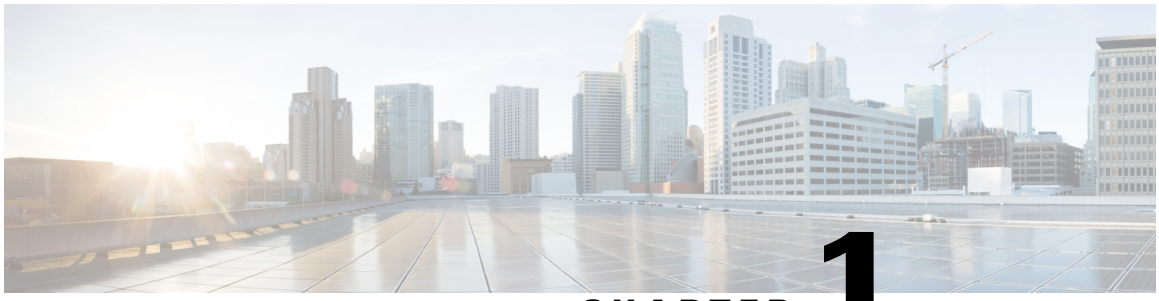
Carrier Ethernet Configuration Guide, Cisco IOS XE Release 3E

First Published: June 28, 2014

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

CONTENTS



CHAPTER 1

Using Link Layer Discovery Protocol in Multivendor Networks

Link Layer Discovery Protocol (LLDP), standardized by the IEEE as part of 802.1ab, enables standardized discovery of nodes, which in turn facilitates future applications of standard management tools such as Simple Network Management Protocol (SNMP) in multivendor networks. Using standard management tools makes physical topology information available and helps network administrators detect and correct network malfunctions and inconsistencies in configuration.

Media Endpoint Discovery (MED) is an LLDP enhancement that was formalized by the Telecommunications Industry Association (TIA) for voice over IP (VoIP) applications.

The Cisco implementation of LLDP is based on the IEEE 802.1ab standard. This document describes LLDP and LLDP-MED and how they are supported in Cisco software.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and 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.

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 Using Link Layer Discovery Protocol in Multivendor Networks

- Type-Length-Value (TLV) types 0 through 127
- To support LLDP-MED, the following organizationally specific TLVs must be implemented:
  - Extended Power-via-Media Dependent Interface (MDI)
  - Inventory
  - LLDP-MED Capabilities
  - MAC/PHY Configuration Status
  - Network Policy
  - Port VLAN ID

Restrictions for Using Link Layer Discovery Protocol in Multivendor Networks

- Use of LLDP is limited to 802.1 media types such as Ethernet, Token Ring, and Fiber Distributed Data Interface (FDDI) networks.
- The maximum number of neighbor entries per chassis is limited on MED-capable network connectivity devices.

Information About Using Link Layer Discovery Protocol in Multivendor Networks

IEEE 802.1ab LLDP

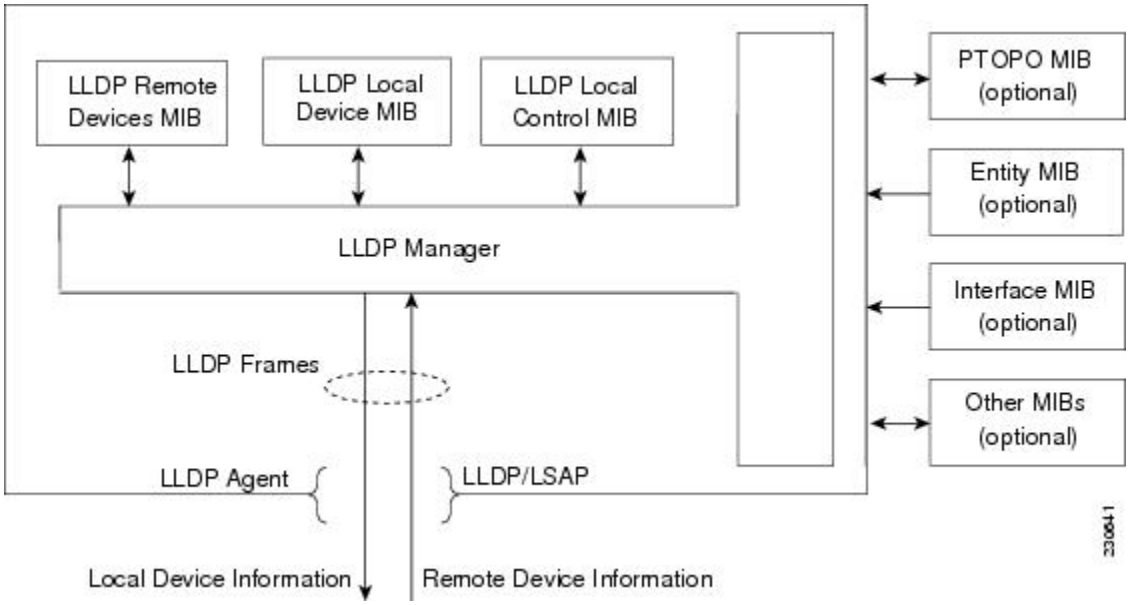
IEEE 802.1ab Link Layer Discovery Protocol (LLDP) is an optional link layer protocol for network topology discovery in multivendor networks. Discovery information includes device identifiers, port identifiers, versions, and other details. As a protocol that aids network management, LLDP provides accurate network mapping, inventory data, and network troubleshooting information.

LLDP is unidirectional, operating only in an advertising mode. LLDP does not solicit information or monitor state changes between LLDP nodes. LLDP periodically sends advertisements to a constrained multicast address. Devices supporting LLDP can send information about themselves while they receive and record information about their neighbors. Additionally, devices can choose to turn off the send or receive functions independently. Advertisements are sent out and received on every active and enabled interface, allowing any device in a network to learn about all devices to which it is connected. Applications that use this information

include network topology discovery, inventory management, emergency services, VLAN assignment, and inline power supply.

Note LLDP and Cisco Discovery Protocol can operate on the same interface.

The figure below shows a high-level view of LLDP operating in a network node.



When you configure LLDP or Cisco Discovery Protocol location information on a per-port basis, remote devices can send Cisco medianet location information to the switch. For more information, see the *Using Cisco Discovery Protocol module.*

LLDP-MED

LLDP-MED operates between several classes of network equipment such as IP phones, conference bridges, and network connectivity devices such as routers and switches. By default, a network connectivity device sends out only LLDP packets until it receives LLDP-MED packets from an endpoint device. The network device then sends out LLDP-MED packets until the remote device to which it is connected ceases to be LLDP-MED capable.

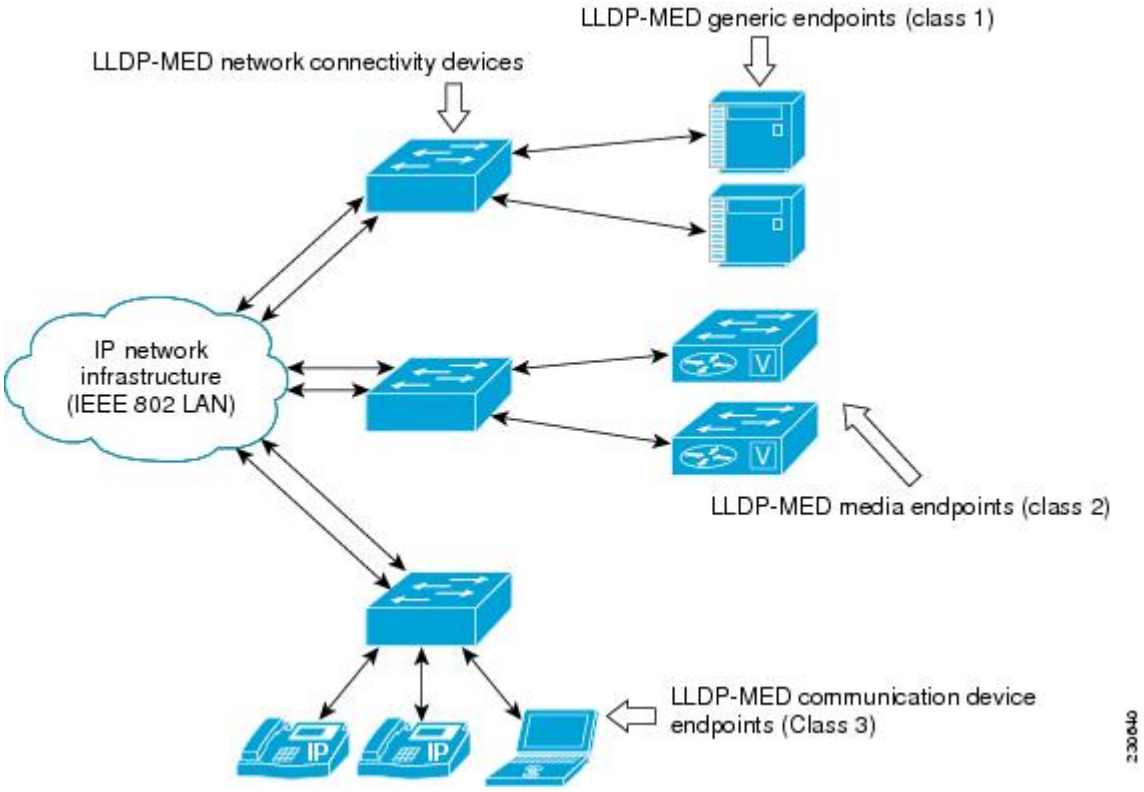
Classes of Endpoints

LLDP-MED network connectivity devices provide IEEE 802 network access to LLDP-MED endpoints. LLDP-MED supports the following three classes of endpoints:

- Generic (class 1)—Basic participant endpoints; for example, IP communications controllers.
- Media (class 2)—Endpoints that support media streams; for example, media gateways and conference bridges.

- Communication Device (class 3)—Endpoints that support IP communications end users; for example, IP phones and Softphone.

The figure below shows an LLDP-MED-enabled LAN.



Types of Discovery Supported

LLDP-MED provides support to discover the following types of information, which are crucial to efficient operation and management of endpoint devices and the network devices supporting them:

- **Capabilities —**Endpoints determine the types of capabilities that a connected device supports and which ones are enabled.
- **Inventory —**LLDP-MED support exchange of hardware, software, and firmware versions, among other inventory details.
- **LAN speed and duplex —**Devices discover mismatches in speed and duplex settings.
- **Location identification —**An endpoint, particularly a telephone, learns its location from a network device. This location information may be used for location-based applications on the telephone and is important when emergency calls are placed.
- **Network policy —**Network connectivity devices notify telephones about the VLANs they should use.
- **Power —**Network connectivity devices and endpoints exchange power information. LLDP-MED provides information about how much power a device needs and how a device is powered. LLDP-MED also determines the priority of the device for receiving power.

Benefits of LLDP-MED

- Follows an open standard
- Supports E-911 emergency service, which is aided by location management
- Provides fast start capability
- Supports interoperability between multivendor devices
- Supports inventory management (location, version, etc.)
- Provides MIB support
- Supports plug and play installation
- Provides several troubleshooting (duplex, speed, network policy) mechanisms

TLV Elements

Link Layer Discovery Protocol (LLDP) and LLDP-Media Endpoint Discovery (MED) use Type-Length-Values (TLVs) to exchange information between network and endpoint devices. TLV elements are embedded in communications protocol advertisements and used for encoding optional information. The size of the type and length fields is fixed at 2 bytes. The size of the value field is variable. The type is a numeric code that indicates the type of field that this part of the message represents, and the length is the size of the value field, in bytes. The value field contains the data for this part of the message.

LLDP-MED supports the following TLVs:

- LLDP-MED capabilities TLV—Allows LLDP-MED endpoints to determine the capabilities that the connected device supports and has enabled.
- Network policy TLV—Allows both network connectivity devices and endpoints to advertise VLAN configurations and associated Layer 2 and Layer 3 attributes for the specific application on that port. For example, the switch can notify a phone of the VLAN number that it should use. The phone can connect to any switch, obtain its VLAN number, and then start communicating with the call control.

By defining a network-policy profile TLV, you can create a profile for voice and voice signalling by specifying the values for VLAN, class of service (CoS), differentiated services code point (DSCP), and tagging mode. These profile attributes are then maintained centrally on the switch and propagated to the phone.

- Power management TLV—Enables advanced power management between LLDP-MED endpoint and network connectivity devices. Allows switches and phones to convey power information, such as how the device is powered, power priority, and how much power the device needs. Supports advertisement of fractional wattage power requirements, endpoint power priority, and endpoint and network connectivity-device power status but does not provide for power negotiation between the endpoint and the network connectivity devices. When LLDP is enabled and power is applied to a port, the power TLV determines the actual power requirement of the endpoint device so that the system power budget can be adjusted accordingly. The switch processes the requests and either grants or denies power based on the current power budget. If the request is granted, the switch updates the power budget. If the request is denied, the switch turns off power to the port, generates a syslog message, and updates the power budget. If LLDP-MED is disabled or if the endpoint does not support the LLDP-MED power TLV, the initial allocation value is used throughout the duration of the connection.

Note A system power budget is the default power allocated to a device based on its device class. However, the total power that can be sourced from a switch is finite, and there will be some power budgeting done by the power module based on the number of ports already being served, total power that can be served, and how much new ports are requesting.

- Inventory management TLV—Allows an endpoint to send detailed inventory information about itself to the switch, including information hardware revision, firmware version, software version, serial number, manufacturer name, model name, and asset ID TLV.
- Location TLV—Provides location information from the switch to the endpoint device. The location TLV can send this information:
  - Civic location information—Provides the civic address information and postal information. Examples of civic location information are street address, road name, and postal community name information.
  - ELIN location information—Provides the location information of a caller. The location is determined by the Emergency location identifier number (ELIN), which is a phone number that routes an emergency call to the local public safety answering point (PSAP) and which the PSAP can use to call back the emergency caller.

Benefits of LLDP

- Follows IEEE 802.1ab standard.
- Enables interoperability among multivendor devices.
- Facilitates troubleshooting of enterprise networks and uses standard network management tools.
- Provides extension for applications such as VoIP.

How to Configure Link Layer Discovery Protocol in Multivendor Networks

Enabling and Disabling LLDP Globally

LLDP is disabled globally by default. This section describes the tasks for enabling and disabling LLDP globally.

Enabling LLDP Globally

Perform this task to enable LLDP globally.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **lldp run**
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**lldp run** **Example:** `Device(config)# lldp run`	Enables LLDP globally. **Note** To disable LLDP globally, use the **no lldp run** command.
Step 4	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

Disabling and Enabling LLDP on a Supported Interface

LLDP is enabled by default on all supported interfaces. This section describes the tasks for disabling and enabling LLDP on a supported interface.

Disabling LLDP on a Supported Interface

Perform this task to disable LLDP on a supported interface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **no lldp** {**med-tlv-select** *tlv* | **receive** | **transmit**}
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Device(config)# interface Gigabitethernet 0/1`	Specifies the interface type and number and enters interface configuration mode.
Step 4	**no lldp** {**med-tlv-select** *tlv*	**receive**	**transmit**} **Example:** `Device(config-if)# no lldp receive`	Disables an LLDP-MED TLV or LLDP packet reception on a supported interface. **Note** To enable LLDP on a Supported Interface, use the **lldp** {**med-tlv-select** *tlv*	**receive**	**transmit** command.
Step 5	**end** **Example:** `Device(config-if)# end`	Returns to privileged EXEC mode.

Setting LLDP Packet Hold Time

Hold time is the duration that a receiving device should maintain LLDP neighbor information before aging it. Perform this task to define a hold time for an LLDP-enabled device.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **lldp holdtime** *seconds*
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**lldp holdtime** *seconds* **Example:** `Device(config)# lldp holdtime 100`	Specifies the hold time.
Step 4	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

Setting LLDP Packet Frequency

Perform this task to specify an interval at which the Cisco software sends LLDP updates to neighboring devices.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **lldp timer** *rate*
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**lldp timer** *rate* **Example:** `Device(config)# lldp timer 75`	Specifies the rate at which LLDP packets are sent every second.
Step 4	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

Monitoring and Maintaining LLDP in Multivendor Networks

Perform this task to monitor and maintain LLDP in multivendor networks. This task is optional, and Steps 2 and 3 can be performed in any sequence.

SUMMARY STEPS

1. **enable**
2. **show lldp** [**entry** {***** | *word*} | **errors** | **interface** [**ethernet** *number*]| **neighbors** [**ethernet** *number*| **detail**]| **traffic**]
3. **clear lldp** {**counters** | **table**}
4. **end**

DETAILED STEPS

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

	Command or Action	Purpose
	Example: `Device> enable`	• Enter your password if prompted.
Step 2	**show lldp** [**entry** {***** | *word*} | **errors** | **interface** [**ethernet** *number*]| **neighbors** [**ethernet** *number*| **detail**]| **traffic**] **Example:** `Device# show lldp entry *`	Displays summarized and detailed LLDP information. **Note** When the **show lldp neighbors** command is issued, if the device ID has more than 20 characters, the ID is truncated to 20 characters in command output because of display constraints.
Step 3	**clear lldp** {**counters** | **table**} **Example:** `Device# clear lldp counters`	Resets LLDP traffic counters and tables to zero.
Step 4	**end** **Example:** `Device# end`	Returns to user EXEC mode.

Enabling and Disabling LLDP TLVs

LLDP TLV support is enabled by default if LLDP is enabled globally and locally on a supported interface. Specific TLVs, however, can be enabled and suppressed.

Enabling LLDP TLVs

Perform this task to enable an LLDP TLV on a supported interface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **lldp tlv-select** *tlv*
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Device(config)# interface Gigabitethernet 0/1`	Specifies the interface type and number on which to enable LLDP-MED and enters interface configuration mode.
Step 4	**lldp tlv-select** *tlv* **Example:** `Device(config-if)# lldp tlv-select power-management`	Enables a specific LLDP TLV on a supported interface. **Note** To disable LLDP TLVs, use the **no lldp tlv-select** *tlv*
Step 5	**end** **Example:** `Device(config-if)# end`	Returns to privileged EXEC mode.

Enabling and Disabling LLDP-MED TLVs

LLDP-MED TLV support is enabled by default if LLDP is enabled globally and locally on a supported interface. Specific TLVs, however, can be enabled and suppressed.

Enabling LLDP-MED TLVs

Perform this task to enable a specific LLDP-MED TLV on a supported interface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **lldp med-tlv-select** *tlv*
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Device(config)# interface Gigabitethernet 0/1`	Specifies the interface type and number on which to enable LLDP-MED and enters interface configuration mode.
Step 4	**lldp med-tlv-select** *tlv* **Example:** `Device(config-if)# lldp med-tlv-select inventory-management`	Enables a specific LLDP-MED TLV on a supported interface. **Note** To disable LLDP-MED TLVs, use the **no lldp med-tlv-select** *tlv* command.
Step 5	**end** **Example:** `Device(config-if)# end`	Returns to privileged EXEC mode.

Configuration Examples for Link Layer Discovery Protocol in Multivendor Networks

Example: Configuring Voice VLAN

The following example shows how to configure voice VLAN and verify

```
Device1> enable
Device1# configure terminal
Device1(config)# interface GigabitEthernet0/1/7
Device1(config-if)# switchport voice vlan 10
Device1(config-if)# no ip address
Device1(config-if)# end
```

The following example displays the updated running configuration on Device 2. LLDP is enabled with hold time, timer, and TLV options configured.

```
Device1# show lldp neighbors detail

Local Intf: Gi0/1/7
Chassis id: 10.10.0.1
Port id: C8F9F9D61BC2:P1
Port Description: SW PORT
System Name: SEPC8F9F9D61BC2

System Description:
Cisco IP Phone 7962G,V12, SCCP42.9-3-1ES27S

Time remaining: 127 seconds
System Capabilities: B,T
Enabled Capabilities: B,T
Management Addresses:
    IP: 10.10.0.1
Auto Negotiation - supported, enabled
Physical media capabilities:
    1000baseT(HD)
    1000baseX(FD)
    Symm, Asym Pause(FD)
    Symm Pause(FD)
Media Attachment Unit type: 16
Vlan ID: - not advertised

MED Information:

    MED Codes:
          (NP) Network Policy, (LI) Location Identification
          (PS) Power Source Entity, (PD) Power Device
          (IN) Inventory

    H/W revision: 12
    F/W revision: tnp62.8-3-1-21a.bin
    S/W revision: SCCP42.9-3-1ES27S
    Serial number: FCH1610A5S5
    Manufacturer: Cisco Systems, Inc.
    Model: CP-7962G
    Capabilities: NP, PD, IN
    Device type: Endpoint Class III
    Network Policy(Voice): VLAN 10, tagged, Layer-2 priority: 5, DSCP: 46
    Network Policy(Voice Signal): VLAN 10, tagged, Layer-2 priority: 4, DSCP: 32
    PD device, Power source: Unknown, Power Priority: Unknown, Wattage: 6.3
    Location - not advertised
```

The following example shows how to configure LLDP timer, hold time, and TLVs options on Device 2.

```
Device> enable
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# lldp run
Device(config)# lldp holdtime 150
Device(config)# lldp timer 15
Device(config)# lldp tlv-select port-vlan
Device(config)# lldp tlv-select mac-phy-cfg
Device2(config)# interface ethernet 0/0
Device2(config-if)# lldp transmit
Device2(config-if)# end
00:08:32: %SYS-5-CONFIG_I: Configured from console by console
```

The following example shows that voice vlan has been configured on the IP phone.

```
Device1# show lldp traffic
LLDP traffic statistics:
    Total frames out: 20
    Total entries aged: 0
    Total frames in: 15
    Total frames received in error: 0
    Total frames discarded: 0
    Total TLVs unrecognized: 0
Device1# show lldp neighbors
Capability codes:
    (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
    (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
Device ID           Local Intf     Hold-time  Capability      Port ID
Device2             Et0/0          150        R               Et0/0
Total entries displayed: 1
Device2# show lldp traffic
LLDP traffic statistics:
    Total frames out: 15
    Total entries aged: 0
    Total frames in: 17
    Total frames received in error: 0
    Total frames discarded: 2
    Total TLVs unrecognized: 0
Device2# show lldp neighbors
Capability codes:
    (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
    (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
Device ID           Local Intf     Hold-time  Capability      Port ID
Device1             Et0/0          150        R               Et0/0
Total entries displayed: 1
```

Example Configuring LLDP on Two Devices

The following example shows how to configure LLDP timer, hold time, and TLVs on two devices in a network. In each case we assume that the Ethernet interfaces being configured are in the UP state.

```
! Configure LLDP on Device 1 with hold time, timer, and TLV options.

Device1> enable
Device1# configure terminal
Device1(config)# lldp run
Device1(config)# lldp holdtime 150
Device1(config)# lldp timer 15
Device1(config)# lldp tlv-select port-vlan
Device1(config)# lldp tlv-select mac-phy-cfg
Device1(config)# interface ethernet 0/0
Device1(config-if)# end
00:08:32: %SYS-5-CONFIG_I: Configured from console by console
! Show the updated running configuration. LLDP is enabled with hold time, timer, and TLV
options configured.
```

```
Device1# show running-config

Building configuration...
Current configuration : 1397 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Device1
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
clock timezone PST -8
ip subnet-zero
!
!
lldp timer 15
lldp holdtime 150
!


! Configure LLDP on Device 2 with hold time, timer, and TLV options.

Device2> enable
Device2# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device2(config)# lldp run
Device2(config)# lldp holdtime 150
Device2(config)# lldp timer 15
Device2(config)# lldp tlv-select port-vlan
Device2(config)# lldp tlv-select mac-phy-cfg
Device2(config)# interface ethernet 0/0
Device2(config-if)# end
00:08:32: %SYS-5-CONFIG_I: Configured from console by console

! Show the updated running configuration on Device 2. LLDP is enabled with hold time, timer,
 and TLV options configured.

Device2# show running-config
Building configuration...
Current configuration : 1412 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname R2
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
clock timezone PST -8
ip subnet-zero
!
!
lldp timer 15
lldp holdtime 150
!


! After both devices are configured for LLDP, issue the show
 command from each device to view traffic and device information.

Device1# show lldp traffic
```

```
LLDP traffic statistics:
    Total frames out: 20
    Total entries aged: 0
    Total frames in: 15
    Total frames received in error: 0
    Total frames discarded: 0
    Total TLVs unrecognized: 0
Device1# show lldp neighbors
Capability codes:
    (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
    (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
Device ID           Local Intf     Hold-time  Capability      Port ID
Device2             Et0/0          150        R               Et0/0
Total entries displayed: 1
Device2# show lldp traffic
LLDP traffic statistics:
    Total frames out: 15
    Total entries aged: 0
    Total frames in: 17
    Total frames received in error: 0
    Total frames discarded: 2
    Total TLVs unrecognized: 0
Device2# show lldp neighbors
Capability codes:
    (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
    (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
Device ID           Local Intf     Hold-time  Capability      Port ID
Device1             Et0/0          150        R               Et0/0
Total entries displayed: 1
```

Additional References for Using Link Layer Discovery Protocol in Multivendor Networks

Related Documents

Related Topic	Document Title
Cisco IOS commands: master list of commands with complete command syntax, command mode, command history, defaults, usage guidelines, and examples	Cisco IOS Master Command List, All Releases
Carrier Ethernet commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	*Cisco IOS Carrier Ethernet Command Reference*
LLDP	*Link Layer Discovery Protocol*
Per Port Location configurations	*Per Port Location Configuration*
Comparison of LLDP Media Endpoint Discovery (MED) and Cisco Discovery Protocol	*LLDP-MED and Cisco Discovery Protocol*

Standards and RFCs

Standards/RFCs	Title
IEEE 802.1ab	*Station and Media Access Control Connectivity Discovery*
RFC 2922	Physical Topology MIB

MIBs

MIB	MIBs Link
PTOPO MIB	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

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 Link Layer Discovery Protocol in Multivendor Networks

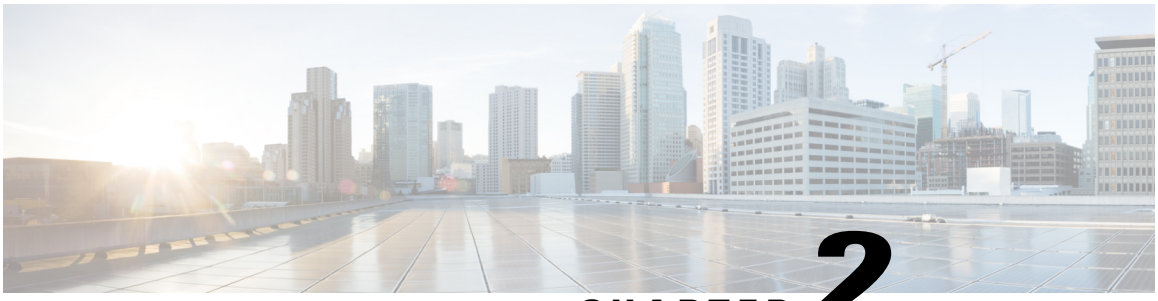
The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train 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 . An account on Cisco.com is not required.

Table 1: Feature Information for Using Link Layer Discovery Protocol in Multivendor Networks

Feature Name	Releases	Feature Information
IEEE 802.1ab LLDP (Link Layer Discovery Protocol)	Cisco IOS XE Release 3.6E	LLDP, standardized by the IEEE as part of 802.1ab, enables standardized discovery of nodes, which in turn facilitates future applications of standard management tools such as SNMP in multivendor networks. In Cisco IOS XE Release 3.6E, this feature is supported on Cisco Catalyst 3850 Series Switches. The following commands were introduced or modified: **clear lldp**, **lldp** and **show lldp**.
ANSI TIA-1057 LLDP-MED Support	Cisco IOS XE Release 3.6E	MED is an LLDP enhancement that was formalized by the TIA for VoIP applications. The Cisco implementation of LLDP is based on the IEEE 802.1ab standard. In Cisco IOS XE Release 3.6E, this feature is supported on Cisco Catalyst 3850 Series Switches. The following commands were introduced or modified: **lldp** and **lldp** (interface).

Feature Name	Releases	Feature Information
IEEE 802.1ab LLDP (Link Layer Discovery Protocol)	Cisco IOS XE Release 3.2E Cisco IOS XE Release 3.6E	IEEE 802.3ad link bundling and load balancing leverages the EtherChannel infrastructure within Cisco software to manage the bundling of various links. The network traffic load-balancing features help minimize network disruption that results when a port is added or deleted from a link bundle. MED is an LLDP enhancement that was formalized by the TIA for VoIP applications. In Cisco IOS XE Release 3.2SE, this feature is supported on the following platforms: • Cisco 5700 Series Wireless LAN Controllers • Cisco Catalyst 3850 Series Switches In Cisco IOS XE Release 3.3SE, this feature is supported on the following platforms: • Cisco Catalyst 3650 Series Switches
LLDP MED Support on ISRG2	Cisco IOS XE Release 3.6E	The LLDP MED feature is supported on Cisco Integrated Services Routers Generation 2 (ISR G2). In Cisco IOS XE Release 3.6E, this feature is supported on Cisco Catalyst 3850 Series Switches. No commands were introduced or modified.



CHAPTER 2

Configuring IEEE 802.3ad Link Bundling and Load Balancing

This document describes how the IEEE 802.3ad link bundling and load balancing leverages the EtherChannel infrastructure within Cisco software to manage the bundling of various links. Also described are network traffic load-balancing features to help minimize network disruption that results when a port is added or deleted from a link bundle.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and 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.

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 Configuring IEEE 802.3ad Link Bundling and Load Balancing

- Knowledge of how EtherChannels and Link Aggregation Control Protocol (LACP) function in a network
- Knowledge of load balancing to mitigate network traffic disruptions
- Verification that both ends of the LACP link have the same baseline software version

Restrictions for Configuring IEEE 802.3ad Link Bundling and Load Balancing

- The number of links supported per bundle is bound by the platform.
- All links must operate at the same link speed and in full-duplex mode (LACP does not support half-duplex mode).
- All links must be configured either as EtherChannel links or as LACP links.
- Only physical interfaces can form aggregations. Aggregations of VLAN interfaces are not possible nor is an aggregation of aggregations.
- If a router is connected to a switch, the bundle terminates on the switch.
- An EtherChannel will not form if one of the LAN ports is a Switched Port Analyzer (SPAN) destination port.
- All ports in an EtherChannel must use the same EtherChannel protocol.
- The LACP Single Fault Direct Load Balance Swapping feature is limited to a single bundled port failure.
- The LACP Single Fault Direct Load Balance Swapping feature cannot be used with the Port Aggregation Protocol (PagP).
- LACP port priority cannot be configured with LACP single fault direct load balance swapping.
- The adaptive algorithm does not apply to service control engines (SCEs) when EtherChannel load distribution is used.

Information About Configuring IEEE 802.3ad Link Bundling and Load Balancing

Gigabit EtherChannel

Gigabit EtherChannel is high-performance Ethernet technology that provides Gbps transmission rates. A Gigabit EtherChannel bundles individual Gigabit Ethernet links into a single logical link that provides the

aggregate bandwidth of up to eight physical links. All LAN ports in each EtherChannel must be the same speed and all must be configured either as Layer 2 or as Layer 3 LAN ports. Inbound broadcast and multicast packets on one link in an EtherChannel are blocked from returning on any other link in the EtherChannel.

When a link within an EtherChannel fails, traffic previously carried over the failed link switches to the remaining links within that EtherChannel. Also when a failure occurs, a trap is sent that identifies the device, the EtherChannel, and the failed link.

Port Channel and LACP-Enabled Interfaces

Each EtherChannel has a numbered port channel interface that, if not already created, is created automatically when the first physical interface is added to the channel group. The configuration of a port channel interface affects all LAN ports assigned to that port channel interface.

To change the parameters of all ports in an EtherChannel, change the configuration of the port channel interface: for example, if you want to configure Spanning Tree Protocol or configure a Layer 2 EtherChannel as a trunk. Any configuration or attribute changes you make to the port channel interface are propagated to all interfaces within the same channel group as the port channel; that is, configuration changes are propagated to the physical interfaces that are not part of the port channel but are part of the channel group.

The configuration of a LAN port affects only that LAN port.

IEEE 802.3ad Link Bundling

The IEEE 802.3ad Link Bundling feature provides a method for aggregating multiple Ethernet links into a single logical channel based on the IEEE 802.3ad standard. This feature helps improve the cost effectiveness of a device by increasing cumulative bandwidth without necessarily requiring hardware upgrades. In addition, IEEE 802.3ad link bundling provides a capability to dynamically provision, manage, and monitor various aggregated links and enables interoperability between various Cisco devices and devices of third-party vendors.

LACP uses the following parameters:

- LACP port priority—You must configure an LACP port priority on each port configured to use LACP. The port priority can be configured automatically or through the CLI. LACP uses the port priority to decide which ports should be put in standby mode when there is a hardware limitation that prevents all compatible ports from aggregating. LACP also uses the port priority with the port number to form the port identifier.
-

Benefits of IEEE 802.3ad Link Bundling

- Increased network capacity without changing physical connections or upgrading hardware
- Cost savings from the use of existing hardware and software for additional functions
- A standard solution that enables interoperability of network devices
- Port redundancy without user intervention when an operational port fails

EtherChannel Load Balancing

EtherChannel load balancing can use MAC addresses; IP addresses; Layer 4 port numbers; either source addresses, destination addresses, or both; or ports. The selected mode applies to all EtherChannels configured on the device.

Traffic load across the links in an EtherChannel is balanced by reducing part of the binary pattern, formed from the addresses in the frame, to a numerical value that selects one of the links in the channel. When a port is added to an EtherChannel or an active port fails, the load balance bits are reset and reassigned for all ports within that EtherChannel and reprogrammed into the ASIC for each port. This reset causes packet loss during the time the reassignment and reprogramming is taking place. The greater the port bandwidth, the greater the packet loss.

Load Distribution in an EtherChannel

In earlier Cisco software releases, only a fixed load distribution algorithm was supported. With this fixed algorithm, the load share bits are assigned sequentially to each port in the bundle. Consequently, the load share bits for existing ports change when a member link joins or leaves the bundle. When these values are programmed in the ASIC, substantial traffic disruption and, in some cases, duplication of traffic can occur.

The EtherChannel Load Distribution feature enhances the load distribution mechanism with the adaptive load distribution algorithm. This algorithm uses a port reassignment scheme that enhances EtherChannel availability by limiting the load distribution reassignment to the port that is added or deleted. The new load on existing bundled ports does not conflict with the load programmed on those ports when a port is added or deleted.

You can enable this feature in either global configuration mode or interface configuration mode. The algorithm is applied at the next hash-distribution instance, which usually occurs when a link fails, is activated, added, or removed, or when shutdown or no shutdown is configured.

Because the selected algorithm is not applied until the next hash-distribution instance, the current and configured algorithms could be different. If the algorithms are different, a message is displayed alerting you to take appropriate action. For example:

```
Device(config-if)# port-channel port hash-distribution fixed
This command will take effect upon a member link UP/DOWN/ADDITION/DELETION event.
Please do a shut/no shut to take immediate effect
```

Also, the output of the **show etherchannel** command is enhanced to show the applied algorithm when the channel group number is specified. This output enhancement is not available, though, when the protocol is also specified because only protocol-specific information is included. Following is an example of output showing the applied algorithm:

```
Device# show etherchannel 10 summary
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      N - not in use, no aggregation
        f - failed to allocate aggregator
<snip>
Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
10     Po10(RU)         LACP      Gi3/7(P)       Gi3/9(P)
! The following line of output is added with support
of the EtherChannel Load Distribution feature. !
Last applied Hash Distribution Algorithm: Fixed
```

How to Configure IEEE 802.3ad Link Bundling and Load Balancing

Enabling LACP

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface port-channel** *channel-number*
4. **exit**
5. **interface type** *number*
6. **channel-group** *channel-group-number* **mode** {**active** | **passive**}
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface port-channel** *channel-number* **Example:** `Device(config)# interface port-channel 10`	Identifies the interface port channel and enters interface configuration mode.
Step 4	**exit** **Example:** `Device(config-if)# exit`	Returns to global config mode.

	Command or Action	Purpose
Step 5	**interface type** *number* **Example:** `Device(config)# interface Gigabitethernet 1/0/5`	Configures an interface and enters interface configuration mode.
Step 6	**channel-group** *channel-group-number* **mode** {**active** | **passive**} **Example:** `Device(config-if)# channel-group 10 mode active`	Configures the interface in a channel group and sets it as active. • In active mode, the port initiates negotiations with other ports by sending Link Aggregate Control Protocol (LACP) packets.
Step 7	**end** **Example:** `Device(config-if)# end`	Returns to privileged EXEC mode.

Configuring a Port Channel

You must manually create a port channel logical interface. Perform this task to configure a port channel.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface port-channel** *channel-number*
4. **no switchport**
5. **ip address** *ip-address mask*
6. **end**
7. **show running-config interface port-channel** *group-number*

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface port-channel** *channel-number* **Example:** `Device(config)# interface port-channel 10`	Identifies the interface port channel and enters interface configuration mode.
Step 4	**no switchport** **Example:** `Device(config-if)# no switchport`	Puts an interface into Layer 3 mode.
Step 5	**ip address** *ip-address mask* **Example:** `Device(config-if)# ip address 172.31.52.10 255.255.255.0`	Assigns an IP address and subnet mask to the EtherChannel.
Step 6	**end** **Example:** `Device(config-if)# end`	Returns to privileged EXEC mode.
Step 7	**show running-config interface port-channel** *group-number* **Example:** `Device# show running-config interface port-channel 10`	Displays the port channel configuration.

Example

This example shows how to verify the configuration:

```
Device# show running-config interface port-channel10

Building configuration...
Current configuration:
!
no switchport
interface Port-channel10
 ip address 172.31.52.10 255.255.255.0
```

```
 no ip directed-broadcast
end
```

Setting LACP System Priority

Perform this task to set the Link Aggregation Control Protocol (LACP) system priority. The system ID is the combination of the LACP system priority and the MAC address of a device.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **lacp system-priority** *priority*
4. **end**
5. **show lacp sys-id**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**lacp system-priority** *priority* **Example:** `Device(config)# lacp system-priority 200`	Sets the system priority.
Step 4	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.
Step 5	**show lacp sys-id** **Example:** `Device# show lacp sys-id`	Displays the system ID, which is a combination of the system priority and the MAC address of the device.

Example

This example shows how to verify the LACP configuration:

```
Device# show lacp sys-id
20369,01b2.05ab.ccd0
```

Adding and Removing Interfaces from a Bundle

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **channel-group** *channel-group-number* **mode** {**active** | **passive**}
5. **no channel-group**
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Device(config)# interface gigabitethernet 5/0/0`	Configures an interface and enters interface configuration mode.
Step 4	**channel-group** *channel-group-number* **mode** {**active** | **passive**} **Example:** `Device(config-if)# channel-group 5 mode active`	Adds an interface to a channel group.

	Command or Action	Purpose
Step 5	**no channel-group** **Example:** `Device(config-if)# no channel-group`	Removes the interface from the channel group.
Step 6	**end** **Example:** `Device(config-if)# end`	Returns to privileged EXEC mode.

Monitoring LACP Status

SUMMARY STEPS

1. **enable**
2. **show lacp** {*number* | **counters** | **internal** | **neighbor** | **sys-id**}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show lacp** {*number*	**counters**	**internal**	**neighbor**	**sys-id**} **Example:** `Device# show lacp internal`	Displays internal device information.

Troubleshooting Tips

To verify and isolate a fault, start at the highest level maintenance domain and do the following:

- Check the device error status.
- When an error exists, perform a loopback test to confirm the error.

- Run a traceroute to the destination to isolate the fault.
- If the fault is identified, correct the fault.
- If the fault is not identified, go to the next lower maintenance domain and repeat these four steps at that maintenance domain level.
- Repeat the first four steps, as needed, to identify and correct the fault.

Configuration Examples for IEEE 802.3ad Link Bundling and Load Balancing

Example: Adding and Removing Interfaces from a Bundle

The following example shows how to add an interface to a bundle:

```
Device# 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 5
                            LACP port     Admin     Oper    Port        Port
Port      Flags   State     Priority      Key       Key     Number      State
Gi7/0/0   SA      bndl      32768         0x5       0x5     0x43        0x3D
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# interface gigabitethernet 5/0/0
Device(config-if)# channel-group 5 mode active
Device(config-if)#
*Aug 20 17:10:19.057: %LINK-3-UPDOWN: Interface GigabitEthernet5/0/0, changed state to down
*Aug 20 17:10:19.469: %C10K_ALARM-6-INFO: ASSERT CRITICAL GigE 5/0/0 Physical Port Link
Down
*Aug 20 17:10:19.473: %C10K_ALARM-6-INFO: CLEAR CRITICAL GigE 5/0/0 Physical Port Link Down

*Aug 20 17:10:21.473: %LINK-3-UPDOWN: Interface GigabitEthernet5/0/0, changed state to up
*Aug 20 17:10:21.473: GigabitEthernet7/0/0 taken out of port-channel5
*Aug 20 17:10:23.413: GigabitEthernet5/0/0 added as member-1 to port-channel5

*Aug 20 17:10:23.473: %LINK-3-UPDOWN: Interface Port-channel5, changed state to up
Device(config-if)# end
Device#
*Aug 20 17:10:27.653: %SYS-5-CONFIG_I: Configured from console by console
*Aug 20 17:11:40.717: GigabitEthernet7/0/0 added as member-2 to port-channel5

Device# 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 5
                            LACP port     Admin     Oper    Port        Port
Port      Flags   State     Priority      Key       Key     Number      State
Gi7/0/0   SA      bndl      32768         0x5       0x5     0x43        0x3D
Gi5/0/0   SA      bndl      32768         0x5       0x5     0x42        0x3D
Device# show interface port-channel5
Port-channel5 is up, line protocol is up
  Hardware is GEChannel, address is 0014.a93d.4aa8 (bia 0000.0000.0000)
  MTU 1500 bytes, BW 2000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
```

```
   No. of active members in this channel: 2
      Member 0 : GigabitEthernet5/0/0 , Full-duplex, 1000Mb/s  <---- added to port channel
 bundle
       Member 1 : GigabitEthernet7/0/0 , Full-duplex, 1000Mb/s
  Last input 00:00:00, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/150/0/0 (size/max/drops/flushes); Total output drops: 0
  Interface Port-channel5 queueing strategy: PXF First-In-First-Out
  Output queue 0/8192, 0 drops; input queue 0/150, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 0 multicast, 0 pause input
     104 packets output, 8544 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 PAUSE output
     0 output buffer failures, 0 output buffers swapped out
```

The following example shows how to remove an interface from a bundle:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# interface gigabitethernet 7/0/0
Device(config-if)# no channel-group
Device(config-if)#
*Aug 20 17:15:49.433: GigabitEthernet7/0/0 taken out of port-channel5
*Aug 20 17:15:49.557: %C10K_ALARM-6-INFO: ASSERT CRITICAL GigE 5/0/0 Physical Port Link
Down
*Aug 20 17:15:50.161: %C10K_ALARM-6-INFO: CLEAR CRITICAL GigE 5/0/0 Physical Port Link Down

*Aug 20 17:15:51.433: %LINK-3-UPDOWN: Interface GigabitEthernet7/0/0, changed state to down
*Aug 20 17:15:52.433: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet7/0/0,
 changed state to down
Device(config-if)# end
Device#
*Aug 20 17:15:58.209: %SYS-5-CONFIG_I: Configured from console by console
Device#
*Aug 20 17:15:59.257: %C10K_ALARM-6-INFO: ASSERT CRITICAL GigE 7/0/0 Physical Port Link
Down
*Aug 20 17:15:59.257: %C10K_ALARM-6-INFO: CLEAR CRITICAL GigE 7/0/0 Physical Port Link Down

Device#
*Aug 20 17:16:01.257: %LINK-3-UPDOWN: Interface GigabitEthernet7/0/0, changed state to up
*Aug 20 17:16:02.257: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet7/0/0,
 changed state to up
Device# 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 5
                            LACP port     Admin     Oper    Port        Port
Port      Flags   State     Priority      Key       Key     Number      State
Gi5/0/0   SA      bndl      32768         0x5       0x5     0x42        0x3D
```

Example: Monitoring LACP Status

The following example shows Link Aggregation Protocol (LACP) activity that you can monitor by using the **show lacp** command.

```
Device# 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 5
```

```
                           LACP port     Admin     Oper    Port        Port
Port      Flags   State    Priority      Key       Key     Number      State
Gi5/0/0   SA      bndl     32768         0x5       0x5     0x42        0x3D
Device# show lacp 5 counters
             LACPDUs          Marker      Marker Response    LACPDUs
Port       Sent   Recv     Sent   Recv     Sent   Recv      Pkts Err
---------------------------------------------------------------------
Channel group: 5
Gi5/0/0     21     18       0      0        0      0         0
Device# show lacp 5 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 5
                           LACP port     Admin     Oper    Port        Port
Port      Flags   State    Priority      Key       Key     Number      State
Gi5/0/0   SA      bndl     32768         0x5       0x5     0x42        0x3D
Device# show lacp 5 neighbor
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 5 neighbors
Partner's information:
         Partner Partner   LACP Partner  Partner   Partner  Partner     Partner
Port     Flags   State     Port Priority Admin Key Oper Key Port Number Port State
Gi5/0/0  SP      32768     0011.2026.7300  11s    0x1     0x14     0x3C
Device# show lacp counters
             LACPDUs          Marker      Marker Response    LACPDUs
Port       Sent   Recv     Sent   Recv     Sent   Recv      Pkts Err
---------------------------------------------------------------------
Channel group: 5
Gi5/0/0     23     20       0      0        0      0         0
Device# show lacp sys-id
32768,0014.a93d.4a00
```

Additional References for IEEE 802.3ad Link Bundling and Load Balancing

Related Documents

Related Topic	Document Title
Configuring EtherChannels	"Configuring Layer 3 and Layer 2 EtherChannel" chapter of the *Catalyst 6500 Release 12.2SXF Software Configuration Guide*
Configuring the Cisco Catalyst 3850 Series Switch	*Catalyst 3850 Series Switch Configuration Guide*
Configuring Carrier Ethernet	*Carrier Ethernet Configuration Guide*
Link Aggregation Control Protocol (LACP) commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	*Cisco IOS Carrier Ethernet Command Reference*

Related Topic	Document Title
Cisco IOS commands: master list of commands with complete command syntax, command mode, command history, defaults, usage guidelines, and examples	Cisco IOS Master Command List, All Releases

Standards

Standard	Title
IEEE 802.3ad-2000	*IEEE 802.3ad-2000 Link Aggregation*

MIBs

MIB	MIBs Link
802.3ad MIB	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

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

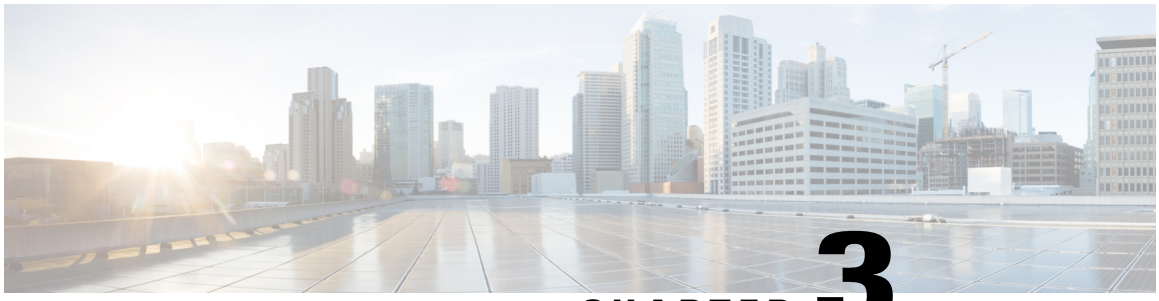
Feature Information for Configuring IEEE 802.3ad Link Bundling and Load Balancing

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 . An account on Cisco.com is not required.

Table 2: Feature Information for Configuring IEEE 802.3ad Link Bundling and Load Balancing

Feature Name	Releases	Feature Information
IEEE 802.3ad Link Bundling and Load Balancing	Cisco IOS XE 3.2SE	IEEE 802.3ad link bundling and load balancing leverages the EtherChannel infrastructure within Cisco software to manage the bundling of various links. The network traffic load-balancing features help minimize network disruption that results when a port is added or deleted from a link bundle. In Cisco IOS XE Release 3.2SE, this feature is supported on the following platforms: • Cisco 5700 Series Wireless LAN Controllers • Cisco Catalyst 3850 Series Switches In Cisco IOS XE Release 3.3SE, this feature is supported on the following platforms: • Cisco Catalyst 3650 Series Switches



CHAPTER 3

IEEE 802.1ad Support on Provider Bridges

First Published: April 19, 2010

Last Updated: May 26, 2011

Service provider bridges (also called provider bridges) allow devices in a service provider network to transparently carry the Layer 2 control frames of a customer. Spanning Tree Protocol (STP) bridge protocol data units (BPDUs) or Cisco Discovery Protocol frames are carried separately from the service provider traffic and from other customer traffic in the network of a service provider.

User network interface (UNI) ports of a provider bridge interface with customer devices have a specific set of requirements defined by the IEEE 802.1ad standard. These requirements enable provider bridges to have the same functionality as Layer 2 protocol tunneling and Q-in-Q (QnQ) bridges.

This document describes the IEEE 802.1ad implementation on Cisco devices using Layer 2 switch ports.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and 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.

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 IEEE 802.1ad Support on Provider Bridges

- The IEEE 802.1ad Support on Provider Bridges feature is not supported on the Cisco ME3400 series switch.
- In Cisco IOS Release 12.2(54)SE, the Cisco ME 3400E and Catalyst 3750 Metro switch platforms support this feature. The Cisco ME3400 switch platform does not support this feature.

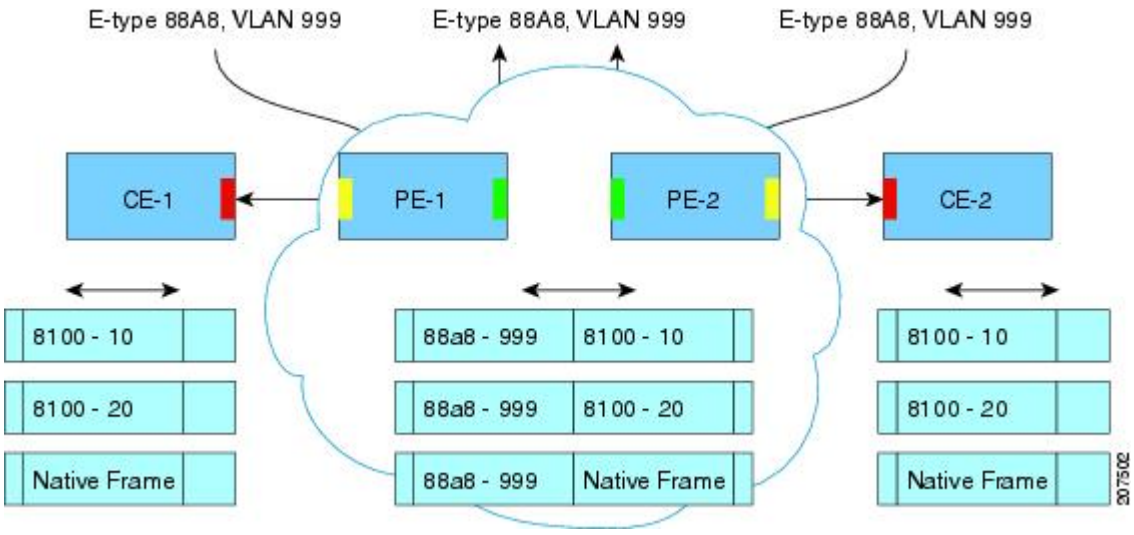
Information About IEEE 802.1ad Support on Provider Bridges

Service Provider Bridges

Provider bridges pass the network traffic of multiple customers. The traffic flow of each customer must be isolated from one another. For Layer 2 protocols within customer domains to function properly, geographically separated customer sites must appear to be connected via a LAN and the provider network must be transparent.

The IEEE has reserved 33 Layer 2 MAC addresses for customer devices that operate Layer 2 protocols. If a provider bridge uses these standard MAC addresses for its Layer 2 protocols, the Layer 2 traffic of the customer devices and the service provider is mixed together. Provider bridges solve this traffic-mixing issue by providing Layer 2 protocol data unit (PDU) tunneling when a provider bridge (S-bridge) component and a provider edge bridge (C-bridge) component are used. The figure below shows the topology.

Figure 1: Layer 2 PDU Tunneling



S-Bridge Component

The S-bridge component is capable of inserting or removing a service provider VLAN (S-VLAN) for all traffic on a particular port. IEEE 802.1ad adds a new tag called a Service tag (S-tag) to all ingress frames traveling from the customer to the service provider.

The VLAN in the S-tag is used for forwarding the traffic in the service provider network. Different customers use different S-VLANs, which results in isolation of traffic of each customer. In the S-tag, provider bridges do not understand the standard Ethertype. Hence, they use an Ethertype value that is different from the standard 802.1Q Ethertype value. This difference makes customer traffic that is tagged with the standard Ethertype appear as untagged in the provider network. The customer traffic is tunneled in the port VLAN of the provider port. 802.1ad service provider user network interfaces (S-UNIs) and network-network interfaces (NNIs) implement the S-bridge component.

For example, a VLAN tag has a VLAN ID of 1, the C-tag Ethertype has a value of 8100 0001, the S-tag Ethertype has a value of 88A8 0001, and the class of service (CoS) has a value of zero.

C-tag S-tag

--- ---

0x8100 | Priority bits | CFI | C-VLAN-ID 0x88A8 | Priority bits | 0 | S-VLAN-ID

--- ---

C-Bridge Component

All customer VLANs (C-VLANs) that enter a user network interface (UNI) port in an S-bridge component receive the same service (marked with the same S-VLAN). C-VLAN components are not supported, but a customer may want to tag a particular C-VLAN packet separately to differentiate between services. Provider bridges allow C-VLAN packet tagging with a provider edge bridge, called the C-bridge component of the provider bridge. C-bridge components are C-VLAN aware and can insert or remove a C-VLAN 802.1Q tag. The C-bridge UNI port is capable of identifying the customer 802.1Q tag and inserting or removing an S-tag on the packet on a per-service instance or C-VLAN basis. A C-VLAN tagged service instance allows service instance selection and identification by C-VLAN. The 801.1ad customer user network interfaces (C-UNIs) implement the C-component.

MAC Addresses for Layer 2 Protocols

Layer 2 protocol data units (PDUs) of customers that are received by a provider bridge are not forwarded. Hence, Layer 2 protocols running at customer sites do not know the complete network topology. By using different set of addresses for the Layer 2 protocols running on provider bridges, IEEE 802.1ad causes Layer 2 PDUs of the customers device that enter the provider bridge to appear as unknown multicast traffic and forwards it on customer ports (on the same service provider VLAN (S-VLAN)). Layer 2 protocols of customer device can then run transparently.

The table below shows Layer 2 MAC addresses that are reserved for the C-VLAN component.

Table 3: Reserved Layer 2 MAC Addresses for the C-VLAN Component

Assignment	Value
Bridge Group Address	01-80-C2-00-00-00
IEEE 802.3 Full Duplex PAUSE Operation	01-80-C2-00-00-01
IEEE 802.3 Slow_Protocols_Multicast_Address	01-80-C2-00-00-02
IEEE 802.1X PAE Address	01-80-C2-00-00-03

Assignment	Value
Provider Bridge Group Address	01-80-C2-00-00-08
Provider Bridge GVRP Address	01-80-C2-00-00-0D
IEEE 802.1AB Link Layer Discovery Protocol Multicast Address	01-80-C2-00-00-0E
Reserved for future standardization	01-80-C2-00-00-04 01-80-C2-00-00-05 01-80-C2-00-00-06 01-80-C2-00-00-07 01-80-C2-00-00-09 01-80-C2-00-00-0A 01-80-C2-00-00-0B 01-80-C2-00-00-0C 01-80-C2-00-00-0F

The table below shows Layer 2 MAC addresses that are reserved for the S-VLAN component. These addresses are a subset of the C-VLAN component addresses, and the C-bridge does not forward the bridge protocol data units (BPDUs) of a provider to a customer network.

Table 4: Reserved Layer 2 MAC Addresses for the S-VLAN Component

Assignment	Value
IEEE 802.3 Full Duplex PAUSE Operation	01-80-C2-00-00-01
IEEE 802.3 Slow_Protocols_Multicast_Address	01-80-C2-00-00-02
IEEE 802.1X PAE Address	01-80-C2-00-00-03
Provider Bridge Group Address	01-80-C2-00-00-08
Reserved for future standardization	01-80-C2-00-00-04 01-80-C2-00-00-05 01-80-C2-00-00-06 01-80-C2-00-00-07 01-80-C2-00-00-09 01-80-C2-00-00-0A

Overview of IEEE 802.1ad Support on Provider Bridges

The IEEE 802.1ad Support on Provider Bridges feature is implemented on switch ports and supports the following IEEE 802.1ad specified functions:

- Operation of individual provider bridges
- Configuration and management of individual provider bridges
- Management of spanning tree and VLAN topologies within a provider network

Layer 2 PDU Destination MAC Addresses for Customer-Facing C-Bridge UNI Ports

The table below shows the Layer 2 protocol data unit (PDU) destination MAC addresses for customer-facing C-bridge user network interface (UNI) ports and how the frames are processed.

Table 5: Layer 2 PDU Destination MAC Addresses for Customer-Facing C-Bridge UNI Ports

MAC Address	Protocol	Significance on the C-Bridge UNI Port	Default Action
01-80-C2-00-00-00	Bridge Group Address (end-to-end BPDUs)	Data, BPDU (based on the CLI configuration of the **l2protocol** command)	BPDU
01-80-C2-00-00-01	802.3X Pause Protocol	BPDU	MAC address processes
01-80-C2-00-00-02	Slow protocol address: 802.3ad LACP, 802.3ah OAM, Cisco Discovery Protocol, DTP, PagP, UDLD, VTP	BPDU	BPDU
01-80-C2-00-00-03	802.1x	BPDU	BPDU
01-80-C2-00-00-04	Reserved for future media access method	Drop	Drop
01-80-C2-00-00-05	Reserved for future media access method	Drop	Drop
01-80-C2-00-00-06	Reserved for future bridge use	Drop	Drop
01-80-C2-00-00-07	Ethernet Local Management Interface	BPDU	BPDU
01-80-C2-00-00-08	Provider STP (BPDU)	Drop	Drop

MAC Address	Protocol	Significance on the C-Bridge UNI Port	Default Action
01-80-C2-00-00-09	Reserved for future bridge use	Drop	Drop
01-80-C2-00-00-0A	Reserved for future bridge use	Drop	Drop
01-80-C2-00-00-0B	Reserved for future S-bridge purposes	Drop	Drop
01-80-C2-00-00-0C	Reserved for future S-bridge purposes	Drop	Drop
01-80-C2-00-00-0D	Provider bridge GVRP address	Drop	Drop
01-80-C2-00-00-0E	802.1ab LLDP	Data, BPDU (based on the CLI configuration of the **l2protocol** command)	BPDU
01-80-C2-00-00-0F	Reserved for future C-bridge or Q-bridge use	Drop	Drop
01-80-C2-00-00-10	All bridges address	BPDU	Peer
01-80-C2-00-00-20	GMRP	Data	Data
01-80-C2-00-00-21	GVRP	Data	Data
01-80-C2-00-00-22-2F	Other GARP addresses	Data	Data
01-00-0C-CC-CC-CC	Cisco Discovery Protocol, DTP, PagP, UDLD, VTP (end-to-end)	Data, BPDU (based on the CLI configuration of the **l2protocol** command)	BPDU
01-00-0C-CC-CC-CD	PVST (end-to-end)	Data, BPDU (based on the CLI configuration of the **l2protocol** command)	BPDU

Layer 2 PDU Destination MAC Addresses for Customer-Facing S-Bridge UNI Ports

If a port is operating as a customer-facing S-bridge user network interface (UNI), the destination MAC addresses shown in the below table are used for defining the Layer 2 protocol protocol data unit (PDU) processing at the S-bridge UNI.

Table 6: Layer 2 PDU Destination MAC Addresses for Customer-Facing S-Bridge UNI Ports

MAC Address	Protocol	Significance on the S-Bridge UNI Port	Default Action
01-80-C2-00-00-00	Bridge Protocol Data Units (BPDUs)	Data, BPDU (based on the CLI configuration of the **l2protocol** command)	Data
01-80-C2-00-00-01	802.3X Pause Protocol	BPDU	MAC address processes
01-80-C2-00-00-02	Slow protocol address: 802.3ad LACP, 802.3ah OAM	BPDU	BPDU
01-80-C2-00-00-03	802.1x	BPDU	BPDU
01-80-C2-00-00-04	Reserved for future media access method	Drop	Drop
01-80-C2-00-00-05	Reserved for future media access method	Drop	Drop
01-80-C2-00-00-06	Reserved for future bridge use	Drop	Drop
01-80-C2-00-00-07	Ethernet Local Management Interface	BPDU	BPDU (drop on NNI)
01-80-C2-00-00-08	Provider STP (BPDU)	BPDU	BPDU
01-80-C2-00-00-09	Reserved for future bridge use	Drop	Drop
01-80-C2-00-00-0A	Reserved for future bridge use	Drop	Drop
01-80-C2-00-00-0B	Reserved for future S-bridge use	Data	Data
01-80-C2-00-00-0C	Reserved for future S-bridge use	Data	Data
01-80-C2-00-00-0D	Provider bridge Generic VLAN Registration Protocol (GVRP) address	Data	Data
01-80-C2-00-00-0E	802.1ab Link Layer Discovery Protocol (LLDP)	Data, BPDU (based on the CLI configuration of the **l2protocol** command)	Data

MAC Address	Protocol	Significance on the S-Bridge UNI Port	Default Action
01-80-C2-00-00-0F	Reserved for future C-bridge or Q-bridge use	Data	Data
01-80-C2-00-00-10	All bridges address	Data	Data
01-80-C2-00-00-20	GARP Multicast Registration Protocol (GMRP)	Data	Data
01-80-C2-00-00-21	Generic VLAN Registration Protocol (GVRP)	Data	Data
01-80-C2-00-00-22-2F	Other Generic Attribute Registration Protocol (GARP) addresses	Data	Data
01-00-0C-CC-CC-CC	Cisco Discovery Protocol, Dynamic Trunking Protocol (DTP), Port Aggregation Protocol (PagP), UniDirectional Link Detection (UDLD), and VLAN Trunk Protocol (VTP)	Data, BPDU (based on the CLI configuration of the **l2protocol** command)	Data
01-00-0C-CC-CC-CD	Per-VLAN Spanning Tree (PVST)	Data, BPDU (based on the CLI configuration of the **l2protocol** command)	Data

How to Configure IEEE 802.1ad Support on Provider Bridges

Configuring a Switch Port to Process 802.1ad BPDUs

In an 802.1ad network, the default behavior for Layer 2 protocol data units (PDUs) on an interface depends on the 802.1ad interface type. If the interface type is an S-bridge user network interface (UNI), all Layer 2 PDUs are tunneled. If the interface type is a C-bridge UNI, all Layer 2 PDUs are processed (peered).

PDU processing on the S-bridge UNI is the same as on an 802.1ad network-network interface (NNI). Both types of interfaces have the same scope of MAC addresses. Perform the tasks in this section to configure switch port-to-peer (process) BPDUs:

Configuring a Switch Port to Process BPDUs

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **switchport mode** {**access** | **trunk**}
5. **ethernet dot1ad** {**nni** | **uni** {**c-port** | **s-port**}}
6. **l2protocol peer** [*protocol*]
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Device(config)# interface gigabitethernet 0/3`	Configures the interface and enters interface configuration mode.
Step 4	**switchport mode** {**access**	**trunk**} **Example:** `Device(config-if)# switchport mode trunk`	Sets the interface type.
Step 5	**ethernet dot1ad** {**nni**	**uni** {**c-port**	**s-port**}} **Example:** `Device(config-if)# ethernet dot1ad uni c-port`	Configures a dot1ad network-network interface (NNI) or user network interface (UNI) port.
Step 6	**l2protocol peer** [*protocol*] **Example:** `Device(config-if)# l2protocol peer vtp`	Processes or forwards Layer 2 bridge protocol data units (BPDUs). • In this example, only VLAN Trunk Protocol (VTP) BPDUs are processed.

	Command or Action	Purpose
Step 7	**end** **Example:** `Device(config-if)# end`	Returns to privileged EXEC mode.

Configuration Examples for IEEE 802.1ad Support on Provider Bridges

Example: Configuring an 802.1ad S-Bridge UNI

The following example shows how to configure GigabitEthernet interface 0/2 of a provider edge (PE) as an 802.1ad S-bridge user network interface (UNI). In this example, only Cisco Discovery Protocol protocol data units (PDUs) will be forwarded (tunneled). Cisco Discovery Protocol PDUs are forwarded between the PE and a customer device.

```
Device# configure terminal
Device(config)# interface GigabitEthernet 0/2
Device(config-if)# switchport access vlan 500
Device(config-if)# ethernet dot1ad uni s-port
Device(config-if)# l2protocol forward cdp
Device(config-if)# end
```

Example: Configuring an 802.1ad C-Bridge UNI

The following example shows how to configure interface GigabitEthernet 0/3 of a PE as an 802.1ad C-bridge user network interface (UNI). In this example, only Cisco Discovery Protocol protocol data units (PDUs) are processed.

```
Device# configure terminal
Device(config)# interface GigabitEthernet 0/3
Device(config-if)# switchport mode trunk
Device(config-if)# ethernet dot1ad uni c-port
Device(config-if)# l2protocol peer cdp
Device(config-if)# end
```

Additional References for IEEE 802.1ad Support on Provider Bridges

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
Cisco IOS Carrier Ethernet commands	Cisco IOS Carrier Ethernet Command Reference

Standards and RFCs

Standard	Title
IEEE 802.1ad	*Provider Bridges*

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 IEEE 802.1ad Support on Provider Bridges

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 . An account on Cisco.com is not required.

Table 7: Feature Information for IEEE 802.1ad Support on Provider Bridges.

Feature Name	Releases	Feature Information
IEEE 802.1ad Support on Provider Bridges	Cisco IOS XE Release 3.6E	The IEEE 802.1ad Support on Provider Bridges feature is the IEEE 802.1ad implementation on Cisco devices using Layer 2 switch ports. In Cisco IOS XE Release 3.6E, this feature is supported on Cisco Catalyst 3850 Series Switches. The following commands were introduced or modified: **ethernet dot1ad**, **l2protocol**, and **show ethernet dot1ad**.

Glossary

DTP—Dynamic Trunking Protocol.

GARP—Generic Attribute Registration Protocol.

GMRP—GARP Multicast Registration Protocol.

GVRP—Generic VLAN Registration Protocol.

LLDP—Link Layer Discovery Protocol.

OAM—Operations, Administration, and Maintenance.

PagP—Port Aggregation Protocol.

PVST—Per-VLAN Spanning Tree.

UDLD—UniDirectional Link Detection.

VTP—VLAN Trunk Protocol.