Contents

Configuring LLDP

About LLDP

The Link Layer Discovery Protocol (LLDP) is a standard link layer protocol that allows network devices from different vendors to discover neighbors and exchange system and configuration information.

In an LLDP-enabled network, a device advertises local device information in LLDP Data Units (LLDPDUs) to the directly connected devices. The information distributed through LLDP is stored by its recipients in standard MIBs, making it possible for the information to be accessed by a Network Management System (NMS) through SNMP.

Information that can be distributed through LLDP includes (but is not limited to):

- Major capabilities of the system.
- Management IP address of the system.
- Device ID.
- Port ID.

LLDP agents and bridge modes

An LLDP agent is a mapping of a protocol entity that implements LLDP. Multiple LLDP agents can run on the same interface.

LLDP agents are classified into the following types:

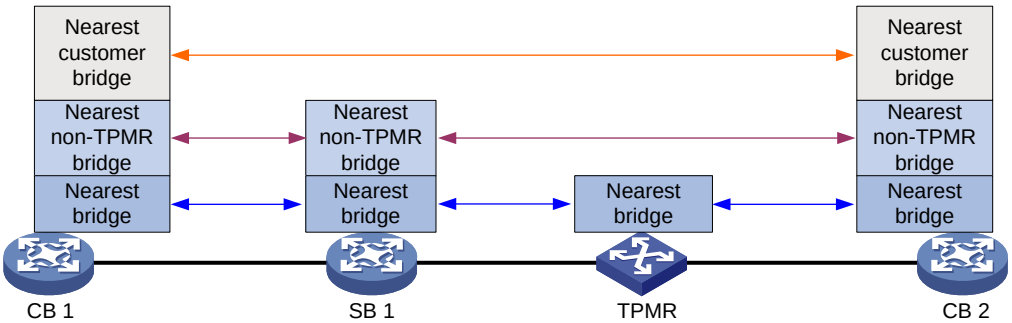
- Nearest bridge agent.
- Nearest customer bridge agent.
- Nearest non-TPMR bridge agent.

  A Two-port MAC Relay (TPMR) is a type of bridge that has only two externally-accessible bridge ports. It supports a subset of the features of a MAC bridge. A TPMR is transparent to all frame-based media-independent protocols except for the following protocols:

  - Protocols destined for the TPMR.
  - Protocols destined for reserved MAC addresses that the relay feature of the TPMR is configured not to forward.

LLDP exchanges packets between neighbor agents and creates and maintains neighbor information for them. Figure 1 shows the neighbor relationships for these LLDP agents.

Figure 1 LLDP neighbor relationships



The types of supported LLDP agents vary with the bridge mode in which LLDP operates. LLDP supports the following bridge modes: customer bridge (CB) and service bridge (SB).

- **Customer bridge mode**—LLDP supports nearest bridge agent, nearest non-TPMR bridge agent, and nearest customer bridge agent. LLDP processes the LLDP frames with destination MAC addresses for these agents and transparently transmits the LLDP frames with other destination MAC addresses in VLANs.
- **Service bridge mode**—LLDP supports nearest bridge agent and nearest non-TPMR bridge agent. LLDP processes the LLDP frames with destination MAC addresses for these agents and transparently transmits the LLDP frames with other destination MAC addresses in VLANs.

LLDP frame formats

LLDP sends device information in LLDP frames. LLDP frames are encapsulated in Ethernet II or Subnetwork Access Protocol (SNAP) format.

LLDP frame encapsulated in Ethernet II

Figure 2 Ethernet II-encapsulated LLDP frame

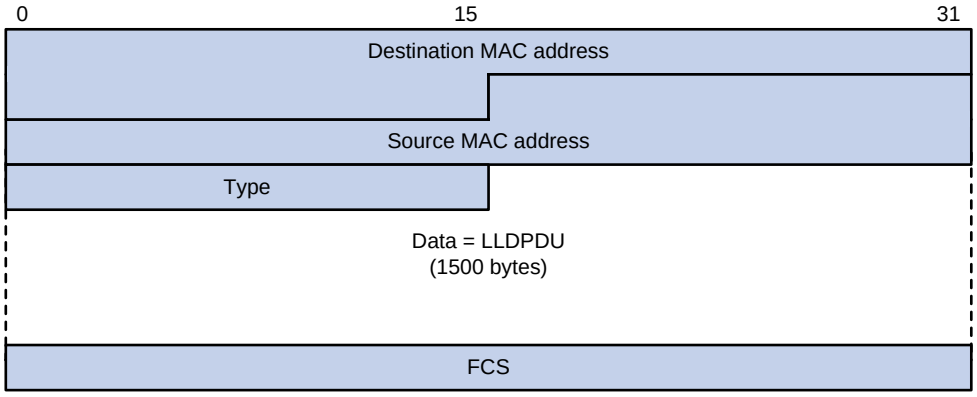


Table 1 Fields in an Ethernet II-encapsulated LLDP frame

Field	Description
Destination MAC address	MAC address to which the LLDP frame is advertised. LLDP specifies different multicast MAC addresses as destination MAC addresses for LLDP frames destined for agents of different types. This helps distinguish between LLDP frames sent and received by different agent types on the same interface. The destination MAC address is fixed to one of the following multicast MAC addresses: • 0x0180-c200-000E for LLDP frames destined for nearest bridge agents. • 0x0180-c200-0000 for LLDP frames destined for nearest customer bridge agents. • 0x0180-c200-0003 for LLDP frames destined for nearest non-TPMR bridge agents.
Source MAC address	MAC address of the sending port.
Type	Ethernet type for the upper-layer protocol. This field is 0x88CC for LLDP.
Data	LLDPDU.
FCS	Frame check sequence, a 32-bit CRC value used to determine the validity of the received Ethernet frame.

LLDP frame encapsulated in SNAP

Figure 3 SNAP-encapsulated LLDP frame

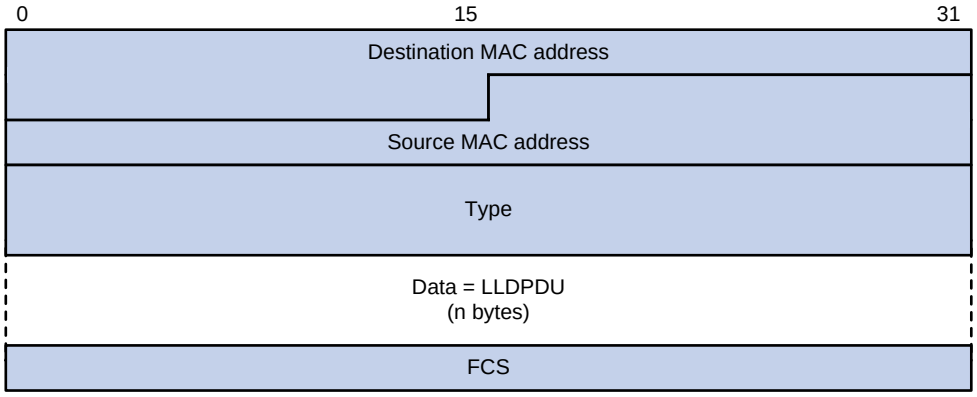


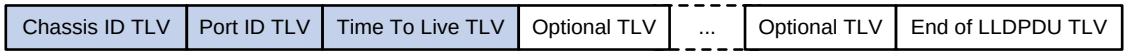
Table 2 Fields in a SNAP-encapsulated LLDP frame

Field	Description
Destination MAC address	MAC address to which the LLDP frame is advertised. It is the same as that for Ethernet II-encapsulated LLDP frames.
Source MAC address	MAC address of the sending port.
Type	SNAP type for the upper-layer protocol. This field is 0xAAAA-0300-0000-88CC for LLDP.
Data	LLDPDU.
FCS	Frame check sequence, a 32-bit CRC value used to determine the validity of the received Ethernet frame.

LLDPDUs

Each LLDP frame contains one LLDPDU. Each LLDPDU is a sequence of type-length-value (TLV) structures.

Figure 4 LLDPDU encapsulation format



As shown in Figure 4, each LLDPDU starts with the following mandatory TLVs: Chassis ID TLV, Port ID TLV, and Time to Live TLV. The mandatory TLVs are followed by a maxiumu of 29 optional TLVs.

TLVs

A TLV is an information element that contains the type, length, and value fields.

LLDPDU TLVs include the following categories:

- Basic management TLVs.
- Organizationally (IEEE 802.1 and IEEE 802.3) specific TLVs.
- LLDP-MED (media endpoint discovery) TLVs.

Basic management TLVs are essential to device management.

Organizationally specific TLVs and LLDP-MED TLVs are used for enhanced device management. They are defined by standardization or other organizations and are optional for LLDPDUs.

Basic management TLVs

Table 3 lists the basic management TLV types. Some of them are mandatory for LLDPDUs.

Table 3 Basic management TLVs

Type	Description	Remarks
Chassis ID	Specifies the bridge MAC address of the sending device.	Mandatory.
Port ID	Specifies the ID of the sending port: • If the LLDPDU carries LLDP-MED TLVs, the port ID TLV carries the MAC address of the sending port. • Otherwise, the port ID TLV carries the port name.	
Time to Live	Specifies the life of the transmitted information on the receiving device.	
End of LLDPDU	Marks the end of the TLV sequence in the LLDPDU.	Optional.
Port Description	Specifies the description for the sending port.	
System Name	Specifies the assigned name of the sending device.	
System Description	Specifies the description for the sending device.	
System Capabilities	Identifies the primary features of the sending device and the enabled primary features.	
Management Address	Specifies the following elements: • The management address of the local device. • The interface number and object identifier (OID) associated with the address.	

IEEE 802.1 organizationally specific TLVs

Table 4 lists the IEEE 802.1 organizationally specific TLVs.

The device can receive protocol identity TLVs and VID usage digest TLVs, but it cannot send these TLVs.

Layer 3 Ethernet ports support only link aggregation TLVs.

Table 4 IEEE 802.1 organizationally specific TLVs

Type	Description
Port VLAN ID (PVID)	Specifies the port VLAN identifier.
Port And Protocol VLAN ID (PPVID)	Indicates whether the device supports protocol VLANs and, if so, what VLAN IDs these protocols will be associated with.
VLAN Name	Specifies the textual name of any VLAN to which the port belongs.
Protocol Identity	Indicates protocols supported on the port.
DCBX	Data center bridging exchange protocol.
EVB module	Edge Virtual Bridging module, including EVB TLV and CDCP TLV. For more information, see *EVB Configuration Guide*.
Link Aggregation	Indicates whether the port supports link aggregation, and if yes, whether link aggregation is enabled.

Type	Description
Management VID	Management VLAN ID.
VID Usage Digest	VLAN ID usage digest.
ETS Configuration	Enhanced Transmission Selection configuration.
ETS Recommendation	ETS recommendation.
PFC	Priority-based Flow Control.
APP	Application protocol.
QCN	Quantized Congestion Notification.

IEEE 802.3 organizationally specific TLVs

Table 5 shows the IEEE 802.3 organizationally specific TLVs.

The Power Stateful Control TLV is defined in IEEE P802.3at D1.0 and is not supported in later versions. The device sends this type of TLVs only after receiving them.

Table 5 IEEE 802.3 organizationally specific TLVs

Type	Description
MAC/PHY Configuration/Status	Contains the bit-rate and duplex capabilities of the port, support for autonegotiation, enabling status of autonegotiation, and the current rate and duplex mode.
Link Aggregation	Indicates whether the port supports link aggregation, and if yes, whether link aggregation is enabled.
Power Via MDI	Contains the power supply capabilities of the port: • Port class (PSE or PD). • Power supply mode. • Whether PSE power supply is supported. • Whether PSE power supply is enabled. • Whether pair selection can be controlled. • Power supply type. • Power source. • Power priority. • PD requested power. • PSE allocated power.
Maximum Frame Size	Indicates the supported maximum frame size.
Power Stateful Control	Indicates the power state control configured on the sending port, including the following: • Power supply mode of the PSE/PD. • PSE/PD priority. • PSE/PD power.
Energy-Efficient Ethernet	Indicates Energy Efficient Ethernet (EEE).

LLDP-MED TLVs

LLDP-MED TLVs provide multiple advanced applications for voice over IP (VoIP), such as basic configuration, network policy configuration, and address and directory management. LLDP-MED TLVs provide a cost-effective and easy-to-use solution for deploying voice devices in Ethernet. LLDP-MED TLVs are shown in Table 6.

If the MAC/PHY configuration/status TLV is not advertisable, none of the LLDP-MED TLVs will be advertised even if they are advertisable.

If the LLDP-MED capabilities TLV is not advertisable, the other LLDP-MED TLVs will not be advertised even if they are advertisable.

Table 6 LLDP-MED TLVs

Type	Description
LLDP-MED Capabilities	Allows a network device to advertise the LLDP-MED TLVs that it supports.
Network Policy	Allows a network device or terminal device to advertise the VLAN ID of a port, the VLAN type, and the Layer 2 and Layer 3 priorities for specific applications.
Extended Power-via-MDI	Allows a network device or terminal device to advertise power supply capability. This TLV is an extension of the Power Via MDI TLV.
Hardware Revision	Allows a terminal device to advertise its hardware version.
Firmware Revision	Allows a terminal device to advertise its firmware version.
Software Revision	Allows a terminal device to advertise its software version.
Serial Number	Allows a terminal device to advertise its serial number.
Manufacturer Name	Allows a terminal device to advertise its vendor name.
Model Name	Allows a terminal device to advertise its model name.
Asset ID	Allows a terminal device to advertise its asset ID. The typical case is that the user specifies the asset ID for the endpoint to facilitate directory management and asset tracking.
Location Identification	Allows a network device to advertise the appropriate location identifier information for a terminal device to use in the context of location-based applications.

Management address

The network management system uses the management address of a device to identify and manage the device for topology maintenance and network management. The management address is encapsulated in the management address TLV.

LLDP operating modes

An LLDP agent can operate in one of the following modes:

- **TxRx mode**—An LLDP agent in this mode can send and receive LLDP frames.
- **Tx mode**—An LLDP agent in this mode can only send LLDP frames.
- **Rx mode**—An LLDP agent in this mode can only receive LLDP frames.
- **Disable mode**—An LLDP agent in this mode cannot send or receive LLDP frames.

Each time the operating mode of an LLDP agent changes, its LLDP protocol state machine reinitializes. A configurable reinitialization delay prevents frequent initializations caused by frequent changes to the operating mode. If you configure the reinitialization delay, an LLDP agent must wait the specified amount of time to initialize LLDP after the LLDP operating mode changes.

Transmitting and receiving LLDP frames

Transmitting LLDP frames

An LLDP agent operating in TxRx mode or Tx mode sends LLDP frames to its directly connected devices both periodically and when the local configuration changes. To prevent LLDP frames from overwhelming the network during times of frequent changes to local device information, LLDP uses the token bucket mechanism to rate limit LLDP frames. For more information about the token bucket mechanism, see *ACL and QoS Configuration Guide*.

LLDP automatically enables the fast LLDP frame transmission mechanism in either of the following cases:

- A new LLDP frame is received and carries device information new to the local device.
- The LLDP operating mode of the LLDP agent changes from Disable or Rx to TxRx or Tx.

The fast LLDP frame transmission mechanism successively sends the specified number of LLDP frames at a configurable fast LLDP frame transmission interval. The mechanism helps LLDP neighbors discover the local device as soon as possible. Then, the normal LLDP frame transmission interval resumes.

Receiving LLDP frames

An LLDP agent operating in TxRx mode or Rx mode confirms the validity of TLVs carried in every received LLDP frame. If the TLVs are valid, the LLDP agent saves the information and starts an aging timer. The initial value of the aging timer is equal to the TTL value in the Time To Live TLV carried in the LLDP frame. When the LLDP agent receives a new LLDP frame, the aging timer restarts. When the aging timer decreases to zero, all saved information ages out.

Collaboration with Track

You can configure a track entry and associate it with an LLDP interface. The LLDP module checks the neighbor availability of the LLDP interface and reports the check result to the Track module. The Track module changes the track entry status accordingly so the associated application module can take correct actions.

The Track module changes the track entry status based on the neighbor availability of a monitored LLDP interface as follows:

- If the neighbor of the LLDP interface is available, the Track module sets the track entry to Positive state.
- If the neighbor of the LLDP interface is unavailable, the Track module sets the track entry to Negative state.

For more information about collaboration between Track and LLDP, see the track configuration in *High Availability Configuration Guide.*

Protocols and standards

- IEEE 802.1AB-2005, *Station and Media Access Control Connectivity Discovery*
- IEEE 802.1AB-2009, *Station and Media Access Control Connectivity Discovery*
- ANSI/TIA-1057, *Link Layer Discovery Protocol for Media Endpoint Devices*
- IEEE Std 802.1Qaz-2011, *Media Access Control (MAC) Bridges and Virtual Bridged Local Area Networks-Amendment 18: Enhanced Transmission Selection for Bandwidth Sharing Between Traffic Classes*

Restrictions and guidelines: LLDP configuration

When you configure LLDP, follow these restrictions and guidelines:

- Some of the LLDP configuration tasks are available in different interface views (see Table 7).

  Table 7 Support of LLDP configuration tasks in different views

Tasks	Supported views
Enabling LLDP	Layer 2 Ethernet interface view Layer 3 Ethernet interface view Management Ethernet interface view Layer 2 aggregate interface view Layer 3 aggregate interface view IRF physical interface view
Setting the LLDP operating mode	
Configuring the advertisable TLVs	
Configuring advertisement of the management address TLV	
Setting the encapsulation format for LLDP frames	
Enabling LLDP polling	
Configuring LLDP trapping and LLDP-MED trapping	

- To use LLDP together with OpenFlow, you must enable LLDP globally on OpenFlow switches. To prevent LLDP from affecting topology discovery of OpenFlow controllers, disable LLDP on ports of OpenFlow instances. For more information about OpenFlow, see *OpenFlow Configuration Guide*.
- You can configure LLDP on an IRF physical interface to monitor the connection and link status of the IRF physical link. An LLDP-enabled IRF physical interface supports only the nearest bridge agent.

LLDP tasks at a glance

To configure LLDP, perform the following tasks:

1. Enabling LLDP
2. Setting the LLDP bridge mode
3. Setting the LLDP operating mode
4. (Optional.) Setting the LLDP reinitialization delay
5. (Optional.) Configuring LLDP packet-related settings
   - Configuring the advertisable TLVs
   - Configuring advertisement of the management address TLV
   - Setting the encapsulation format for LLDP frames
   - Setting LLDP frame transmission parameters
   - Setting the timeout for receiving LLDP frames
6. (Optional.) Enabling LLDP polling
7. (Optional.) Disabling LLDP PVID inconsistency check
8. (Optional.) Configuring CDP compatibility
9. (Optional.) Configuring LLDP trapping and LLDP-MED trapping
10. (Optional.) Configuring LLDP neighbor validation and aging
    - Configuring LLDP neighbor validation on an interface
    - Configuring LLDP neighbor aging on an interface

11. (Optional.) Configuring MAC address learning for DCN
    - (Optional.) Setting the source MAC address of LLDP frames
    - (Optional.) Enabling generation of ARP or ND entries for received management address TLVs

Enabling LLDP

Restrictions and guidelines

For LLDP to take effect on specific ports, you must enable LLDP both globally and on these ports.

Procedure

1. Enter system view.
   system-view
2. Enable LLDP globally.
   lldp global enable
   If the device is started with the software default settings, LLDP is disabled globally.
   If the device is started with the factory default settings, LLDP is enabled globally.
3. Enter interface view.
   interface *interface-type interface-number*
4. Enable LLDP.
   lldp enable
   By default, LLDP is enabled on a port.

Setting the LLDP bridge mode

1. Enter system view.
   system-view
2. Set the LLDP bridge mode.
   - Set the LLDP bridge mode to service bridge.
     lldp mode service-bridge
     By default, LLDP operates in customer bridge mode.
   - Set the LLDP bridge mode to customer bridge.
     undo lldp mode

   By default, LLDP operates in customer bridge mode.

Setting the LLDP operating mode

1. Enter system view.
   system-view
2. Enter interface view.
   interface *interface-type interface-number*
3. Set the LLDP operating mode.
   - In Layer 2/Layer 3 Ethernet interface view or management Ethernet interface view:
     lldp [**agent** { **nearest-customer** | **nearest-nontpmr** }] **admin-status** { **disable** | **rx** | **tx** | **txrx** }

In Ethernet interface view, if you do not specify an agent type, the command sets the operating mode for the nearest bridge agent.

- In Layer 2/Layer 3 aggregate interface view:

  lldp agent { **nearest-customer** | **nearest-nontpmr** } **admin-status** { **disable** | **rx** | **tx** | **txrx** }

  In aggregate interface view, you can set the operating mode only for the nearest customer bridge agent and nearest non-TPMR bridge agent.

- In IRF physical interface view:

  lldp admin-status { **disable** | **rx** | **tx** | **txrx** }

  In IRF physical interface view, you can set the operating mode only for the nearest bridge agent.

By default:

- The nearest bridge agent operates in TxRx mode.
- The nearest customer bridge agent and nearest non-TPMR bridge agent operate in **Disable** mode.

Setting the LLDP reinitialization delay

About LLDP reinitialization delay

When the LLDP operating mode changes on a port, the port initializes the protocol state machines after an LLDP reinitialization delay. By adjusting the delay, you can avoid frequent initializations caused by frequent changes to the LLDP operating mode on a port.

Procedure

1. Enter system view.

   system-view

2. Set the LLDP reinitialization delay.

   lldp timer reinit-delay *delay*

   The default LLDP reinitialization delay is 2 seconds.

Configuring the advertisable TLVs

1. Enter system view.

   system-view

2. Enter interface view.

   interface *interface-type interface-number*

3. Configure the advertisable TLVs.

   - In Layer 2 Ethernet interface view:

     lldp tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [**ipv6**] [*ip-address* | **interface loopback** *interface-number*] } | **dot1-tlv** { **all** | **congestion-notification** | **port-vlan-id** | **link-aggregation** | **dcbx** | **protocol-vlan-id** [*vlan-id*] | **vlan-name** [*vlan-id*] | **management-vid** [*mvlan-id*] } | **dot3-tlv** { **all** | **link-aggregation** | **mac-physic** | **max-frame-size** | **power** } | **med-tlv** { **all** | **capability** | **inventory** | **network-policy** [*vlan-id*] | **power-over-ethernet** | **location-id** { **civic-address** *device-type*

country-code { *ca-type ca-value* }&<1-10> | **elin-address** *tel-number* } } }

By default, the nearest bridge agent advertises all supported TLVs except the following TLVs:

- DCBX TLVs.
- Location identification TLVs.
- Port and protocol VLAN ID TLVs.
- VLAN name TLVs.
- Management VLAN ID TLVs.

lldp agent nearest-nontpmr tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [**ipv6**] [*ip-address*] } | **dot1-tlv** { **all** | **congestion-notification** | **evb** | **port-vlan-id** | **link-aggregation** } | **dot3-tlv** { **all** | **link-aggregation** } }

lldp tlv-enable dot1-tlv { **protocol-vlan-id** [*vlan-id*] | **vlan-name** [*vlan-id*] | **management-vid** [*mvlan-id*] }

By default:

- For the S6820 and S6861 switch series, the **evb** keyword is not supported. The nearest non-TPMR bridge agent does not advertise any TLVs.
- For other switch series, the nearest non-TPMR bridge agent advertises only EVB TLVs.

lldp agent nearest-customer tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [**ipv6**] [*ip-address*] } | **dot1-tlv** { **all** | **congestion-notification** | **port-vlan-id** | **link-aggregation** } | **dot3-tlv** { **all** | **link-aggregation** } }

lldp tlv-enable dot1-tlv { **protocol-vlan-id** [*vlan-id*] | **vlan-name** [*vlan-id*] | **management-vid** [*mvlan-id*] }

By default, the nearest customer bridge agent advertises all the supported basic management TLVs and IEEE 802.1 organizationally specific TLVs.

- In Layer 3 Ethernet interface view:

lldp tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [**ipv6**] [*ip-address* | **interface loopback** *interface-number*] } | **dot1-tlv** { **all** | **link-aggregation** } | **dot3-tlv** { **all** | **link-aggregation** | **mac-physic** | **max-frame-size** | **power** } | **med-tlv** { **all** | **capability** | **inventory** | **power-over-ethernet** | **location-id** { **civic-address** *device-type country-code* { *ca-type ca-value* }&<1-10> | **elin-address** *tel-number* } } }

By default, the nearest bridge agent advertises the following TLVs:

- Link aggregation TLVs in the 802.1 organizationally specific TLV set.
- All supported 802.3 organizationally specific TLVs.
- All supported LLDP-MED TLVs except the network policy TLVs.

lldp agent { **nearest-nontpmr** | **nearest-customer** } **tlv-enable** { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [**ipv6**] [*ip-address*] } | **dot1-tlv** { **all** | **link-aggregation** } | **dot3-tlv** { **all** | **link-aggregation** } }

By default:

- The nearest non-TPMR bridge agent does not advertise any TLVs.

- The nearest customer bridge agent advertises all supported basic management TLVs and link aggregation TLVs in the IEEE 802.1 organizationally specific TLV set.

- In management Ethernet interface view:

  lldp tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [**ipv6**] [*ip-address*] } | **dot1-tlv** { **all** | **link-aggregation** } | **dot3-tlv** { **all** | **link-aggregation** | **mac-physic** | **max-frame-size** | **power** } | **med-tlv** { **all** | **capability** | **inventory** | **power-over-ethernet** | **location-id** { **civic-address** *device-type country-code* { *ca-type ca-value* }&<1-10> | **elin-address** *tel-number* } } }

  By default, the nearest bridge agent advertises the following TLVs:

  - Link aggregation TLVs in the 802.1 organizationally specific TLV set.
  - All supported 802.3 organizationally specific TLVs.
  - All supported LLDP-MED TLVs except the network policy TLVs.

  lldp agent { **nearest-nontpmr** | **nearest-customer** } **tlv-enable** { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [**ipv6**] [*ip-address*] } | **dot1-tlv** { **all** | **link-aggregation** } | **dot3-tlv** { **all** | **link-aggregation** } }

  By default:

  - The nearest non-TPMR bridge agent does not advertise anyTLVs.
  - The nearest customer bridge agent advertises all supported basic management TLVs and link aggregation TLVs in the IEEE 802.1 organizationally specific TLV set.

- In Layer 2 aggregate interface view:

  lldp tlv-enable dot1-tlv { **protocol-vlan-id** [*vlan-id*] | **vlan-name** [*vlan-id*] | **management-vid** [*mvlan-id*]

  lldp agent nearest-nontpmr tlv-enable { **basic-tlv** { **all** | **management-address-tlv** [**ipv6**] [*ip-address*] | **port-description** | **system-capability** | **system-description** | **system-name** } | **dot1-tlv** { **all** | **evb** | **port-vlan-id** } }

  By default:

  - For the S6820 and S6861 switch series, the **evb** keyword is not supported. The nearest non-TPMR bridge agent does not advertise any TLVs.
  - For other switch series, the nearest non-TPMR bridge agent advertises only EVB TLVs.

  lldp agent nearest-customer tlv-enable { **basic-tlv** { **all** | **management-address-tlv** [**ipv6**] [*ip-address*] | **port-description** | **system-capability** | **system-description** | **system-name** } | **dot1-tlv** { **all** | **port-vlan-id** } }

  By default, the nearest customer bridge agent advertises all supported basic management TLVs and the following IEEE 802.1 organizationally specific TLVs:

  - Port and protocol VLAN ID TLVs.
  - VLAN name TLVs.
  - Management VLAN ID TLVs.

  The nearest bridge agent is not supported.

- In Layer 3 aggregate interface view:

  lldp agent { **nearest-customer** | **nearest-nontpmr** } **tlv-enable basic-tlv** { **all** | **management-address-tlv** [**ipv6**] [*ip-address*] |

port-description | **system-capability** | **system-description** | **system-name** }

By default:

- The nearest non-TPMR bridge agent does not advertise any TLVs.
- The nearest customer bridge agent advertises all supported basic management TLVs.

The nearest bridge agent is not supported.

- In IRF physical interface view:

  lldp tlv-enable basic-tlv { **port-description** | **system-capability** | **system-description** | **system-name** }

  By default, the nearest bridge agent advertises all supported basic management TLVs.

  Only the nearest bridge agent is supported.

Configuring advertisement of the management address TLV

About advertisement of the management address TLV

LLDP encodes management addresses in numeric or string format in management address TLVs.

If a neighbor encodes its management address in string format, set the encoding format of the management address to **string** on the connecting port. This guarantees normal communication with the neighbor.

You can configure advertisement of the management address TLV globally or on a per-interface basis. The device selects the management address TLV advertisement setting for an interface in the following order:

1. Interface-based setting, configured by using the **lldp tlv-enable** command with the **management-address-tlv** keyword.
2. Global setting, configured by using the **lldp global tlv-enable basic-tlv management-address-tlv** command.
3. Default setting for the interface.

   By default:

   - The nearest bridge agent and nearest customer bridge agent advertise the management address TLV.
   - The nearest non-TPMR bridge agent does not advertise the management address TLV.

Procedure

1. Enter system view.

   system-view

2. Enable advertisement of the management address TLV globally and set the management address to be advertised.

   lldp [**agent** { **nearest-customer** | **nearest-nontpmr** }] **global tlv-enable basic-tlv management-address-tlv** [**ipv6**] { *ip-address* | **interface loopback** *interface-number* | **interface m-gigabitethernet** *interface-number* | **interface vlan-interface** *interface-number* }

   By default, advertisement of the management address TLV is disabled globally.

3. Enter interface view.

   interface *interface-type interface-number*

4. Enable advertisement of the management address TLV on the interface and set the management address to be advertised.
   - In Layer 2 Ethernet interface view or management Ethernet interface view:

     lldp tlv-enable basic-tlv management-address-tlv [**ipv6**] [*ip-address* | **interface loopback** *interface-number*]

     lldp agent { **nearest-customer** | **nearest-nontpmr** } **tlv-enable basic-tlv management-address-tlv** [**ipv6**] [*ip-address*]
   - In Layer 3 Ethernet interface view:

     lldp [**agent** { **nearest-customer** | **nearest-nontpmr** }] **tlv-enable basic-tlv management-address-tlv** [**ipv6**] [*ip-address*] | **interface loopback** *interface-number*]
   - In Layer 2/Layer 3 aggregate interface view:

     lldp agent { **nearest-customer** | **nearest-nontpmr** } **tlv-enable basic-tlv management-address-tlv** [**ipv6**] [*ip-address*]

   By default:
   - The nearest bridge agent and nearest customer bridge agent advertise the management address TLVs.
   - The nearest non-TPMR bridge agent does not advertise the management address TLV.

   The device supports only the numeric encoding format for IPv6 management addresses.
5. Set the encoding format of the management address to string.
   - In Layer 2/Layer 3 Ethernet interface view or management Ethernet interface view:

     lldp [**agent** { **nearest-customer** | **nearest-nontpmr** }] **management-address-format string**
   - In Layer 2/Layer 3 aggregate interface view:

     lldp agent { **nearest-customer** | **nearest-nontpmr** } **management-address-format string**

   The default management address encoding format is numeric.

Setting the encapsulation format for LLDP frames

About setting the LLDP frame encapsulation format

Earlier versions of LLDP require the same encapsulation format on both ends to process LLDP frames. To successfully communicate with a neighboring device running an earlier version of LLDP, the local device must be set with the same encapsulation format.

Procedure

1. Enter system view.

   system-view
2. Enter interface view.

   interface *interface-type interface-number*
3. Set the encapsulation format for LLDP frames to SNAP.
   - In Layer 2/Layer 3 Ethernet interface view or management Ethernet interface view:

     lldp [**agent** { **nearest-customer** | **nearest-nontpmr** }] **encapsulation snap**
   - In Layer 2/Layer 3 aggregate interface view:

     lldp agent { **nearest-customer** | **nearest-nontpmr** } **encapsulation snap**

- In IRF physical interface view:
  lldp encapsulation snap

By default, the Ethernet II encapsulation format is used.

Setting LLDP frame transmission parameters

About setting LLDP frame transmission parameters

The Time to Live TLV carried in an LLDPDU determines how long the device information carried in the LLDPDU can be saved on a recipient device.

By setting the TTL multiplier, you can configure the TTL of locally sent LLDPDUs. The TTL is expressed by using the following formula:

TTL = Min (65535, (TTL multiplier × LLDP frame transmission interval + 1))

As the expression shows, the TTL can be up to 65535 seconds. TTLs greater than 65535 will be rounded down to 65535 seconds.

Procedure

1. Enter system view.
   system-view
2. Set the TTL multiplier.
   lldp hold-multiplier *value*
   The default setting is 4.
3. Set the LLDP frame transmission interval.
   lldp timer tx-interval *interval*
   The default setting is 30 seconds.
4. Set the token bucket size for sending LLDP frames.
   lldp max-credit *credit-value*
   The default setting is 5.
5. Set the number of LLDP frames sent each time fast LLDP frame transmission is triggered.
   lldp fast-count *count*
   The default setting is 4.
6. Set the fast LLDP frame transmission interval.
   lldp timer fast-interval *interval*
   The default setting is 1 second.

Setting the timeout for receiving LLDP frames

About the timeout for receiving LLDP frames

This feature allows the device to detect the presence of directly connected neighbors by setting the timeout timer for receiving LLDP frames. If an interface has not received any frames when the timeout timer expires, the device reports a no LLDP neighbor event to the NETCONF module.

Restrictions and guidelines

To avoid misdetection, make sure the timeout for receiving LLDP frames is greater than the LLDP frame transmission interval.

Procedure

1. Enter system view.

system-view

2. Set the timeout for receiving LLDP frames.

   lldp timer rx-timeout *timeout*

   By default, no timeout is set for receiving LLDP frames, and the device does not report no LLDP neighbor events.

Enabling LLDP polling

About LLDP polling

With LLDP polling enabled, a device periodically searches for local configuration changes. When the device detects a configuration change, it sends LLDP frames to inform neighboring devices of the change.

Procedure

1. Enter system view.

   system-view

2. Enter interface view.

   interface *interface-type interface-number*

3. Enable LLDP polling and set the polling interval.

   - In Layer 2/Layer 3 Ethernet interface view or management Ethernet interface view:

     lldp [**agent** { **nearest-customer** | **nearest-nontpmr** }] **check-change-interval** *interval*

   - In Layer 2/Layer 3 aggregate interface view:

     lldp agent { **nearest-customer** | **nearest-nontpmr** } **check-change-interval** *interval*

   - In IRF physical interface view:

     lldp check-change-interval *interval*

   By default, LLDP polling is disabled.

Disabling LLDP PVID inconsistency check

About LLDP PVID inconsistency check

By default, when the system receives an LLDP packet, it compares the PVID value contained in the packet with the PVID configured on the receiving interface. If the two PVIDs do not match, a log message will be printed to notify the user.

You can disable PVID inconsistency check if different PVIDs are required on a link.

Procedure

1. Enter system view.

   system-view

2. Disable LLDP PVID inconsistency check.

   lldp ignore-pvid-inconsistency

   By default, LLDP PVID inconsistency check is enabled.

Configuring CDP compatibility

About CDP compatibility

To enable your device to exchange information with a directly connected Cisco device that supports only CDP, you must enable CDP compatibility.

CDP compatibility enables your device to receive and recognize CDP packets from the neighboring CDP device and send CDP packets to the neighboring device. The CDP packets sent to the neighboring CDP device carry the following information:

- Device ID.
- ID of the port connecting to the neighboring device.
- Port IP address.
- TTL.

The port IP address is the primary IP address of a VLAN interface in up state. The VLAN ID of the VLAN interface must be the lowest among the VLANs permitted on the port. If no VLAN interfaces of the permitted VLANs are assigned an IP address or all VLAN interfaces are down, no port IP address will be advertised.

You can view the neighboring CDP device information that can be recognized by the device in the output of the **`display lldp neighbor-information`** command. For more information about the **`display lldp neighbor-information`** command, see LLDP commands in *Layer 2—LAN Switching Command Reference*.

To make your device work with Cisco IP phones, you must enable CDP compatibility.

If your LLDP-enabled device cannot recognize CDP packets, it does not respond to the requests of Cisco IP phones for the voice VLAN ID configured on the device. As a result, a requesting Cisco IP phone sends voice traffic without any tag to your device. Your device cannot differentiate the voice traffic from other types of traffic.

CDP compatibility enables your device to receive and recognize CDP packets from a Cisco IP phone and respond with CDP packets carrying TLVs with the configured voice VLAN. If no voice VLAN is configured for CDP packets, CDP packets carry the voice VLAN of the port or the voice VLAN assigned by the RADIUS server. The assigned voice VLAN has a higher priority. According to TLVs with the voice VLAN configuration, the IP phone automatically configures the voice VLAN. As a result, the voice traffic is confined in the configured voice VLAN and is differentiated from other types of traffic.

For more information about voice VLANs, see "Configuring voice VLANs."

When the device is connected to a Cisco IP phone that has a host attached to its data port, the host must access the network through the Cisco IP phone. If the data port goes down, the IP phone will send a CDP packet to the device so the device can log out the user.

CDP-compatible LLDP operates in one of the following modes:

- **TxRx**—CDP packets can be transmitted and received.
- **Rx**—CDP packets can be received but cannot be transmitted.
- **Disable**—CDP packets cannot be transmitted or received.

Restrictions and guidelines

When you configure CDP compatibility for LLDP, follow these restrictions and guidelines:

- To make CDP-compatible LLDP take effect on a port, follow these steps:
  a. Enable CDP-compatible LLDP globally.
  b. Configure CDP-compatible LLDP to operate in TxRx mode on the port.

- The maximum TTL value that CDP allows is 255 seconds. To make CDP-compatible LLDP work correctly with Cisco IP phones, configure the LLDP frame transmission interval to be no more than 1/3 of the TTL value.

Prerequisites

Before you configure CDP compatibility, complete the following tasks:

- Globally enable LLDP.
- Enable LLDP on the port connecting to a CDP device.
- Configure LLDP to operate in TxRx mode on the port.

Procedure

1. Enter system view.
   system-view
2. Enable CDP compatibility globally.
   lldp compliance cdp
   By default, CDP compatibility is disabled globally.
3. Enter Layer 2/Layer 3 Ethernet interface view or management Ethernet interface view.
   interface *interface-type interface-number*
4. Configure CDP-compatible LLDP to operate in TxRx mode.
   lldp compliance admin-status cdp txrx
   By default, CDP-compatible LLDP operates in **disable** mode.
5. Set the voice VLAN ID carried in CDP packets.
   cdp voice-vlan *vlan-id*
   By default, no voice VLAN ID is configured to be carried in CDP packets.

Configuring LLDP trapping and LLDP-MED trapping

About LLDP trapping and LLDP-MED trapping

LLDP trapping or LLDP-MED trapping notifies the network management system of events such as newly detected neighboring devices and link failures.

To prevent excessive LLDP traps from being sent when the topology is unstable, set a trap transmission interval for LLDP.

Procedure

1. Enter system view.
   system-view
2. Enter interface view.
   interface *interface-type interface-number*
3. Enable LLDP trapping.
   - In Layer 2/Layer 3 Ethernet interface view or management Ethernet interface view:
     lldp [**agent** { **nearest-customer** | **nearest-nontpmr** }] **notification remote-change enable**
   - In Layer 2/Layer 3 aggregate interface view:
     lldp agent { **nearest-customer** | **nearest-nontpmr** } **notification remote-change enable**

- In IRF physical interface view:

  lldp notification remote-change enable

By default, LLDP trapping is disabled.

4. (In Layer 2/Layer 3 Ethernet interface view or management Ethernet interface view.) Enable LLDP-MED trapping.

   lldp notification med-topology-change enable

   By default, LLDP-MED trapping is disabled.

5. Return to system view.

   quit

6. (Optional.) Set the LLDP trap transmission interval.

   lldp timer notification-interval *interval*

   The default setting is 30 seconds.

Configuring LLDP neighbor validation and aging

Configuring LLDP neighbor validation on an interface

About LLDP neighbor validation

LLDP neighbor validation enables an interface to validate the identity of the neighbor based on the neighbor validation criteria configured on the interface. The neighbor validation criteria can be the chassis ID TLV, port ID TLV, or both. Each incoming LLDP packet must match all the validation criteria configured on the interface. If the neighbor information in an incoming LLDP packet does not match the criteria, the system shuts down the data link layer and disables data transmission on the interface.

Procedure

1. Enter system view.

   system-view

2. Enter Layer 2 or Layer 3 Ethernet interface view.

   interface *interface-type interface-number*

3. Configure the neighbor validation criteria. Choose the following tasks as needed:

   - Configure the chassis ID TLV criterion.

     lldp neighbor-identity chassis-id *chassis-id-subtype chassis-id*

   - Configure the port ID TLV criterion.

     lldp neighbor-identity port-id *port-id-subtype port-id*

   By default, no neighbor validation criteria exist on an interface.

4. Enable LLDP neighbor validation on the interface.

   lldp neighbor-protection validation

   By default, LLDP neighbor validation is disabled on an interface.

Configuring LLDP neighbor aging on an interface

About LLDP neighbor aging

An LLDP neighbor aging-enabled interface ages out a neighbor if it does not receive an LLDP packet from the neighbor within the aging time.

LLDP takes either of the following actions when neighbor aging occurs on an interface:

- **Block**—Blocks the interface. The **block** action places the data link layer protocol of the interface in **DOWN** state. In this state, the interface cannot transfer data packets. The data transfer capability automatically recovers when the interface receives an LLDP packet.
- **Shutdown**—Shuts down the interface. The **shutdown** action places the interface in **LLDP DOWN** state. In this state, the interface can neither transfer data packets nor LLDP packets. You must manually execute the **undo lldp neighbor-protection aging** or **undo shutdown** command to bring up the interface.

Procedure

1. Enter system view.
   system-view
2. Enter Layer 2 or Layer 3 Ethernet interface view.
   interface *interface-type interface-number*
3. Enable LLDP neighbor aging on the interface.
   lldp neighbor-protection aging { **block** | **shutdown** }
   By default, neighbor aging is disabled on an interface.

Configuring MAC address learning for DCN

About MAC address learning for DCN

For the data communication network (DCN) to implement operation, administration, and maintenance on network elements (NEs), you must configure the NEs to learn their neighbors' MAC addresses through LLDP.

An NE learns the MAC address of its neighbor through the ARP or ND entry generated based on the management address TLV in LLDP frames received from the neighbor. For more information about DCN, see *Layer 3—IP Routing Configuration Guide*.

MAC address learning for DCN tasks at a glance

Configuring MAC address learning for DCN on a Layer 2 Ethernet interface

1. Setting the source MAC address of LLDP frames
2. Enabling generation of ARP or ND entries for received management address TLVs

Configuring MAC address learning for DCN on a Layer 3 Ethernet interface

1. (Optional.) Setting the source MAC address of LLDP frames
2. Enabling generation of ARP or ND entries for received management address TLVs

Setting the source MAC address of LLDP frames

About setting the source MAC address of LLDP frames

This feature allows you to set the source MAC address of LLDP frames to the MAC address of a VLAN interface or a Layer 3 Ethernet subinterface.

Restrictions and guidelines

In Layer 2 Ethernet interface view, you must configure this feature so the interface can use the MAC address of a VLAN interface instead of its own MAC address as the source MAC address of LLDP frames. This ensures that the neighbor NE can generate correct ARP or ND entries for the local NE.

Procedure

1. Enter system view.

   system-view

2. Enter Ethernet interface view.

   interface *interface-type interface-number*

3. Set the source MAC address of LLDP frames to the MAC address of a VLAN interface or a Layer 3 Ethernet subinterface.

   lldp source-mac vlan *vlan-id*

   By default, the source MAC address of LLDP frames is the MAC address of the egress interface.

   To use the MAC address of a Layer 3 Ethernet subinterface as the source MAC address, use *vlan-id* to specify the subinterface ID in Layer 3 Ethernet interface view.

Enabling generation of ARP or ND entries for received management address TLVs

About generation of ARP or ND entries for received management address TLVs

This feature enables the device to generate an ARP or ND entry after receiving an LLDP frame containing a management address TLV on an interface. The ARP or ND entry maps the advertised management address to the source MAC address of the frame.

You can enable generation of both ARP and ND entries on an interface. If the management address TLV contains an IPv4 address, the device generates an ARP entry. If the management address TLV contains an IPv6 address, the device generates an ND entry.

Restrictions and guidelines

In Layer 2 Ethernet interface view, you must configure the interface to use the MAC address of a VLAN interface instead of its own MAC address as the source MAC address of LLDP frames. This ensures that the neighbor NE can generate correct ARP or ND entries.

In Layer 3 Ethernet interface view, you can specify an existing Layer 3 Ethernet subinterface as the output interface in the generated ARP or ND entry. Make sure the Layer 3 Ethernet subinterface has an IP address that can be used for communications with the neighbor device.

Procedure

1. Enter system view.

   system-view

2. Enter Ethernet interface view.

   interface *interface-type interface-number*

3. Enable generation of ARP or ND entries for management address TLVs received on the interface.

   lldp management-address { **arp-learning** | **nd-learning** } [**vlan** *vlan-id*]

   By default, generation of ARP or ND entries for received management address TLVs is disabled on an interface.

   In Layer 3 Ethernet interface view, the **vlan** *vlan-id* option specifies the ID of a Layer 3 Ethernet subinterface used as the output interface in the ARP or ND entry.

   In Layer 2 Ethernet interface view, the **vlan** *vlan-id* option specifies the ID of the VLAN to which the generated ARP or ND entry belongs. To prevent the ARP or ND entries from overwriting each other, do not specify the same VLAN ID for different Layer 2 Ethernet interfaces.

   You can enable generation of both ARP and ND entries on an interface.

Display and maintenance commands for LLDP

Execute **display** commands in any view.

Task	Command
Display local LLDP information.	**display lldp local-information** [**global** | **interface** *interface-type interface-number*]
Display the information contained in the LLDP TLVs sent from neighboring devices.	**display lldp neighbor-information** [[[**interface** *interface-type interface-number*] [**agent** { **nearest-bridge** | **nearest-customer** | **nearest-nontpmr** }] [**verbose**]] | **list** [**system-name** *system-name*]]
Display LLDP statistics.	**display lldp statistics** [**global** | [**interface** *interface-type interface-number*] [**agent** { **nearest-bridge** | **nearest-customer** | **nearest-nontpmr** }]]
Display LLDP status of a port.	**display lldp status** [**interface** *interface-type interface-number*] [**agent** { **nearest-bridge** | **nearest-customer** | **nearest-nontpmr** }]
Display types of advertisable optional LLDP TLVs.	**display lldp tlv-config** [**interface** *interface-type interface-number*] [**agent** { **nearest-bridge** | **nearest-customer** | **nearest-nontpmr** }]
Clear LLDP statistics on ports.	**reset lldp statistics** [**interface** *interface-type interface number*] [**agent** { **nearest-bridge** | **nearest-customer** | **nearest-nontpmr** }]

LLDP configuration examples

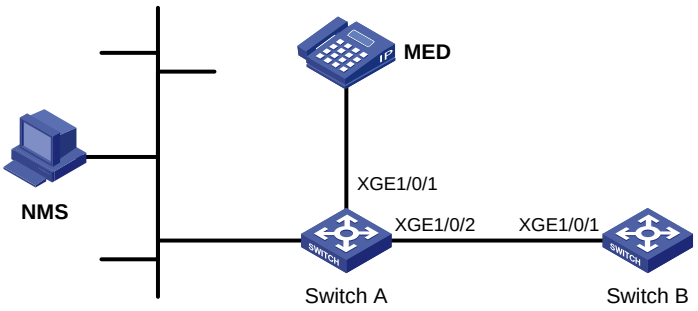
Example: Configuring basic LLDP functions

Network configuration

As shown in Figure 5, enable LLDP globally on Switch A and Switch B to perform the following tasks:

- Monitor the link between Switch A and Switch B on the NMS.
- Monitor the link between Switch A and the MED device on the NMS.

Figure 5 Network diagram



Procedure

1. Configure Switch A:

   # Enable LLDP globally.

   ```
   <SwitchA> system-view
   [SwitchA] lldp global enable
   ```

   # Enable LLDP on Ten-GigabitEthernet 1/0/1. By default, LLDP is enabled on ports.

   ```
   [SwitchA] interface ten-gigabitethernet 1/0/1
   [SwitchA-Ten-GigabitEthernet1/0/1] lldp enable
   ```

   # Set the LLDP operating mode to Rx on Ten-GigabitEthernet 1/0/1.

   ```
   [SwitchA-Ten-GigabitEthernet1/0/1] lldp admin-status rx
   [SwitchA-Ten-GigabitEthernet1/0/1] quit
   ```

   # Enable LLDP on Ten-GigabitEthernet 1/0/2. By default, LLDP is enabled on ports.

   ```
   [SwitchA] interface gigabitethernet1/2
   [SwitchA-Ten-GigabitEthernet1/0/2] lldp enable
   ```

   # Set the LLDP operating mode to Rx on Ten-GigabitEthernet 1/0/2.

   ```
   [SwitchA-Ten-GigabitEthernet1/0/2] lldp admin-status rx
   [SwitchA-Ten-GigabitEthernet1/0/2] quit
   ```

2. Configure Switch B:

   # Enable LLDP globally.

   ```
   <SwitchB> system-view
   [SwitchB] lldp global enable
   ```

   # Enable LLDP on Ten-GigabitEthernet 1/0/1. By default, LLDP is enabled on ports.

   ```
   [SwitchB] interface ten-gigabitethernet 1/0/1
   [SwitchB-Ten-GigabitEthernet1/0/1] lldp enable
   ```

   # Set the LLDP operating mode to Tx on Ten-GigabitEthernet 1/0/1.

   ```
   [SwitchB-Ten-GigabitEthernet1/0/1] lldp admin-status tx
   [SwitchB-Ten-GigabitEthernet1/0/1] quit
   ```

Verifying the configuration

Verify the following items:

- Ten-GigabitEthernet 1/0/1 of Switch A connects to a MED device.
- Ten-GigabitEthernet 1/0/2 of Switch A connects to a non-MED device.
- Both ports operate in Rx mode, and they can receive LLDP frames but cannot send LLDP frames.

```
[SwitchA] display lldp status
Global status of LLDP: Enable
Bridge mode of LLDP: customer-bridge
The current number of LLDP neighbors: 2
The current number of CDP neighbors: 0
LLDP neighbor information last changed time: 0 days, 0 hours, 4 minutes, 40 seconds
Transmit interval              : 30s
Fast transmit interval         : 1s
Transmit credit max            : 5
Hold multiplier                : 4
Reinit delay                   : 2s
Trap interval                  : 30s
Fast start times               : 4
```

```
LLDP status information of port 1 [Ten-GigabitEthernet1/0/1]:
LLDP agent nearest-bridge:
Port status of LLDP            : Enable
Admin status                   : Rx_Only
Trap flag                      : No
MED trap flag                  : No
Polling interval               : 0s
Number of LLDP neighbors       : 1
Number of MED neighbors        : 1
Number of CDP neighbors        : 0
Number of sent optional TLV    : 21
Number of received unknown TLV : 0

LLDP agent nearest-customer:
Port status of LLDP            : Enable
Admin status                   : Disable
Trap flag                      : No
MED trap flag                  : No
Polling interval               : 0s
Number of LLDP neighbors       : 0
Number of MED neighbors        : 0
Number of CDP neighbors        : 0
Number of sent optional TLV    : 16
Number of received unknown TLV : 0

LLDP status information of port 2 [Ten-GigabitEthernet1/0/2]:
LLDP agent nearest-bridge:
Port status of LLDP            : Enable
Admin status                   : Rx_Only
Trap flag                      : No
MED trap flag                  : No
Polling interval               : 0s
Number of LLDP neighbors       : 1
Number of MED neighbors        : 0
Number of CDP neighbors        : 0
Number of sent optional TLV    : 21
Number of received unknown TLV : 3

LLDP agent nearest-nontpmr:
Port status of LLDP            : Enable
Admin status                   : Disable
Trap flag                      : No
MED trap flag                  : No
Polling interval               : 0s
Number of LLDP neighbors       : 0
Number of MED neighbors        : 0
Number of CDP neighbors        : 0
```

```
Number of sent optional TLV    : 1
Number of received unknown TLV : 0

LLDP agent nearest-customer:
Port status of LLDP            : Enable
Admin status                   : Disable
Trap flag                      : No
MED trap flag                  : No
Polling interval               : 0s
Number of LLDP neighbors       : 0
Number of MED neighbors        : 0
Number of CDP neighbors        : 0
Number of sent optional TLV    : 16
Number of received unknown TLV : 0
```

Remove the link between Switch A and Switch B.

Verify that Ten-GigabitEthernet 1/0/2 of Switch A does not connect to any neighboring devices.

```
[SwitchA] display lldp status
Global status of LLDP: Enable
The current number of LLDP neighbors: 1
The current number of CDP neighbors: 0
LLDP neighbor information last changed time: 0 days, 0 hours, 5 minutes, 20 seconds
Transmit interval              : 30s
Fast transmit interval         : 1s
Transmit credit max            : 5
Hold multiplier                : 4
Reinit delay                   : 2s
Trap interval                  : 30s
Fast start times               : 4

LLDP status information of port 1 [Ten-GigabitEthernet1/0/1]:
LLDP agent nearest-bridge:
Port status of LLDP            : Enable
Admin status                   : Rx_Only
Trap flag                      : No
MED trap flag                  : No
Polling interval               : 0s
Number of LLDP neighbors       : 1
Number of MED neighbors        : 1
Number of CDP neighbors        : 0
Number of sent optional TLV    : 0
Number of received unknown TLV : 5

LLDP agent nearest-nontpmr:
Port status of LLDP            : Enable
Admin status                   : Disable
Trap flag                      : No
MED trap flag                  : No
Polling interval               : 0s
```

```
Number of LLDP neighbors       : 0
Number of MED neighbors        : 0
Number of CDP neighbors        : 0
Number of sent optional TLV    : 1
Number of received unknown TLV : 0

LLDP status information of port 2 [Ten-GigabitEthernet1/0/2]:
LLDP agent nearest-bridge:
Port status of LLDP            : Enable
Admin status                   : Rx_Only
Trap flag                      : No
MED trap flag                  : No
Polling interval               : 0s
Number of LLDP neighbors       : 0
Number of MED neighbors        : 0
Number of CDP neighbors        : 0
Number of sent optional TLV    : 0
Number of received unknown TLV : 0

LLDP agent nearest-nontpmr:
Port status of LLDP            : Enable
Admin status                   : Disable
Trap flag                      : No
MED trap flag                  : No
Polling interval               : 0s
Number of LLDP neighbors       : 0
Number of MED neighbors        : 0
Number of CDP neighbors        : 0
Number of sent optional TLV    : 1
Number of received unknown TLV : 0

LLDP agent nearest-customer:
Port status of LLDP            : Enable
Admin status                   : Disable
Trap flag                      : No
MED trap flag                  : No
Polling interval               : 0s
Number of LLDP neighbors       : 0
Number of MED neighbors        : 0
Number of CDP neighbors        : 0
Number of sent optional TLV    : 16
Number of received unknown TLV : 0
```

Example: Configuring CDP-compatible LLDP

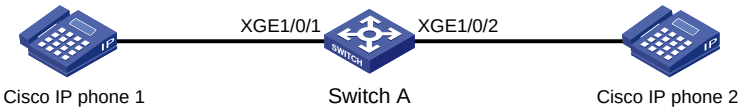
Network configuration

As shown in Figure 6, Ten-GigabitEthernet 1/0/1 and Ten-GigabitEthernet 1/0/2 of Switch A are each connected to a Cisco IP phone, which sends tagged voice traffic.

Configure voice VLAN 2 on Switch A. Enable CDP compatibility of LLDP on Switch A to allow the Cisco IP phones to automatically configure the voice VLAN. The voice VLAN feature performs the following operations:

- Confines the voice traffic to the voice VLAN.
- Isolates the voice traffic from other types of traffic.

Figure 6 Network diagram



Procedure

1. Configure a voice VLAN on Switch A:

Create VLAN 2.

```
<SwitchA> system-view
[SwitchA] vlan 2
[SwitchA-vlan2] quit
```

Set the link type of Ten-GigabitEthernet 1/0/1 and Ten-GigabitEthernet 1/0/2 to trunk, and enable voice VLAN on them.

```
[SwitchA] interface ten-gigabitethernet 1/0/1
[SwitchA-Ten-GigabitEthernet1/0/1] port link-type trunk
[SwitchA-Ten-GigabitEthernet1/0/1] voice-vlan 2 enable
[SwitchA-Ten-GigabitEthernet1/0/1] quit
[SwitchA] interface ten-gigabitethernet 1/0/2
[SwitchA-Ten-GigabitEthernet1/0/2] port link-type trunk
[SwitchA-Ten-GigabitEthernet1/0/2] voice-vlan 2 enable
[SwitchA-Ten-GigabitEthernet1/0/2] quit
```

2. Configure CDP-compatible LLDP on Switch A:

Enable LLDP globally, and enable CDP compatibility globally.

```
[SwitchA] lldp global enable
[SwitchA] lldp compliance cdp
```

Enable LLDP on Ten-GigabitEthernet 1/0/1. By default, LLDP is enabled on ports.

```
[SwitchA] interface ten-gigabitethernet 1/0/1
[SwitchA-Ten-GigabitEthernet1/0/1] lldp enable
```

Configure LLDP to operate in TxRx mode on Ten-GigabitEthernet 1/0/1.

```
[SwitchA-Ten-GigabitEthernet1/0/1] lldp admin-status txrx
```

Configure CDP-compatible LLDP to operate in TxRx mode on Ten-GigabitEthernet 1/0/1.

```
[SwitchA-Ten-GigabitEthernet1/0/1] lldp compliance admin-status cdp txrx
[SwitchA-Ten-GigabitEthernet1/0/1] quit
```

Enable LLDP on Ten-GigabitEthernet 1/0/2. By default, LLDP is enabled on ports.

```
[SwitchA] interface ten-gigabitethernet 1/0/2
[SwitchA-Ten-GigabitEthernet1/0/2] lldp enable
```

Configure LLDP to operate in TxRx mode on Ten-GigabitEthernet 1/0/2.

```
[SwitchA-Ten-GigabitEthernet1/0/2] lldp admin-status txrx
```

Configure CDP-compatible LLDP to operate in TxRx mode on Ten-GigabitEthernet 1/0/2.

```
[SwitchA-Ten-GigabitEthernet1/0/2] lldp compliance admin-status cdp txrx
[SwitchA-Ten-GigabitEthernet1/0/2] quit
```

Verifying the configuration

Verify that Switch A has completed the following operations:

- Discovering the IP phones connected to Ten-GigabitEthernet 1/0/1 and Ten-GigabitEthernet 1/0/2.
- Obtaining IP phone information.

```
[SwitchA] display lldp neighbor-information

CDP neighbor-information of port 1[Ten-GigabitEthernet1/0/1]:
LLDP agent nearest-bridge:
 CDP neighbor index  : 1
 Chassis ID          : SEP00141CBCDBFE
 Port ID             : Port 1

CDP neighbor-information of port 2[Ten-GigabitEthernet1/0/2]:
LLDP agent nearest-bridge:
 CDP neighbor index  : 2
 Chassis ID          : SEP00141CBCDBFF
 Port ID             : Port 1
```

Configuring DCBX

About DCBX

Data Center Ethernet (DCE), also known as Converged Enhanced Ethernet (CEE), is enhancement and expansion of traditional Ethernet local area networks for use in data centers. DCE uses the Data Center Bridging Exchange Protocol (DCBX) to negotiate and remotely configure the bridge capability of network elements.

DCBX versions

DCBX has the following self-adaptable versions:

- DCB Capability Exchange Protocol Specification Rev 1.00.
- DCB Capability Exchange Protocol Base Specification Rev 1.01.
- IEEE Std 802.1Qaz-2011 (Media Access Control (MAC) Bridges and Virtual Bridged Local Area Networks-Amendment 18: Enhanced Transmission Selection for Bandwidth Sharing Between Traffic Classes).

DCBX functions

DCBX offers the following functions:

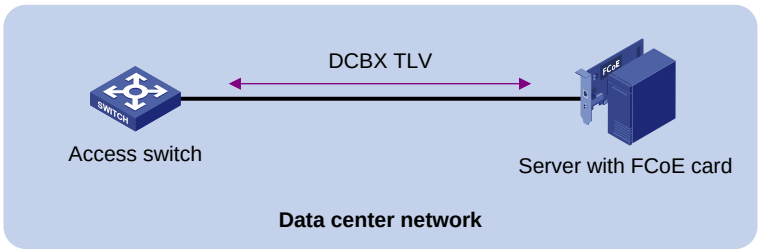
- Discovers the peer devices' capabilities and determines whether devices at both ends support these capabilities.
- Detects configuration errors on peer devices.
- Remotely configures the peer device if the peer device accepts the configuration.

NOTE:

H3C devices support only the remote configuration feature.

DCBX application scenario

Figure 7 DCBX application scenario



DCBX enables lossless packet transmission on DCE networks.

As shown in Figure 7, DCBX applies to an FCoE-based data center network, and operates on an access switch. DCBX enables the switch to control the server or storage adapter, and simplifies the configuration and guarantees configuration consistency. DCBX extends LLDP by using the IEEE 802.1 organizationally specific TLVs (DCBX TLVs) to transmit DCBX data, including:

- In DCBX Rev 1.00 and DCBX Rev 1.01:

    - Application Protocol (APP).
    - Enhanced Transmission Selection (ETS).
    - Priority-based Flow Control (PFC).
- In IEEE Std 802.1Qaz-2011:
    - ETS Configuration.
    - ETS Recommendation.
    - PFC.
    - APP.

H3C devices can send these types of DCBX information to a server or storage adapter supporting FCoE. However, H3C devices cannot accept these types of DCBX information.

Protocols and standards

- *DCB Capability Exchange Protocol Specification Rev 1.00*
- *DCB Capability Exchange Protocol Base Specification Rev 1.01*

DCBX tasks at a glance

To configure DCBX, perform the following tasks:

1. Enabling LLDP and DCBX TLV advertising
2. Setting the DCBX version
3. Configuring APP parameters
4. Configuring ETS parameters
    a. Configuring the 802.1p-to-local priority mapping
    b. Configuring group-based WRR queuing
5. Configuring PFC parameters

Enabling LLDP and DCBX TLV advertising

Restrictions and guidelines

To enable the device to advertise APP, ETS, and PFC data through an interface, perform the following tasks:

- Enable LLDP globally.
- Enable LLDP and DCBX TLV advertising on the interface.

Procedure

1. Enter system view.

   `system-view`
2. Enable LLDP globally.

   `lldp global enable`

   By default:
    - If the device is started with the software default settings, LLDP is disabled globally.
    - If the device is started with the factory default settings, LLDP is enabled globally.

   For more information about device startup with software or factory default settings, see configuration file management in *Fundamentals Configuration Guide*.

3. Enter Layer 2 Ethernet interface view.
   interface *interface-type interface-number*
4. Enable LLDP on the interface.
   lldp enable
   By default, LLDP is enabled on an interface.
5. Enable the interface to advertise DCBX TLVs.
   lldp tlv-enable dot1-tlv dcbx
   By default, DCBX TLV advertisement is disabled on an interface.

Setting the DCBX version

Restrictions and guidelines

When you set the DCBX version, follow these restrictions and guidelines:

- For DCBX to work correctly, configure the same DCBX version on the local port and peer port. As a best practice, configure the highest version supported on both ends. IEEE Std 802.1Qaz-2011, DCBX Rev 1.01, and DCBX Rev 1.00 are in descending order.
- After the configuration, LLDP frames sent by the local port carry information about the configured DCBX version. The local port and peer port do not negotiate the DCBX version.
- When the DCBX version is autonegotiated, the version IEEE Std 802.1Qaz-2011 is preferably negotiated.

Procedure

1. Enter system view.
   system-view
2. Enter Layer 2 Ethernet interface view.
   interface *interface-type interface-number*
3. Set the DCBX version.
   dcbx version { **rev100** | **rev101** | **standard** }
   By default, the DCBX version is not configured. It is autonegotiated by the local port and peer port.

Configuring APP parameters

About APP parameters

The device negotiates with the server adapter by using the APP parameters to achieve the following purposes:

- Control the 802.1p priority values of the protocol packets that the server adapter sends.
- Identify traffic based on the 802.1p priority values.

For example, the device can use the APP parameters to negotiate with the server adapter to set 802.1p priority 3 for all FCoE and FIP frames. When the negotiation succeeds, all FCoE and FIP frames that the server adapter sends to the device carry the 802.1p priority 3.

Restrictions and guidelines

When you configure APP parameters, follow these restrictions and guidelines:

- A Layer 2 ACL identifies application protocol packets by frame type.
- An IPv4 advanced ACL identifies application protocol packets by TCP/UDP port number.

- DCBX Rev 1.00 identifies application protocol packets only by frame type and advertises only TLVs with frame type 0x8906 (FCoE).
- DCBX Rev 1.01 has the following attributes:
  - Supports identifying application protocol packets by both frame type and TCP/UDP port number.
  - Does not restrict the frame type or TCP/UDP port number for advertising TLVs.
  - Can advertise up to 77 TLVs according to the remaining length of the current packet.
- In a QoS policy, you can configure multiple class-behavior associations. A packet might be configured with multiple 802.1p priority marking or mapping actions, and the one configured first takes effect.

Procedure

1. Enter system view.

   system-view

2. Create an ACL and enter its view.
   - Create a Layer 2 ACL and configure a rule for the ACL.

     acl mac { *acl-number* | **name** *acl-name* } [**match-order** { **auto** | **config** }]

     rule [*rule-id*] **permit type** *protocol-type* **ffff**
   - Create an IPv4 advanced ACL and configure a rule for the ACL.

     acl advanced { *acl-number* | **name** *acl-name* } [**match-order** { **auto** | **config** }]

     rule [*rule-id*] **permit** { **tcp** | **udp** } **destination-port eq** *port*

   DCBX Rev 1.00 supports only Layer 2 ACLs. DCBX Rev 1.01 and IEEE Std 802.1Qaz-2011 support both Layer 2 ACLs and IPv4 advanced ACLs.

3. Return to system view.

   quit

4. Configure a class:
   a. Create a class, specify the operator of the class as OR, and enter class view.

      traffic classifier *classifier-name* **operator or**

   b. Use the previously configured ACL as the match criterion of the class.

      if-match acl *acl-numbe*r

   c. Return to system view.

      quit

5. Configure a traffic behavior:
   a. Create a traffic behavior and enter its view.

      traffic behavior *behavior-name*

   b. Configure the behavior to mark packets with an 802.1p priority.

      remark dot1p *8021p*

   c. Return to system view.

      quit

6. Configure a QoS policy:
   a. Create a QoS policy and enter its view.

      qos policy *policy-name*

   b. Associate the class with the traffic behavior in the QoS policy, and apply the association to DCBX.

      classifier *classifier-name* **behavior** *behavior-name* **mode dcbx**

c. Return to system view.

quit

7. Apply the QoS policy.

Choose one option as needed:

- Apply the QoS policy to the outgoing traffic of all ports.

  qos apply policy *policy-name* **global outbound**
- Apply the QoS policy to the outgoing traffic of a Layer 2 Ethernet interface.

  interface *interface-type interface-number*

  qos apply policy *policy-name* **outbound**

The configuration in system view applies to all interfaces. The configuration in Layer 2 Ethernet interface view applies only to the Layer 2 Ethernet interface.

Configuring ETS parameters

About ETS parameters

ETS provides committed bandwidth. To avoid packet loss caused by congestion, the device performs the following operations:

- Uses ETS parameters to negotiate with the server adapter.
- Controls the server adapter's transmission speed of the specified type of traffic.
- Guarantees that the transmission speed is within the committed bandwidth of the interface.

Restrictions and guidelines

To configure ETS parameters, perform the following tasks:

1. Configure the 802.1p-to-local priority mapping by using either of the following methods:

- MQC method.
- Priority mapping table method.

If you configure the 802.1p-to-local priority mapping in both methods, the configuration made in the MQC method applies. For information about the QoS commands for configuring 802.1p-to-local priority mapping, see *ACL and QoS Command Reference*.

2. Configure group-based WRR queuing to allocate bandwidth.

For information about the WRR queuing configuration commands, see *ACL and QoS Command Reference*.

Configuring the 802.1p-to-local priority mapping

Configuring the 802.1p-to-local priority mapping in the MQC method

1. Enter system view.

system-view

2. Create a traffic class, specify the operator of the class as OR, and enter class view.

traffic classifier *classifier-name* **operator or**

3. Configure the class to match packets with the specified service provider network 802.1p priority values.

if-match service-dot1p *8021p-list*

By default, no match criterion is configured for the class to match packets.

4. Return to system view.
   quit
5. Create a traffic behavior and enter traffic behavior view.
   traffic behavior *behavior-name*
6. Configure the behavior to mark packets with the specified local precedence value.
   remark local-precedence *local-precedence*

   By default, no local precedence marking action is configured.
7. Return to system view.
   quit
8. Create a QoS policy and enter its view.
   qos policy *policy-name*
9. Associate the class with the traffic behavior in the QoS policy, and apply the association to DCBX.
   classifier *classifier-name* **behavior** *behavior-name* **mode dcbx**

   By default, no class-behavior associations exist.

Configuring the 802.1p-to-local priority mapping in the priority mapping table method

1. Enter system view.
   system-view
2. Enter 802.1p-to-local priority mapping table view for the outgoing traffic.
   qos map-table dot1p-lp
3. Configure the priority mapping table to map the specified 802.1p priority values to a local precedence value.
   import *import-value-list* **export** *export-value*

   For information about the default priority mapping tables, see *ACL and QoS Configuration Guide*.

Configuring group-based WRR queuing

1. Enter system view.
   system-view
2. Enter Layer 2 Ethernet interface view.
   interface *interface-type interface-number*
3. Enable WRR queuing.
   qos wrr byte-count

   By default, an interface uses the WRR queue scheduling algorithm.
4. Configure a queue.

   Choose one option as needed:
   - Add a queue to WRR priority group 1 and configure the scheduling weight for the queue.
     qos wrr *queue-id* **group 1 byte-count** *schedule-value*
   - Configure a queue to use SP queuing.
     qos wrr *queue-id* **group sp**

Configuring PFC parameters

About PFC parameters

To prevent packets with an 802.1p priority value from being dropped, enable PFC for the 802.1p priority value. This feature reduces the sending rate of packets carrying this priority when network congestion occurs.

The device uses PFC parameters to negotiate with the server adapter and to enable PFC for the specified 802.1p priorities on the server adapter.

For more information about PFC commands, see *Interface Command Reference.*

Procedure

1. Enter system view.
   `system-view`
2. Enter Layer 2 Ethernet interface view.
   `interface` *`interface-type interface-number`*
3. Enable PFC in auto mode on the Ethernet interface.
   `priority-flow-control auto`
   By default, PFC is disabled.
   To advertise the PFC data, you must enable PFC in auto mode.
4. Enable PFC for the specified 802.1p priorities.
   `priority-flow-control no-drop dot1p` *`dot1p-list`*
   By default, PFC is disabled for all 802.1p priorities.

DCBX configuration examples

Example: Configuring DCBX

Network configuration

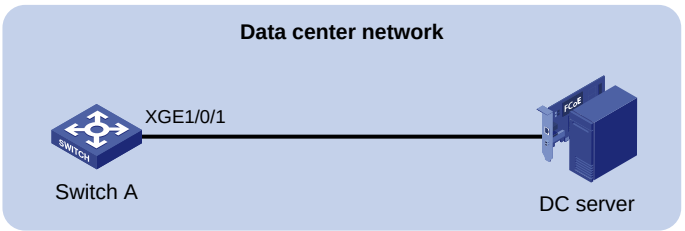
As shown in Figure 8, Ten-GigabitEthernet 1/0/1 of the access switch (Switch A) connects to the FCoE adapter of the data center server (DC server).

Configure Switch A to implement lossless FCoE and FIP frame transmission to DC server.

NOTE:

In this example, both Switch A and the DC server support DCBX Rev 1.01.

Figure 8 Network diagram



Procedure

1. Enable LLDP and DCBX TLV advertising:

Enable LLDP globally.

```
<SwitchA> system-view
[SwitchA] lldp global enable
```

Enable LLDP and DCBX TLV advertising on Ten-GigabitEthernet 1/0/1.

```
[SwitchA] interface ten-gigabitethernet 1/0/1
[SwitchA-Ten-GigabitEthernet1/0/1] lldp enable
[SwitchA-Ten-GigabitEthernet1/0/1] lldp tlv-enable dot1-tlv dcbx
```

2. Set the DCBX version to Rev. 1.01 on Ten-GigabitEthernet 1/0/1.

```
[SwitchA-Ten-GigabitEthernet1/0/1] dcbx version rev101
[SwitchA-Ten-GigabitEthernet1/0/1] quit
```

3. Configure APP parameters:

Create Layer 2 ACL 4000.

```
[SwitchA] acl mac 4000
```

Configure ACL 4000 to permit FCoE frames (frame type is 0x8906) and FIP frames (frame type is 0x8914) to pass through.

```
[SwitchA-acl-mac-4000] rule permit type 8906 ffff
[SwitchA-acl-mac-4000] rule permit type 8914 ffff
[SwitchA-acl-mac-4000] quit
```

Create a class named **app_c**, set the operator of the class to OR, and use ACL 4000 as the match criterion of the class.

```
[SwitchA] traffic classifier app_c operator or
[SwitchA-classifier-app_c] if-match acl mac 4000
[SwitchA-classifier-app_c] quit
```

Create a traffic behavior named **app_b**, and configure the traffic behavior to mark packets with 802.1p priority value 3.

```
[SwitchA] traffic behavior app_b
[SwitchA-behavior-app_b] remark dot1p 3
[SwitchA-behavior-app_b] quit
```

Create a QoS policy named **plcy**, associate class **app_c** with traffic behavior **app_b** in the QoS policy, and apply the association to DCBX.

```
[SwitchA] qos policy plcy
[SwitchA-qospolicy-plcy] classifier app_c behavior app_b mode dcbx
[SwitchA-qospolicy-plcy] quit
```

Apply QoS policy **plcy** to the outgoing traffic of Ten-GigabitEthernet 1/0/1.

```
[SwitchA] interface ten-gigabitethernet 1/0/1
[SwitchA-Ten-GigabitEthernet1/0/1] qos apply policy plcy outbound
[SwitchA-Ten-GigabitEthernet1/0/1] quit
```

4. Configure ETS parameters:

Configure the 802.1p-to-local priority mapping table to map 802.1p priority value 3 to local precedence 3. (This is the default mapping table. You can modify this configuration as needed.)

```
[SwitchA] qos map-table outbound dot1p-lp
[SwitchA-maptbl-out-dot1p-lp] import 3 export 3
[SwitchA-maptbl-out-dot1p-lp] quit
```

Enable byte-count WRR queuing on Ten-GigabitEthernet 1/0/1, and configure queue 3 on the interface to use SP queuing.

```
[SwitchA] interface ten-gigabitethernet 1/0/1
[SwitchA-Ten-GigabitEthernet1/0/1] qos wrr byte-count
[SwitchA-Ten-GigabitEthernet1/0/1] qos wrr 3 group sp
```

5. Configure PFC:

   # Enable PFC in auto mode on Ten-GigabitEthernet 1/0/1.

   ```
   [SwitchA-Ten-GigabitEthernet1/0/1] priority-flow-control auto
   ```

   # Enable PFC for 802.1 priority 3.

   ```
   [SwitchA-Ten-GigabitEthernet1/0/1] priority-flow-control no-drop dot1p 3
   ```

Verifying the configuration

Display the data exchange result on the DC server through the software interface. This example uses the data exchange result for a QLogic adapter on the DC server.

```
-----------------------------------------------------
DCBX Parameters Details for CNA Instance 0 - QLE8142
-----------------------------------------------------

Mon May 17 10:00:50 2010

DCBX TLV (Type-Length-Value) Data
================================
DCBX Parameter Type and Length
        DCBX Parameter Length: 13
        DCBX Parameter Type: 2

DCBX Parameter Information
        Parameter Type: Current
        Pad Byte Present: Yes
        DCBX Parameter Valid: Yes
        Reserved: 0

DCBX Parameter Data
        Priority Group ID of Priority 1: 0
        Priority Group ID of Priority 0: 2

        Priority Group ID of Priority 3: 15
        Priority Group ID of Priority 2: 1

        Priority Group ID of Priority 5: 5
        Priority Group ID of Priority 4: 4

        Priority Group ID of Priority 7: 7
        Priority Group ID of Priority 6: 6

        Priority Group 0 Percentage: 2
        Priority Group 1 Percentage: 4
        Priority Group 2 Percentage: 6
        Priority Group 3 Percentage: 0
        Priority Group 4 Percentage: 10
        Priority Group 5 Percentage: 18
        Priority Group 6 Percentage: 27
        Priority Group 7 Percentage: 31
```

```
        Number of Traffic Classes Supported: 8

DCBX Parameter Information
        Parameter Type: Remote
        Pad Byte Present: Yes
        DCBX Parameter Valid: Yes
        Reserved: 0

DCBX Parameter Data
        Priority Group ID of Priority 1: 0
        Priority Group ID of Priority 0: 2

        Priority Group ID of Priority 3: 15
        Priority Group ID of Priority 2: 1

        Priority Group ID of Priority 5: 5
        Priority Group ID of Priority 4: 4

        Priority Group ID of Priority 7: 7
        Priority Group ID of Priority 6: 6

        Priority Group 0 Percentage: 2
        Priority Group 1 Percentage: 4
        Priority Group 2 Percentage: 6
        Priority Group 3 Percentage: 0
        Priority Group 4 Percentage: 10
        Priority Group 5 Percentage: 18
        Priority Group 6 Percentage: 27
        Priority Group 7 Percentage: 31

        Number of Traffic Classes Supported: 8

DCBX Parameter Information
        Parameter Type: Local
        Pad Byte Present: Yes
        DCBX Parameter Valid: Yes
        Reserved: 0

DCBX Parameter Data
        Priority Group ID of Priority 1: 0
        Priority Group ID of Priority 0: 0

        Priority Group ID of Priority 3: 1
        Priority Group ID of Priority 2: 0

        Priority Group ID of Priority 5: 0
        Priority Group ID of Priority 4: 0
```

```
        Priority Group ID of Priority 7: 0
        Priority Group ID of Priority 6: 0

        Priority Group 0 Percentage: 50
        Priority Group 1 Percentage: 50
        Priority Group 2 Percentage: 0
        Priority Group 3 Percentage: 0
        Priority Group 4 Percentage: 0
        Priority Group 5 Percentage: 0
        Priority Group 6 Percentage: 0
        Priority Group 7 Percentage: 0

        Number of Traffic Classes Supported: 2
```

The output shows that the DC server will use SP queuing (priority group ID 15) for 802.1p priority 3.

```
DCBX Parameter Type and Length
        DCBX Parameter Length: 2
        DCBX Parameter Type: 3

DCBX Parameter Information
        Parameter Type: Current
        Pad Byte Present: No
        DCBX Parameter Valid: Yes
        Reserved: 0

DCBX Parameter Data
        PFC Enabled on Priority 0: No
        PFC Enabled on Priority 1: No
        PFC Enabled on Priority 2: No
        PFC Enabled on Priority 3: Yes
        PFC Enabled on Priority 4: No
        PFC Enabled on Priority 5: No
        PFC Enabled on Priority 6: No
        PFC Enabled on Priority 7: No

        Number of Traffic Classes Supported: 6

DCBX Parameter Information
        Parameter Type: Remote
        Pad Byte Present: No
        DCBX Parameter Valid: Yes
        Reserved: 0

DCBX Parameter Data
        PFC Enabled on Priority 0: No
        PFC Enabled on Priority 1: No
        PFC Enabled on Priority 2: No
        PFC Enabled on Priority 3: Yes
        PFC Enabled on Priority 4: No
```

```
        PFC Enabled on Priority 5: No
        PFC Enabled on Priority 6: No
        PFC Enabled on Priority 7: No

        Number of Traffic Classes Supported: 6

DCBX Parameter Information
        Parameter Type: Local
        Pad Byte Present: No
        DCBX Parameter Valid: Yes
        Reserved: 0

DCBX Parameter Data
        PFC Enabled on Priority 0: No
        PFC Enabled on Priority 1: No
        PFC Enabled on Priority 2: No
        PFC Enabled on Priority 3: Yes
        PFC Enabled on Priority 4: No
        PFC Enabled on Priority 5: No
        PFC Enabled on Priority 6: No
        PFC Enabled on Priority 7: No

        Number of Traffic Classes Supported: 1
```

The output shows that the DC server will use PFC for 802.1p priority 3.