secondary links are selected from the down links.
Configured	Defaulted	Only the primary link is specified. `encapsulation dot1Q` *vlan-id* `primary` *interface-number* A secondary link that is different than the primary link is internally selected.
Configured	–	Only a primary link is specified, and only one link is defined. `encapsulation dot1Q` *vlan-id* `primary` *interface-number* No secondary link can be selected as default when only one link is defined in the EC.
Defaulted	–	Neither a primary nor secondary link is specified, and only one link is defined. `encapsulation dot1Q` *vlan-id* A default for a primary link is selected, but no default can be selected for a secondary link if only one link is defined in the EC.

Primary Status	Secondary Status	Description
–	–	Neither a primary nor secondary link is specified, and no links are defined. `encapsulation dot1Q` *vlan-id* Defaults cannot be selected, and no links are defined in the EC.

Note Default mappings do not override user-configured mappings, even if the user-configured mappings are defined incorrectly. Once the (VLAN, primary, secondary) association is performed (either through CLI, defaults or combination), the system validates the mapping and downloads it to the dataplane. If there are no VLANs configured, all traffic forwarded over the port channel is dropped.

Adding Channel Member Links

When a new member link is added, new buckets are created and downloaded in the dataplane. For all VLANs that have this interface as either primary or secondary new VLAN-to-bucket mappings are downloaded in the dataplane. For all VLANs that need a default for primary and secondary, the default selection algorithm is triggered, and if QoS validation passes, the VLAN-to-bucket mappings are downloaded. QoS policies create VLAN queues on the newly added link.

Deleting Member Links

When a member link is removed, a warning message is displayed. The VLAN queues from the link that is about to be deleted, VLAN-to-bucket mappings are removed, and all affected buckets are removed.

EC Link Down Notification

When a link goes down, all the traffic for the VLANs that have this link assigned as primary have to be switched to the links that are designated as secondary if the secondary link is up. The traffic for the VLANs that have this link assigned as secondary is not affected. The EC Link Down notification causes all buckets associated with a primary-secondary pair where the primary link is the down link and the secondary link is up to be updated with the secondary link. The change is communicated to the dataplane.

All buckets associated with a primary-secondary pair where secondary link is the down link and where primary link is down to be updated so that the primary is now the active link. The change is communicated to the dataplane.

EC Link Up Notification

When a link goes up, all the traffic for the VLANs that have this link assigned as primary is switched to this link. The traffic for the VLANs that have this link assigned as secondary is not affected. The EC Link Up notification causes all buckets associated with a primary-secondary pair where primary link is the link that came up and where secondary link is up to be notified that the primary link is up. The change is communicated to the dataplane.

All buckets associated with a primary-secondary pair where secondary link is the link that went up and where primary link is down are notified that the secondary link is now the primary link. The change is communicated to the dataplane.

How to Configure VLAN Mapping to GEC Links

Configuring VLAN-Based Manual Load Balancing

Perform this task to configure VLAN port-channel linking and to enable VLAN load balancing on port channels.

One primary and one secondary link must be associated with a given VLAN. The primary and secondary options are available only if VLAN manual load balancing is enabled. If all of the following conditions are met, the load balancing information is downloaded in the forwarding plane. If any of these conditions is no longer met, the load balancing information is removed from the forwarding plane.

- VLAN load balancing must be enabled globally.
- IEEE 802.1Q encapsulation must be configured on each VLAN.
- One primary and one secondary member link must be enabled to manually map the VLAN traffic to the EtherChannel links.
- The primary and secondary links must be part of the port channel for traffic to use these links.

If only a primary link is specified, a default secondary different from the specified primary is selected as the default. If neither the primary nor the secondary link is explicitly configured, a primary and a secondary link are selected by default. There is no attempt to perform equal VLAN distribution across links when default links are chosen.

If the interfaces specified as primary or secondary are not configured as part of the port channel, or if the global VLAN load balancing is not enabled, warning messages are displayed.

VLAN 500's main interface is not the channel group of primary=GigabitEthernet 4/0/1 Per-VLAN manual load-balancing will not take effect until channel-group is configured under the primary interface.

VLAN 500's main interface is not the channel group of secondary=GigabitEthernet 1/0/0 Per-VLAN manual load-balancing will not take effect until channel-group is configured under the primary interface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **port-channel load-balancing vlan-manual**
4. **interface port-channel** *channel-number*
5. **ip address** *ip-address address-mask*
6. **exit**
7. **interface** *interface-type interface-number.subinterface-number*
8. **channel-group** *channel-number*
9. **exit**
10. **interface port-channel** *interface-number.subinterface-number*
11. **encapsulation dot1Q** *vlan-id* **primary** *interface-type slot /port* **secondary** *interface-type slot /port*
12. **ip address** *ip-address address-mask*
13. **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	**port-channel load-balancing vlan-manual** **Example:** `Router(config)# port-channel load-balancing vlan-manual`	Enables port-channel load balancing on the router.
Step 4	**interface port-channel** *channel-number* **Example:** `Router(config)# interface port-channel 1`	Enters interface configuration mode and defines the interface as a port channel.

	Command or Action	Purpose
Step 5	**ip address** *ip-address address-mask* **Example:** `Router(config-if)# ip address 172.1.2.3 255.255.0.0`	Specifies the IP address and mask.
Step 6	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode and returns to global configuration mode.
Step 7	**interface** *interface-type interface-number.subinterface-number* **Example:** `Router(config)# interface gigbabitethernet 1/1/0`	Enters interface configuration mode on the Gigabit Ethernet interface.
Step 8	**channel-group** *channel-number* **Example:** `Router(config-if)# channel-group 1`	Assigns the Gigabit Ethernet interface to the specified channel group. • The channel number is the same channel number that you specified when you created the port-channel interface
Step 9	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode and returns to global configuration mode.
Step 10	**interface port-channel** *interface-number.subinterface-number* **Example:** `Router(config)# interface port-channel 1.100`	Specifies the interface type, interface number, and subinterface number.
Step 11	**encapsulation dot1Q** *vlan-id* **primary** *interface-type slot /port* **secondary** *interface-type slot /port* **Example:** `Router(config-if)# encapsulation dot1Q 100 primary GigabitEthernet 1/1/1 secondary GigabitEthernet 1/2/1`	Enables IEEE 802.1Q encapsulation on the interface.

	Command or Action	Purpose
Step 12	**ip address** *ip-address address-mask* **Example:** `Router(config-if)# ip address 172.1.2.100 255.255.255.0`	Specifies the port channel IP address and mask.

Step 13	**end**
	Example:
	`Router(config-if)# end`
		Exits interface configuration mode, and returns to privileged EXEC mode.

- Troubleshooting Tips, page 43

Troubleshooting Tips

- Use the **show etherchannel load-balancing** command to display the port channel load balancing method currently in use.
- Use the **show interfaces port-channel etherchannel** command to display the traffic distribution currently in use.

Disabling Load Balancing on the EtherChannel

To disable load balancing on the EtherChannel, use the **no port-channel load-balancing vlan-manual** command. When this command is issued, a warning message is displayed if any VLAN subinterfaces exist:

```
Warning: Removing the Global VLAN LB command will affect traffic for all dot1Q VLANs
```

Removing a Member Link from the EtherChannel

To remove a member link from the EtherChannel (EC), use the **no channel-group**command

When a member link is removed from EC, if the link is included in a VLAN mapping, the following warning message is displayed:

```
Warning: Removing GigabitEthernet 4/0/0 from the port-channel will affect traffic for the
dot1Q VLANs that include this link in their mapping.
```

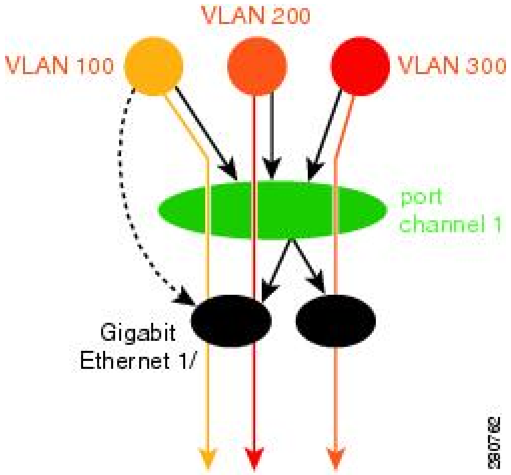
Configuration Examples for VLAN Mapping to GEC Member Links

- Example: VLAN Load Balancing, page 44
- Example: Troubleshooting, page 45

Example: VLAN Load Balancing

This example shows a load balancing configuration, including QoS features that might be applied to define policies for handling traffic. This example enables load balancing globally using the **port-channel load-balancing** command. Note that IEEE 802.1Q encapsulation is configured on each port-channel interface. The figure below illustrates the port channel bundle with the three VLANs used in the following configuration example:

Figure 5 *Port Channel Bundle*



```
port-channel load-balancing vlan-manual
!
class-map match-all BestEffort
!
class-map match-all video
!
class-map match-all voice
!
policy-map subscriber
  class voice
    priority level 1
  class video
    priority level 2
  class class-default service-fragment BE
    shape average 10000
    bandwidth remaining percent 80
policy-map aggregate-member-link
    class BestEffort service-fragment BE
    shape average 100000
!
interface Port-channel1
 ip address 172.1.2.3 255.255.0.0
!
interface Port-channel1.100
 encapsulation dot1Q 100 primary GigabitEthernet 1/1/1
                secondary GigabitEthernet 1/2/1
 ip address 172.1.2.100 255.255.255.0
 service-policy output subscriber
!
interface Port-channel1.200
 encapsulation dot1Q 200 primary GigabitEthernet 1/2/1
 ip address 172.1.2.200 255.255.255.0
 service-policy output subscriber
!
interface Port-channel1.300
```

```
 encapsulation dot1Q 300
 ip address 172.1.2.300 255.255.255.0
 service-policy output subscriber
!
interface GigabitEthernet 1/1/1
 no ip address
 channel-group 1 mode on
 service-policy output aggregate-member-link
!
interface GigabitEthernet 1/2/1
 no ip address
 channel-group 1 mode on
 service-policy output aggregate-member-link
```

Example: Troubleshooting

Example 1:

```
Router# show etherchannel load-balancing
EtherChannel Load-Balancing Configuration:
        vlan-manual
```

Example 2:

```
Router# show etherchannel load-balancing
EtherChannel Load-Balancing Configuration: not configured
```

Use the **show interfaces port-channel** command to display the traffic distribution currently in use.

```
Router# show interfaces port-channel 1 etherchannel

Active Member List contains 0 interfaces
 Passive Member List contains 2 interfaces
  Port: GigabitEthernet 4/0/0
    VLAN 1 (Pri, Ac, D, P)    VLAN 100 (Pri, Ac, C, P)    VLAN 200 (Sec, St, C, P)
  Port: GigabitEthernet 1/0/0
    VLAN 1 (Sec, St, D, P)    VLAN 100 (Sec, St, C, P)    VLAN 200 (Pri, Ac, C, P)
 Bucket Information for VLAN Manual LB:
    Bucket 0   (p=GigabitEthernet 4/0/0, s=GigabitEthernet 4/0/0) active GigabitEthernet
4/0/0
    Bucket 1   (p=Gigabitthernet 4/0/0, s=GigabitEthernet 1/0/0) active GigabitEthernet
4/0/0
    Bucket 4   (p=GigabitEthernet 1/0/0, s=GigabitEthernet 4/0/0) active GigabitEthernet
1/0/0
    Bucket 5   (p=GigabitEthernet 1/0/0, s=GigabitEthernet 1/0/0) active GigabitEthernet
1/0/0
```

To see the mapping of a VLAN to the primary and secondary links, use the **show vlans** command.

```
Router# show vlans 100
VLAN ID: 100 (IEEE 802.1Q Encapsulation)
   Protocols Configured:          Received:        Transmitted:
VLAN trunk interfaces for VLAN ID 100:
Port-channel1.1 (100)
      Mapping for traffic load-balancing using bucket 1:
          primary   = GigabitEthernet 4/0/0 (active, C, P)
          secondary = GigabitEthernet 1/0/0 (standby, C, P)
      Total 0 packets, 0 bytes input
      Total 0 packets, 0 bytes output
No subinterface configured with ISL VLAN ID 100
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
LAN Switching commands	*Cisco IOS LAN Switching Command Reference*

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for VLAN Mapping to GEC Member Links

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 7 Feature Information for VLAN Mapping to Gigabit EtherChannel Member Links

Feature Name	Releases	Feature Information
VLAN Mapping to Gigabit EtherChannel Member Links	Cisco IOS XE Release 2.1	The VLAN Mapping to Gigabit EtherChannel Member Links feature allows you to configure static assignment of user traffic as identified by a VLAN ID to a given member link of a GEC bundle. You can manually assign VLAN subinterfaces to a primary and secondary link. This feature includes load balancing to downstream equipment, regardless of vendor equipment capabilities, and provides failover protection by redirecting traffic to the secondary member link if the primary link fails. Member links are supported with up to 16 bundles per chassis. The following commands were modified by this feature: **encapsulation dot1q**, **port-channel load-balancing vlan-manual**, **show etherchannel load-balancing**, **show interfaces port-channel vlan mapping**.

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.

EtherChannel Flow-Based Limited 1 1 Redundancy

EtherChannel flow-based limited 1:1 redundancy provides MAC, or layer 2, traffic protection to avoid higher layer protocols from reacting to single link failures and re-converging. To use EtherChannel flow-based limited 1:1 redundancy, you configure an EtherChannel with two ports (one active and one standby). If the active link goes down, the EtherChannel stays up and the system performs fast switchover to the hot-standby link. Depending on how you have the priorities set, when the failed link becomes operational again, the EtherChannel performs another fast switchover to revert to the original active link. if all port-priorities are the same, it will not revert, but remain on the current active link.

With 1:1 redundancy configured, only one link is active at any given time so all flows are directed over the active link.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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.

Information About EtherChannel Flow-Based Limited 1 1 Redundancy

EtherChannel Flow-Based Limited 1 1 Redundancy

EtherChannel flow-based limited 1:1 redundancy provides an EtherChannel configuration with one active link and fast switchover to a hot standby link. To use EtherChannel flow-based limited 1:1 redundancy, you configure a Link Aggregation Control Protocol (LACP) EtherChannel with two ports (one active and one standby). If the active link goes down, the EtherChannel stays up and the system performs fast switchover to the hot standby link. Depending on how the priorities of the links are set, when the failed link becomes operational again, the EtherChannel performs another fast switchover to revert to the original active link, or to the link with the higher priority.

For EtherChannel flow-based limited 1:1 redundancy to work correctly (especially the fast switchover capability) the feature must be enabled at both ends of the link.

How to Configure EtherChannel Flow-Based Limited 1 1 Redundancy

Configuring EtherChannel Flow-Based Limited 1 1 Redundancy with Fast-Switchover

To configure an LACP EtherChannel with two ports (one active and one standby), perform the following steps. This feature must be enabled at both ends of the link.

You can control which link is the primary active link by setting the port priority on the links used for the redundancy. To configure a primary link and enable the EtherChannel to revert to the original link, one link must have a higher port priority than the other and the LACP max-bundle must be set to 1. This configuration results in link 1 being active and link 2 being in hot standby state.

To prevent the switchover to revert, you can assign both links the same priority.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface port-channel** *channel -number*
4. **lacp fast-switchover**
5. **lacp max-bundle 1**
6. **exit**
7. **interface tengigabitethernet** *slot* / *port* / *number*
8. **channel-group 1 mode** *mode*
9. **lacp port-priority** *priority*
10. **exit**
11. **interface tengigabitethernet** *slot* / *port* / *number*
12. **channel-group 1 mode** *mode*
13. **lacp port-priority** *priority*
14. **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 port-channel** *channel -number* **Example:** `Router(config)# interface port-channel 1`	Selects an LACP port channel interface.
Step 4	**lacp fast-switchover** **Example:** `Router(config-if)# lacp fast-switchover`	Enables the fast switchover feature for this EtherChannel.

	Command or Action	Purpose
Step 5	**lacp max-bundle 1** **Example:** `Router(config-if)# lacp max-bundle 1`	Sets the maximum number of active member ports to 1.
Step 6	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode and returns to global configuration mode.
Step 7	**interface tengigabitethernet** *slot* / *port* / *number* **Example:** `Router(config)# interface tengigabitethernet 0/0/0`	Selects the first interface to add to the port channel.
Step 8	**channel-group 1 mode** *mode* **Example:** `Router(config-if)# channel-group 1 mode active`	Adds the member link to the port-channel and actively participates in LACP negotiation.
Step 9	**lacp port-priority** *priority* **Example:** `Router(config-if)# lacp port-priority 32768`	Sets the priority on the port-channel. This priority is set to the default value.
Step 10	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode and returns to global configuration mode.
Step 11	**interface tengigabitethernet** *slot* / *port* / *number* **Example:** `Router(config)# interface tengigabitethernet 1/0/0`	Selects the interface to add to the port channel.

	Command or Action	Purpose
Step 12	**channel-group 1 mode** *mode* **Example:** `Router(config-if)# channel-group 1 mode active`	Adds the member link to the port-channel and actively participates in LACP negotiation.
Step 13	**lacp port-priority** *priority* **Example:** `Router(config-if)# lacp port-priority 32767`	Sets the port priority higher than the other link by using a value lower than the default value of 32768. This forces this link to be the active link whenever it is capable of carrying traffic.

Step 14	**end**
	Example:
	`Router(config-if)# end`
		Exits interface configuration mode.

Setting the Switchover Rate with Carrier Delay

Optionally, you can control the speed of the switchover between the active and standby links by setting the carrier delay on each link. The **carrier-delay** command controls how long it takes for Cisco IOS to propagate the information about the links status to other modules.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface tengigabitethernet** *slot* / *port* / *number*
4. **carrier-delay msec** *msec*
5. **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	**interface tengigabitethernet** *slot* / *port* / *number* **Example:** `Router(config)# interface tengigabitethernet 0/1/0`	Enters interface configuration mode and opens the configuration for the specified interface.
Step 4	**carrier-delay msec** *msec* **Example:** `Router(config-if)# carrier-delay msec 11`	Sets how long it takes to propagate the link status to other modules.

Step 5	**end**
	Example:
	`Router(config-if)# end`
		Exits interface configuration mode.

Verifying EtherChannel Flow-Based Limited 1 1 Redundancy

Use these show commands to verify the configuration and to display information about the port channel.

SUMMARY STEPS

1. **enable**
2. **show running-config interface** *type slot* / *port* / *number*
3. **show interfaces port-channel** *channel-number* **etherchannel**
4. **show etherchannel** *channel-number* **port-channel**
5. **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	**show running-config interface** *type slot* / *port* / *number* **Example:** `Router# show running-config interface tengigabitethernet 0/0/0`	Verifies the configuration. - *type* --**gigabitethernet** or **tengigabitethernet**.
Step 3	**show interfaces port-channel** *channel-number* **etherchannel** **Example:** `Router# show interfaces port-channel 1 etherchannel`	Displays the bucket distribution currently in use.
Step 4	**show etherchannel** *channel-number* **port-channel** **Example:** `Router# show etherchannel 1 port-channel`	Displays the port channel fast-switchover feature capability.

Step 5	**end**
	Example:
	`Router# end`
		Exits privileged EXEC mode.

Configuration Examples for EtherChannel Flow-Based Limited1 1 Redundancy

- EtherChannel 1 1 Active Standby Example, page 55
- Setting Priority for 1 1 Redundancy Using LACP Example, page 56

EtherChannel 1 1 Active Standby Example

This example shows how to configure a port channel for 1:1 link redundancy for equal priority ports so there is no preference which port is active.

```
Router# enable
Router# configure terminal
Router(config)# interface port-channel 2
Router(config-if)# ip address 10.1.1.1 255.255.0.0
Router(config-if)# negotiation auto
Router(config-if)# lacp max-bundle 1
Router(config-if)# lacp fast-switchover
Router(config)# interface Tengigabitethernet0/1/0
Router(config-if)# channel-group 2 mode active
Router(config-if)# negotiation auto
Router(config)# interface Tengigabitethernet 2/1/0
Router(config-if)# channel-group 2 mode active
Router(config-if)# negotiation auto
Router(config)# interface GigabitEthernet0/1/6
Router(config-if)# negotiation auto
Router(config-if)# channel-group 19 mode active
Router(config)# interface GigabitEthernet0/1/7
Router(config-if)# negotiation auto
Router(config-if)# channel-group 19 mode active
Router(config-if)# interface Port-channel19
Router(config-if)# ip address 10.19.1.1 255.255.255.0
Router(config-if)# no negotiation auto
Router(config-if)# lacp fast-switchover
Router(config-if)# lacp max-bundle 1
Router(config-if)# end
```

Notice in the **show** command display the priorities are the same value.

```
Router# show lacp internal
Flags: S - Device is requesting Slow LACPDUs
    F - Device is requesting Fast LACPDUs
    A - Device is in Active mode P - Device is in Passive mode
Channel group 19
LACP port Admin Oper Port Port
Port Flags State Priority Key Key Number State
Gi0/1/6 SA bndl 32768 0x13 0x13 0x47 0x3D
Gi0/1/7 FA hot-sby 32768 0x13 0x13 0x48 0x7
```

Setting Priority for 1 1 Redundancy Using LACP Example

This example shows how to configure an LACP EtherChannel with 1:1 redundancy. GigabitEthernet 0/1/7 is the active link, because it is configured with a lower number which give it a higher port priority.

```
Router# configure terminal
Router(config)# interface GigabitEthernet0/1/6
Router(config-if)# lacp port-priority 32767
Router(config-if)# exit
Router(config)# interface GigabitEthernet0/1/7
Router(config-if)# lacp fast-switchover
Router(config-if)# lacp max-bundle 1
Router(config-if)# negotiation auto
Router(config-if)# channel-group 19 mode active
```

In this show display, notice that the bundled link is set at a higher priority. This will ensure that the bundled link is used as the first active link in the standby configuration.

```
Router# show lacp internal

Flags: S - Device is requesting Slow LACPDUs
    F - Device is requesting Fast LACPDUs
    A - Device is in Active mode P - Device is in Passive mode
Channel group 19
LACP port Admin Oper Port Port
Port Flags State Priority Key Key Number State
Gi0/1/6 FA hot-sby 32768 0x13 0x13 0x47 0x7
Gi0/1/7 SA bndl 32767 0x13 0x13 0x48 0x3D
```

Additional References

The following sections provide references related to the EtherChannel Flow-based Limited1:1 Redundancy feature.

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
LAN Switching commands	*Cisco IOS LAN Switching Command Reference*

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS XE software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported by this feature, and support for existing standards has not been modified by this feature.	--

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/cisco/web/support/index.html

Feature Information for EtherChannel Flow-based Limited 1 1 Redundancy

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 8 Feature Information for EtherChannel Flow-based Limited 1:1 Redundancy

Feature Name	Releases	Feature Information
EtherChannel Flow-Based Limited 1:1 Redundancy	Cisco IOS XE Release 2.4	EtherChannel flow-based limited 1:1 redundancy provides MAC, or layer 2, traffic protection to avoid higher layer protocols from reacting to single link failures and re-converging. To use EtherChannel flow-based limited 1:1 redundancy, you configure an EtherChannel with two ports (one active and one standby). If the active link goes down, the EtherChannel stays up and the system performs fast switchover to the hot-standby link. Depending on how you have the priorities set, when the failed link becomes operational again, the EtherChannel performs another fast switchover to revert to the original active link. if all port-priorities are the same, it will not revert, but remain on the current active link. No commands were modified or created to support this feature.

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.

Flow-Based per Port-Channel Load Balancing

The Flow-Based per Port-Channel Load Balancing feature allows different flows of traffic over a Gigabit EtherChannel (GEC) interface to be identified based on the packet header and then mapped to the different member links of the port channel. This feature enables you to apply flow-based load balancing and VLAN-manual load balancing to specific port channels.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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.

Restrictions for Flow-Based per Port-Channel Load Balancing

- Supports up to 64 GEC interfaces.
- Supports up to four member links per GEC interface.

Information About Flow-Based per Port-Channel Load Balancing

Flow-Based Load Balancing

Flow-based load balancing identifies different flows of traffic based on the key fields in the data packet. For example, IPv4 source and destination IP addressees can be used to identify a flow. The various data traffic flows are then mapped to the different member links of a port channel. After the mapping is done, the data traffic for a flow is transmitted through the assigned member link. The flow mapping is dynamic and changes when there is any change in the state of a member link to which a flow is assigned. The flow mappings can also change if member links are added to or removed from the GEC interface. Multiple flows can be mapped to each member link.

Buckets for Flow-Based Load Balancing

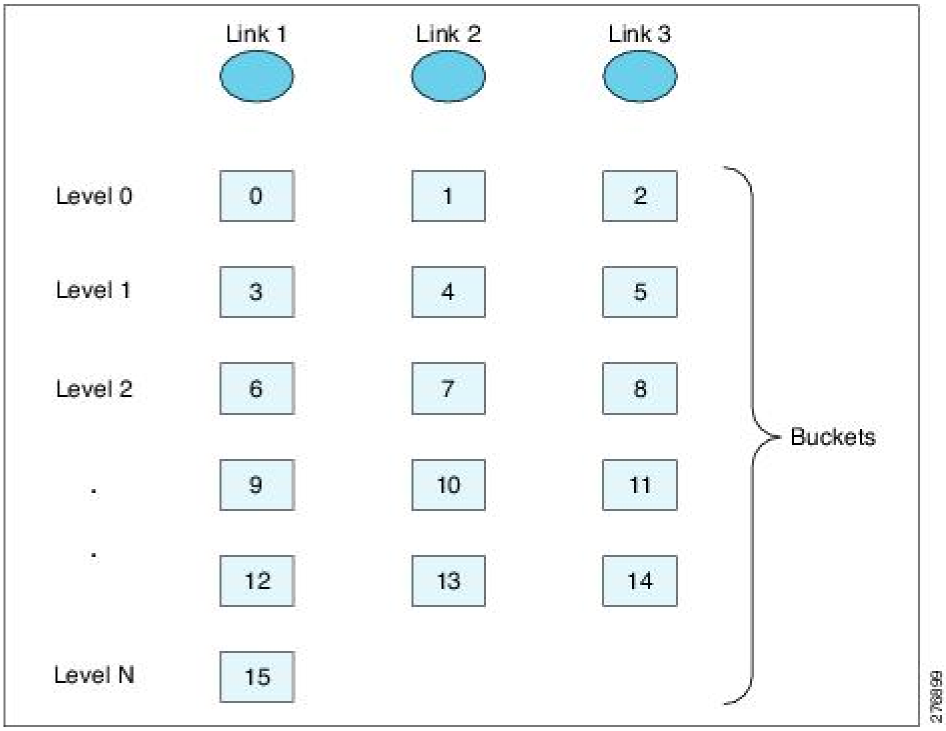
Load balancing dynamically maps traffic flows to the member links of a GEC interface through the concept of buckets. The various defined traffic flows are mapped to the buckets and the buckets are evenly distributed among the member links. Each port channel maintains 16 buckets, with one active member link associated with each bucket. All traffic flows mapped to a bucket use the member link to which the bucket is assigned.

The router creates the buckets-to-member links mappings when you apply flow-based load balancing to a port channel and the port channel has at least one active member link. The mappings are also created when the first member link is added, or comes up, and the load-balancing method is set to flow-based.

When a member link goes down or is removed from a port channel, the buckets associated with that member link are redistributed among the other active member links in a round-robin fashion. When a member link comes up or is added to a port channel, some of the buckets associated with other links are assigned to this link.

The figure below illustrates an example of 16 buckets distributed among three member links. The numbers shown in the buckets are the bucket IDs. Note that the first member link has an extra bucket.

Figure 6 Example of 16 Buckets Mapped to Three Member Links



If you change the load-balancing method, the bucket-to-member link mappings for flow-based load balancing are deleted. The mappings are also deleted if the port channel is deleted or the last member link in the port channel is deleted or goes down.

Load Balancing on Port Channels

GEC interfaces can use either dynamic flow-based load balancing or VLAN-manual load balancing. You can configure the load-balancing method globally for all port channels or directly on specific port channels. The global configuration applies only to those port channels for which you have not explicitly configured load balancing. The port-channel configuration overrides the global configuration.

Flow-based load balancing is enabled by default at the global level. You must explicitly configure VLAN load balancing or the load-balancing method is flow-based.

For more information about configuring VLAN load balancing, see the module VLAN Mapping to Gigabit EtherChannel (GEC) Member Links.

The table below lists the load-balancing method that is applied to port channels based on the configuration:

Table 9 Flow-Based Load Balancing Configuration Options

Global Configuration	Port-Channel Configuration	Load Balancing Applied
Not configured	Not configured	Flow-based
	Flow-based	Flow-based
	VLAN-manual	VLAN-manual
VLAN-manual	Not configured	VLAN-manual
	Flow-based	Flow-based
	VLAN-manual	VLAN-manual

The table below lists the configuration that results if you change the global load-balancing method.

Table 10 Results When Global Configuration Changes

Port-Channel Configuration	Global Configuration	Action Taken at Port Channel	
–	From	To	–
Not configured	Not configured	VLAN-manual	Changed from flow-based to VLAN-manual
	VLAN-manual	Not configured	Changed from VLAN-manual to flow-based
Configured	Any	Any	No change

The table below lists the configuration that results if you change the port-channel load-balancing method.

Table 11 Results When Port-Channel Configuration Changes

Global Configuration	Port-Channel Configuration	Action Taken at Port Channel	
–	From	To	–
Not configured	Not configured	VLAN-manual	Changed from flow-based to VLAN-manual
	Not configured	Flow-based	No action taken
	VLAN-manual	Flow-based	Changed from VLAN-manual to flow-based
	VLAN-manual	Not configured	Changed from VLAN-manual to flow-based
	Flow-based	VLAN-manual	Changed from flow-based to VLAN-manual
	Flow-based	Not configured	No action taken
VLAN-manual	Not configured	VLAN-manual	No action taken
	Not configured	Flow-based	Changed from VLAN-manual to flow-based
	VLAN-manual	Flow-based	Changed from VLAN-manual to flow-based
	VLAN-manual	Not configured	No action taken
	Flow-based	VLAN-manual	Changed from flow-based to VLAN-manual
	Flow-based	Not configured	Changed from flow-based to VLAN-manual

How to Enable Flow-Based per Port-Channel Load Balancing

- Configuring Load Balancing on a Port Channel, page 64
- Verifying Load-Balancing Configuration on a GEC Interface, page 65

Configuring Load Balancing on a Port Channel

To configure load balancing on a port channel, perform the following steps. Repeat these steps for each GEC interface.

If you have already configured your desired load-balancing method globally and want to use that method for all port channels, you need not perform this task. To configure load balancing globally, use the **port-**

channel load-balancing vlan-manual command. If you do not configure the global command, flow-based load balancing is applied to all port channels.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface port-channel** *channel-number*
4. **load-balancing** {**flow** | **vlan**}
5. **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 port-channel** *channel-number* **Example:** `Router(config)# interface port-channel 1`	Enters interface configuration mode and defines the interface as a port channel.

Step 4	**load-balancing** {**flow** | **vlan**}
	Example:
	`Router(config-if)# load-balancing flow`
		Applies a load-balancing method to the specific port channel.
		• If you do not configure this command, the port channel uses the global load-balancing method configured with the **port-channel load-balancing vlan-manual** command. The global default is flow-based.

Step 5	**end**
	Example:
	`Router(config-if)# end`
		Exits configuration mode.

Verifying Load-Balancing Configuration on a GEC Interface

Use these show commands to verify the load-balancing configuration and to display information about the bucket distribution on the port channel. You can use these commands in any order.

SUMMARY STEPS

1. **show running-config interface port-channel** *channel-number*
2. **show etherchannel load-balancing**
3. **show interfaces port-channel** *channel-number* **etherchannel**

DETAILED STEPS

Step 1 **show running-config interface port-channel** *channel-number*

Use this command to verify the configuration of the port channel.

Example:

```
Router# show running-config interface port-channel 1
Building configuration...

Current configuration : 88 bytes
!
interface Port-channel1
 ip address 10.1.1.1 255.0.0.0
 no negotiation auto
 load-balancing flow
end
```

Step 2 **show etherchannel load-balancing**

Use this command to display the load-balancing method applied to each port channel. The following example shows output for a configuration with load balancing set globally to VLAN-manual and set to flow-based on port channel 1:

Example:

```
Router# show etherchannel load-balancing


EtherChannel Load-Balancing Method:
Global LB Method: vlan-manual

  Port-Channel:                       LB Method
    Port-channel1                   :  flow-based
```

Step 3 **show interfaces port-channel** *channel-number* **etherchannel**

Use this command to display the bucket distribution currently in use. The following example shows output for an interface with load balancing set to flow-based:

Example:

```
Router(config)# show interface port-channel 2 etherchannel

 All IDBs List contains 3 configured interfaces
  Port: GigabitEthernet2/1/6 (index: 0)
  Port: GigabitEthernet2/1/7 (index: 1)
  Port: GigabitEthernet2/1/0 (index: 2)

 Active Member List contains 1 interfaces
  Port: GigabitEthernet2/1/0

 Passive Member List contains 2 interfaces
 Port: GigabitEthernet2/1/6

 Port: GigabitEthernet2/1/7

Load-Balancing method applied: flow-based

Bucket Information for Flow-Based LB:
Interface:                                Buckets
   GigabitEthernet2/1/0:
                          Bucket 0 , Bucket 1 , Bucket 2 , Bucket 3
                          Bucket 4 , Bucket 5 , Bucket 6 , Bucket 7
                          Bucket 8 , Bucket 9 , Bucket 10, Bucket 11
                          Bucket 12, Bucket 13, Bucket 14, Bucket 15
```

Configuration Examples for Flow-Based per Port-Channel Load Balancing

Flow-Based Load Balancing Example

The following example shows a configuration where flow-based load balancing is configured on port-channel 2 while the VLAN-manual method is configured globally:

```
!
no aaa new-model
port-channel load-balancing vlan-manual
ip source-route
.
.
.
interface Port-channel2
 ip address 10.0.0.1 255.255.255.0
 no negotiation auto
 load-balancing flow
!
interface Port-channel2.10
 ip rsvp authentication key 11223344
 ip rsvp authentication
!
interface Port-channel2.50
 encapsulation dot1Q 50
!
interface GigabitEthernet2/1/0
 no ip address
 negotiation auto
 cdp enable
 channel-group 2
!
```

Additional References

The following sections provide references related to the Flow-Based per Port-Channel Load Balancing feature.

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Cisco IOS LAN switching commands	*Cisco IOS LAN Switching Command Reference*

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS XE software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported by this feature, and support for existing standards has not been modified by this feature.	--

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/cisco/web/support/index.html

Feature Information for Flow-Based per Port-Channel Load Balancing

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 12 Feature Information for Flow-Based per Port-Channel Load Balancing

Feature Name	Releases	Feature Information
Flow-Based per Port-Channel Load Balancing	Cisco IOS XE Release 2.5	This feature allows different flows of traffic over a GEC interface to be identified and mapped to the different member links. It also enables you to apply load balancing to specific port channels. The following commands were introduced or modified: **load-balancing**, **port-channel load-balancing vlan-manual**, **show etherchannel load-balancing, show interfaces port-channel etherchannel**.
IPv6 Loadbalancing on GEC	Cisco IOS XE Release 3.4S	The IPv6 Loadbalancing on GEC feature provides load balancing for IPv6 traffic on Gigabit EtherChannel.

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.