



Configuring Layer 2 Interfaces

This chapter contains the following sections:

- [Information About Ethernet Interfaces, page 1](#)
- [Carrier Delay, page 5](#)
- [Information About Ethernet Interfaces, page 5](#)
- [Information About Default Interfaces, page 8](#)
- [Information About Access and Trunk Interfaces, page 9](#)
- [Configuring Access and Trunk Interfaces, page 12](#)
- [Verifying the Interface Configuration, page 17](#)
- [Configuring Ethernet Interfaces, page 17](#)
- [Displaying Interface Information, page 35](#)
- [Default Physical Ethernet Settings, page 37](#)

Information About Ethernet Interfaces

The Ethernet ports can operate as standard Ethernet interfaces connected to servers or to a LAN.

The Ethernet interfaces are enabled by default.

Interface Command

You can enable the various capabilities of the Ethernet interfaces on a per-interface basis using the **interface** command. When you enter the **interface** command, you specify the following information:

- Interface type—All physical Ethernet interfaces use the **ethernet** keyword.
- Slot number
 - Slot 1—a fixed LEM.
 - Slot 2—a fixed LEM.

- Slot 3—a fixed LEM.
 - Slot 4—a fixed LEM.
 - Slot 5—a hot-swappable LEM (if populated)
 - Slot 6—a hot-swappable LEM (if populated)
 - Slot 7—a hot-swappable LEM (if populated)
 - Slot 8—a hot-swappable LEM (if populated)
- QSFP-module—This is used if the port is in breakout mode. For more information about breakout mode, see [Configuring Linecard Expansion Modules](#).
 - Port number— Port number within the group.

The interface numbering convention is extended to support use with a Cisco Nexus Fabric Extender as follows:

switch(config)# **interface ethernet** [*chassis*]/*slot/port*

- The chassis ID is an optional entry that you can use to address the ports of a connected Fabric Extender. The chassis ID is configured on a physical Ethernet or EtherChannel interface on the switch to identify the Fabric Extender discovered through the interface. The chassis ID ranges from 100 to 199.

The command syntax for the Linecard Expansion Module (LEM) is the following:

- In 40G mode: switch(config)# **interface ethernet** *slot/port*
- In 10G mode: switch(config)# **interface ethernet** *slot/QSFP-module/port*

Information About Unified Ports

Cisco Nexus unified ports allow you to configure a physical port on a Cisco Nexus device switch as a 1/10-Gigabit Ethernet, Fibre Channel over Ethernet (FCoE), or 2-, 4-, 8-Gigabit native Fibre Channel port.

Currently, most networks have two types of switches for different types of networks. For example, LAN switches carry Ethernet traffic up to Catalyst or Nexus switches carry FC traffic from servers to MDS switches. With unified port technology, you can deploy a unified platform, unified device, and unified wire approach. Unified ports allow you to move from an existing segregated platform approach where you choose LAN and SAN port options to transition to a single, unified fabric that is transparent and consistent with existing practices and management software. A unified fabric includes the following:

- Unified platform—Uses the same hardware platform and the same software code level and certifies it once for your LAN and SAN environments.
- Unified device—Runs LAN and SAN services on the same platform switch. The unified device allows you to connect your Ethernet and Fibre Channel cables to the same device.
- Unified wire—Converges LAN and SAN networks on a single converged network adapter (CNA) and connects them to your server.

A unified fabric allows you to manage Ethernet and FCoE features independently with existing Cisco tools.

Guidelines and Limitations for Unified Ports

- Ethernet ports and Fibre Channel ports must be configured in the following order:
 - Fibre Channel ports must be configured from the last port of the module.
 - Ethernet ports must be configured from the first port of the module.

If the order is not followed, the following errors are displayed:

```
ERROR: Ethernet range starts from first port of the module  
ERROR: FC range should end on last port of the module
```



Note

- All ports of same type (Fibre Channel or Ethernet) should be contiguous on the module.
- On a Cisco Nexus 5672UP switch, the Fibre Channel port range can be among 33-48, but must end at Port 48.
- On a Cisco Nexus 56128P switch, only the expansion modules in slot 2 and 3 support native FC type. On each module, the Fibre Channel port range can be among 1-24, but must start from Port 1.
- On a Cisco Nexus 5696Q switch, only M20UP expansion modules support native FC type. All 20 ports can be configured as native Fibre Channel ports, but port range must either start with 1 or end at 20.
- On a Cisco Nexus N5672, the Fibre Channel ports must be configured from the last port onwards.
- On a Cisco Nexus N56128 with N56-M24UP2Q LEMs, only the first 20 ports can be configured as Fibre Channel and this ports must be configured from the first port onwards.

Unidirectional Link Detection Parameter

The Cisco-proprietary Unidirectional Link Detection (UDLD) protocol allows ports that are connected through fiber optics or copper (for example, Category 5 cabling) Ethernet cables to monitor the physical configuration of the cables and detect when a unidirectional link exists. When the switch detects a unidirectional link, UDLD shuts down the affected LAN port and alerts the user. Unidirectional links can cause a variety of problems, including spanning tree topology loops.

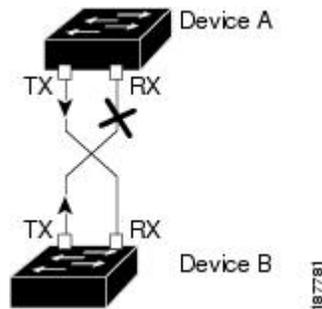
UDLD is a Layer 2 protocol that works with the Layer 1 protocols to determine the physical status of a link. At Layer 1, autonegotiation takes care of physical signaling and fault detection. UDLD performs tasks that autonegotiation cannot perform, such as detecting the identities of neighbors and shutting down misconnected LAN ports. When you enable both autonegotiation and UDLD, Layer 1 and Layer 2 detections work together to prevent physical and logical unidirectional connections and the malfunctioning of other protocols.

A unidirectional link occurs whenever traffic transmitted by the local device over a link is received by the neighbor but traffic transmitted from the neighbor is not received by the local device. If one of the fiber strands in a pair is disconnected, and if autonegotiation is active, the link does not stay up. In this case, the logical link is undetermined, and UDLD does not take any action. If both fibers are working normally at Layer 1, then UDLD at Layer 2 determines whether those fibers are connected correctly and whether traffic is flowing bidirectionally between the correct neighbors. This check cannot be performed by autonegotiation, because autonegotiation operates at Layer 1.

A Cisco Nexus device periodically transmits UDLD frames to neighbor devices on LAN ports with UDLD enabled. If the frames are echoed back within a specific time frame and they lack a specific acknowledgment (echo), the link is flagged as unidirectional and the LAN port is shut down. Devices on both ends of the link must support UDLD in order for the protocol to successfully identify and disable unidirectional links.

The following figure shows an example of a unidirectional link condition. Device B successfully receives traffic from Device A on the port. However, Device A does not receive traffic from Device B on the same port. UDLD detects the problem and disables the port.

Figure 1: Unidirectional Link



Default UDLD Configuration

The following table shows the default UDLD configuration.

Table 1: UDLD Default Configuration

| Feature | Default Value |
|--|---|
| UDLD global enable state | Globally disabled |
| UDLD aggressive mode | Disabled |
| UDLD per-port enable state for fiber-optic media | Enabled on all Ethernet fiber-optic LAN ports |
| UDLD per-port enable state for twisted-pair (copper) media | Enabled |

UDLD Aggressive and Nonaggressive Modes

UDLD aggressive mode is disabled by default. You can configure UDLD aggressive mode only on point-to-point links between network devices that support UDLD aggressive mode. If UDLD aggressive mode is enabled, when a port on a bidirectional link that has a UDLD neighbor relationship established stops receiving UDLD frames, UDLD tries to reestablish the connection with the neighbor. After eight failed retries, the port is disabled.

To prevent spanning tree loops, nonaggressive UDLD with the default interval of 15 seconds is fast enough to shut down a unidirectional link before a blocking port transitions to the forwarding state (with default spanning tree parameters).

When you enable the UDLD aggressive mode, the following occurs:

- One side of a link has a port stuck (both transmission and receive)
- One side of a link remains up while the other side of the link is down

In these cases, the UDLD aggressive mode disables one of the ports on the link, which prevents traffic from being discarded.

Interface Speed

The Cisco Nexus 6004 switch has default port in 40 Gigabit Ethernet mode. The port speed can be changed in group of 12 Quad Small Form-factor Pluggable (QSFP) ports. You need to reset the group after the port mode is changed. The hardware support is provided for port speed of every 3 QSFP interfaces.

Carrier Delay



Note

You can configure the carrier delay timer only on VLAN network interfaces. The timer cannot be configured on physical Ethernet interfaces, port channels, and loopback interfaces. See “Configuring Layer 3 Interfaces,” for information about configuring VLAN network interfaces.

If a link goes down and comes back up before the carrier delay timer expires, the down state is effectively filtered, and the rest of the software on the device is not aware that a link-down event occurred. A large carrier delay timer results in fewer link-up/link-down events being detected. When you set the carrier delay time to 0, the device detects each link-up/link-down event that occurs.

In most environments, a lower carrier delay time is better than a higher one. The exact value that you choose depends on the nature of the link outages and how long you expect these linkages to last in your network. If your data links are subject to short outages (especially if those outages last less time than it takes for your IP routing to converge), you should set a long carrier delay value to prevent these short outages from causing unnecessary problems in your routing tables. However, if your outages tend to be longer, you might want to set a shorter carrier delay time so that the outages are detected sooner, and the IP route convergence begins and ends sooner. The default carrier-delay time is 100 milliseconds.

Information About Ethernet Interfaces

The Ethernet ports can operate as standard Ethernet interfaces connected to servers or to a LAN.

The Ethernet interfaces are enabled by default.

Cisco Discovery Protocol

The Cisco Discovery Protocol (CDP) is a device discovery protocol that runs over Layer 2 (the data link layer) on all Cisco-manufactured devices (routers, bridges, access servers, and switches) and allows network management applications to discover Cisco devices that are neighbors of already known devices. With CDP, network management applications can learn the device type and the Simple Network Management Protocol

(SNMP) agent address of neighboring devices that are running lower-layer, transparent protocols. This feature enables applications to send SNMP queries to neighboring devices.

CDP runs on all media that support Subnetwork Access Protocol (SNAP). Because CDP runs over the data-link layer only, two systems that support different network-layer protocols can learn about each other.

Each CDP-configured device sends periodic messages to a multicast address, advertising at least one address at which it can receive SNMP messages. The advertisements also contain time-to-live, or holdtime information, which is the length of time a receiving device holds CDP information before discarding it. Each device also listens to the messages sent by other devices to learn about neighboring devices.

The switch supports both CDP Version 1 and Version 2.

Default CDP Configuration

The following table shows the default CDP configuration.

Table 2: Default CDP Configuration

| Feature | Default Setting |
|-------------------------------------|-----------------|
| CDP interface state | Enabled |
| CDP timer (packet update frequency) | 60 seconds |
| CDP holdtime (before discarding) | 180 seconds |
| CDP Version-2 advertisements | Enabled |

Error-Disabled State

An interface is in the error-disabled (err-disabled) state when the interface is enabled administratively (using the **no shutdown** command) but disabled at runtime by any process. For example, if UDLD detects a unidirectional link, the interface is shut down at runtime. However, because the interface is administratively enabled, the interface status displays as err-disabled. Once an interface goes into the err-disabled state, you must manually reenabling it or you can configure an automatic timeout recovery value. The err-disabled detection is enabled by default for all causes. The automatic recovery is not configured by default.

When an interface is in the err-disabled state, use the **errdisable detect cause** command to find information about the error.

You can configure the automatic err-disabled recovery timeout for a particular err-disabled cause by changing the time variable.

The **errdisable recovery cause** command provides automatic recovery after 300 seconds. To change the recovery period, use the **errdisable recovery interval** command to specify the timeout period. You can specify 30 to 65535 seconds.

If you do not enable the err-disabled recovery for the cause, the interface stays in the err-disabled state until you enter the **shutdown** and **no shutdown** commands. If the recovery is enabled for a cause, the interface is brought out of the err-disabled state and allowed to retry operation once all the causes have timed out. Use the **show interface status err-disabled** command to display the reason behind the error.

About Port Profiles

You can create a port profile that contains many interface commands and apply that port profile to a range of interfaces on the . Port profiles can be applied to the following interface types:

- Ethernet
- VLAN network interface
- Port channel

A command that is included in a port profile can be configured outside of the port profile. If the new configuration in the port profile conflicts with the configurations that exist outside the port profile, the commands configured for an interface in configuration terminal mode have higher priority than the commands in the port profile. If changes are made to the interface configuration after a port profile is attached to it, and the configuration conflicts with that in the port profile, the configurations in the interface will be given priority.

You inherit the port profile when you attach the port profile to an interface or range of interfaces. When you attach, or inherit, a port profile to an interface or range of interfaces, the switch applies all the commands in that port profile to the interfaces.

You can have one port profile inherit the settings from another port profile. Inheriting another port profile allows the initial port profile to assume all of the commands of the second, inherited, port profile that do not conflict with the initial port profile. Four levels of inheritance are supported. The same port profile can be inherited by any number of port profiles.

To apply the port profile configurations to the interfaces, you must enable the specific port profile. You can configure and inherit a port profile onto a range of interfaces prior to enabling the port profile; you then enable that port profile for the configurations to take effect on the specified interfaces.

When you remove a port profile from a range of interfaces, the switch undoes the configuration from the interfaces first and then removes the port profile link itself. When you remove a port profile, the switch checks the interface configuration and either skips the port profile commands that have been overridden by directly entered interface commands or returns the command to the default value.

If you want to delete a port profile that has been inherited by other port profiles, you must remove the inheritance before you can delete the port profile.

You can choose a subset of interfaces from which to remove a port profile from among that group of interfaces that you originally applied the profile. For example, if you configured a port profile and configured ten interfaces to inherit that port profile, you can remove the port profile from just some of the specified ten interfaces. The port profile continues to operate on the remaining interfaces to which it is applied.

If you delete a specific configuration for a specified range of interfaces using the interface configuration mode, that configuration is also deleted from the port profile for that range of interfaces only. For example, if you have a channel group inside a port profile and you are in the interface configuration mode and you delete that port channel, the specified port channel is also deleted from the port profile as well.

After you inherit a port profile on an interface or range of interfaces and you delete a specific configuration value, that port profile configuration will not operate on the specified interfaces.

If you attempt to apply a port profile to the wrong type of interface, the switch returns an error.

When you attempt to enable, inherit, or modify a port profile, the switch creates a checkpoint. If the port profile configuration fails, the switch rolls back to the prior configuration and returns an error. A port profile is never only partially applied.

Guidelines and Limitations for Port Profiles

Port profiles have the following configuration guidelines and limitations:

- Each port profile must have a unique name across interface types and the network.
- Commands that you enter under the interface mode take precedence over the port profile's commands if there is a conflict. However, the port profile retains that command in the port profile.
- The port profile's commands take precedence over the default commands on the interface, unless the default command explicitly overrides the port profile command.
- After you inherit a port profile onto an interface or range of interfaces, you can override individual configuration values by entering the new value at the interface configuration level. If you remove the individual configuration values at the interface configuration level, the interface uses the values in the port profile again.
- There are no default configurations associated with a port profile.
- A subset of commands are available under the port profile configuration mode, depending on which interface type that you specify.
- You cannot use port profiles with Session Manager.

Debounce Timer Parameters

MTU Configuration

The Cisco Nexus device switch does not fragment frames. As a result, the switch cannot have two ports in the same Layer 2 domain with different maximum transmission units (MTUs). A per-physical Ethernet interface MTU is not supported. Instead, the MTU is set according to the QoS classes. You modify the MTU by setting class and policy maps.

**Note**

When you show the interface settings, a default MTU of 1500 is displayed for physical Ethernet interfaces.

Information About Default Interfaces

You can use the default interface feature to clear the configured parameters for both physical and logical interfaces such as the Ethernet, loopback, VLAN network, and the port-channel interface.

The default interface feature allows you to clear the existing configuration of multiple interfaces such as Ethernet, loopback, VLAN network, and port-channel interfaces. All user configuration under a specified interface will be deleted. You can optionally create a checkpoint before clearing the interface configuration so that you can later restore the deleted configuration.

**Note**

The default interfaces feature is supported for management interfaces but is not recommended because the device might be in an unreachable state.

Information About Access and Trunk Interfaces

Understanding Access and Trunk Interfaces

Ethernet interfaces can be configured either as access ports or a trunk ports, as follows:

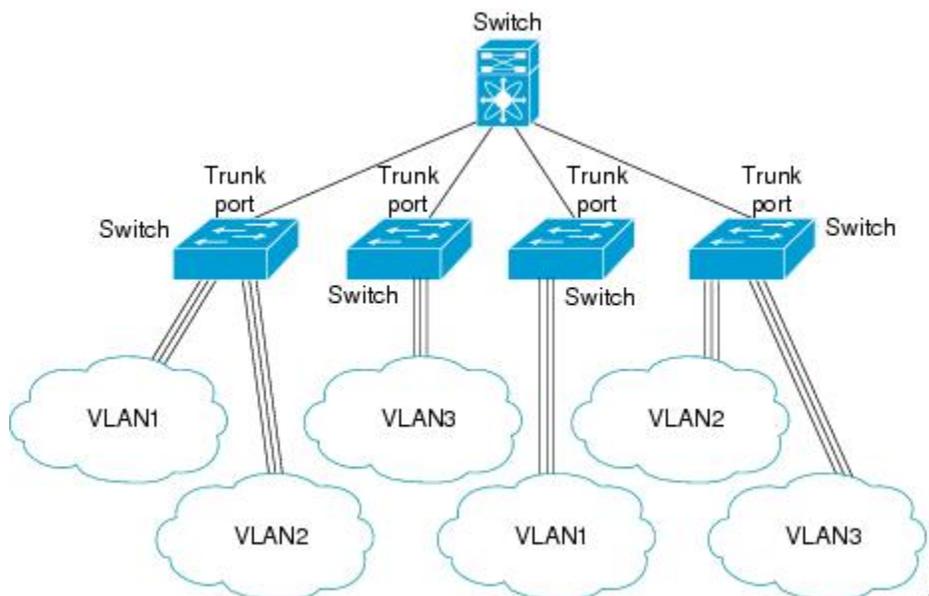
- An access port can have only one VLAN configured on the interface; it can carry traffic for only one VLAN.
- A trunk port can have two or more VLANs configured on the interface; it can carry traffic for several VLANs simultaneously.

**Note**

Cisco NX-OS supports only IEEE 802.1Q-type VLAN trunk encapsulation.

The following figure shows how you can use trunk ports in the network. The trunk port carries traffic for two or more VLANs.

Figure 2: Devices in a Trunking Environment



In order to correctly deliver the traffic on a trunk port with several VLANs, the device uses the IEEE 802.1Q encapsulation or tagging method.

To optimize the performance on access ports, you can configure the port as a host port. Once the port is configured as a host port, it is automatically set as an access port, and channel grouping is disabled. Use the host designation to decrease the time it takes the designated port to begin to forward packets.



Note Only an end station can be set as a host port; you will receive an error message if you attempt to configure other ports as hosts.

If an access port receives a packet with an 802.1Q tag in the header other than the access VLAN value, that port drops the packet without learning its MAC source address.



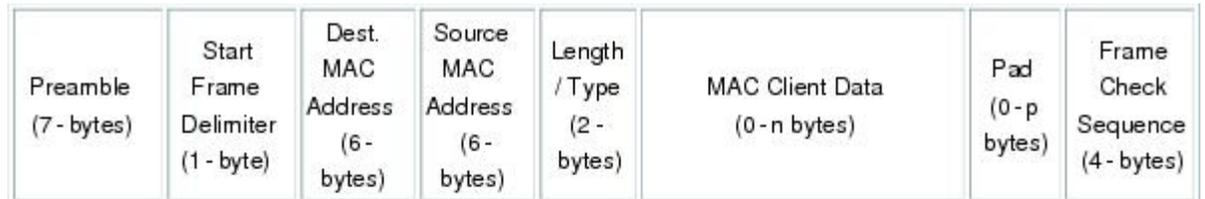
Note An Ethernet interface can function as either an access port or a trunk port; it cannot function as both port types simultaneously.

Understanding IEEE 802.1Q Encapsulation

A trunk is a point-to-point link between the device and another networking device. Trunks carry the traffic of multiple VLANs over a single link and allow you to extend VLANs across an entire network.

To correctly deliver the traffic on a trunk port with several VLANs, the device uses the IEEE 802.1Q encapsulation (tagging) method. This tag carries information about the specific VLAN to which the frame and packet belong. This method allows packets that are encapsulated for several different VLANs to traverse the same port and maintain traffic separation between the VLANs.

Figure 3: Header Without and With 802.1Q Tag Included



3 bits = User Priority field
 1 bit = Canonical Format Identifier (CFI)
 12 bits = VLAN Identifier (VLAN ID)

183779

Understanding Access VLANs

When you configure a port in access mode, you can specify which VLAN will carry the traffic for that interface. If you do not configure the VLAN for a port in access mode, or an access port, the interface carries traffic for the default VLAN (VLAN1).

You can change the access port membership in a VLAN by specifying the new VLAN. You must create the VLAN before you can assign it as an access VLAN for an access port. If you change the access VLAN on an access port to a VLAN that is not yet created, the system will shut that access port down.



Note If you change the VLAN on an access port or a trunk port it will flap the interface. However, if the port is part of a vPC, then first change the native VLAN on the secondary vPC, and then to primary vPC.

If an access port receives a packet with an 802.1Q tag in the header other than the access VLAN value, that port drops the packet without learning its MAC source address.



Note If you assign an access VLAN that is also a primary VLAN for a private VLAN, all access ports with that access VLAN will also receive all the broadcast traffic for the primary VLAN in the private VLAN mode.

Understanding the Native VLAN ID for Trunk Ports

A trunk port can carry untagged packets simultaneously with the 802.1Q tagged packets. When you assign a default port VLAN ID to the trunk port, all untagged traffic travels on the default port VLAN ID for the trunk port, and all untagged traffic is assumed to belong to this VLAN. This VLAN is referred to as the native VLAN ID for a trunk port. The native VLAN ID is the VLAN that carries untagged traffic on trunk ports.

The trunk port sends an egressing packet with a VLAN that is equal to the default port VLAN ID as untagged; all the other egressing packets are tagged by the trunk port. If you do not configure a native VLAN ID, the trunk port uses the default VLAN.



Note Native VLAN ID numbers *must* match on both ends of the trunk.

Understanding Allowed VLANs

By default, a trunk port sends traffic to and receives traffic from all VLANs. All VLAN IDs are allowed on each trunk. However, you can remove VLANs from this inclusive list to prevent traffic from the specified VLANs from passing over the trunk. You can add any specific VLANs later that you may want the trunk to carry traffic for back to the list.

To partition the Spanning Tree Protocol (STP) topology for the default VLAN, you can remove VLAN1 from the list of allowed VLANs. Otherwise, VLAN1, which is enabled on all ports by default, will have a very big STP topology, which can result in problems during STP convergence. When you remove VLAN1, all data traffic for VLAN1 on this port is blocked, but the control traffic continues to move on the port.

Understanding Native 802.1Q VLANs

To provide additional security for traffic passing through an 802.1Q trunk port, the **vlan dot1q tag native** command was introduced. This feature provides a means to ensure that all packets going out of a 802.1Q trunk port are tagged and to prevent reception of untagged packets on the 802.1Q trunk port.

Without this feature, all tagged ingress frames received on a 802.1Q trunk port are accepted as long as they fall inside the allowed VLAN list and their tags are preserved. Untagged frames are tagged with the native VLAN ID of the trunk port before further processing. Only those egress frames whose VLAN tags are inside the allowed range for that 802.1Q trunk port are received. If the VLAN tag on a frame happens to match that of the native VLAN on the trunk port, the tag is stripped off and the frame is sent untagged.

This behavior could potentially be exploited to introduce "VLAN hopping" in which a hacker could try and have a frame jump to a different VLAN. It is also possible for traffic to become part of the native VLAN by sending untagged packets into an 802.1Q trunk port.

To address the above issues, the **vlan dot1q tag native** command performs the following functions:

- On the ingress side, all untagged data traffic is dropped.
- On the egress side, all traffic is tagged. If traffic belongs to native VLAN it is tagged with the native VLAN ID.

This feature is supported on all the directly connected Ethernet and Port Channel interfaces. It is also supported on all the host interface ports of any attached Fabric Extender (FEX).



Note

You can enable the **vlan dot1q tag native** command by entering the command in the global configuration mode.

Configuring Access and Trunk Interfaces

Configuring a LAN Interface as an Ethernet Access Port

You can configure an Ethernet interface as an access port. An access port transmits packets on only one, untagged VLAN. You specify which VLAN traffic that the interface carries. If you do not specify a VLAN for an access port, the interface carries traffic only on the default VLAN. The default VLAN is VLAN1.

The VLAN must exist before you can specify that VLAN as an access VLAN. The system shuts down an access port that is assigned to an access VLAN that does not exist.

Procedure

| | Command or Action | Purpose |
|--------|-----------------------------------|-----------------------------------|
| Step 1 | switch# configure terminal | Enters global configuration mode. |

| | Command or Action | Purpose |
|---------------|---|---|
| Step 2 | switch(config)# interface {{ <i>type slot/port</i> } { port-channel number }} | Specifies an interface to configure, and enters interface configuration mode. Note If this is a 10G breakout port, the <i>slot/port</i> syntax is <i>slot/QSFP-module/port</i> . |
| Step 3 | switch(config-if)# switchport mode { access trunk } | Sets the interface as a nontrunking nontagged single-VLAN Ethernet interface. An access port can carry traffic in one VLAN only. By default, an access port carries traffic for VLAN1; to set the access port to carry traffic for a different VLAN, use the switchport access vlan command. |
| Step 4 | switch(config-if)# switchport access vlan <i>vlan-id</i> | Specifies the VLAN for which this access port will carry traffic. If you do not enter this command, the access port carries traffic on VLAN1 only; use this command to change the VLAN for which the access port carries traffic. |

This example shows how to set an interface as an Ethernet access port that carries traffic for a specific VLAN only:

```
switch# configure terminal
switch(config)# interface ethernet 1/10
switch(config-if)# switchport mode access
switch(config-if)# switchport access vlan 5
```

Configuring Access Host Ports

By using a switchport host, you can make an access port a spanning-tree edge port, and enable BPDU Filtering and BPDU Guard at the same time.

Before You Begin

Ensure that you are configuring the correct interface; it must be an interface that is connected to an end station.

Procedure

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | switch# configure terminal | Enters global configuration mode. |
| Step 2 | switch(config)# interface <i>type slot/port</i> | Specifies an interface to configure, and enters interface configuration mode. Note If this is a 10G breakout port, the <i>slot/port</i> syntax is <i>slot/QSFP-module/port</i> . |
| Step 3 | switch(config-if)# switchport host | Sets the interface to spanning-tree port type edge, turns on BPDU Filtering and BPDU Guard. Note Apply this command only to switchports that connect to hosts. |

| | Command or Action | Purpose |
|--|-------------------|---------|
|--|-------------------|---------|

This example shows how to set an interface as an Ethernet access host port with EtherChannel disabled:

```
switch# configure terminal
switch(config)# interface ethernet 1/10
switch(config-if)# switchport host
```

Configuring Trunk Ports

You can configure an Ethernet port as a trunk port; a trunk port transmits untagged packets for the native VLAN plus encapsulated, tagged, packets for multiple VLANs.



Note

Cisco NX-OS supports only 802.1Q encapsulation.

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | switch# configure terminal | Enters global configuration mode. |
| Step 2 | switch(config)# interface { <i>type slot/port</i> port-channel number } | Specifies an interface to configure, and enters interface configuration mode. Note If this is a 10G breakout port, the <i>slot/port</i> syntax is <i>slot/QSFP-module/port</i> . |
| Step 3 | switch(config-if)# switchport mode { access trunk } | Sets the interface as an Ethernet trunk port. A trunk port can carry traffic in one or more VLANs on the same physical link (VLANs are based on the trunk-allowed VLANs list). By default, a trunk interface can carry traffic for all VLANs. To specify that only certain VLANs are allowed on the specified trunk, use the switchport trunk allowed vlan command. |

This example shows how to set an interface as an Ethernet trunk port:

```
switch# configure terminal
switch(config)# interface ethernet 1/3
switch(config-if)# switchport mode trunk
```

Configuring the Native VLAN for 802.1Q Trunking Ports

If you do not configure this parameter, the trunk port uses the default VLAN as the native VLAN ID.

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | switch# configure terminal | Enters global configuration mode. |
| Step 2 | switch(config)# interface { <i>type slot/port</i> port-channel number } | Specifies an interface to configure, and enters interface configuration mode. Note If this is a 10G breakout port, the <i>slot/port</i> syntax is <i>slot/QSFP-module/port</i> . |
| Step 3 | switch(config-if)# switchport trunk native vlan <i>vlan-id</i> | Sets the native VLAN for the 802.1Q trunk. Valid values are from 1 to 4094, except those VLANs reserved for internal use. The default value is VLAN1. |

This example shows how to set the native VLAN for an Ethernet trunk port:

```
switch# configure terminal
switch(config)# interface ethernet 1/3
switch(config-if)# switchport trunk native vlan 5
```

Configuring the Allowed VLANs for Trunking Ports

You can specify the IDs for the VLANs that are allowed on the specific trunk port.

Before you configure the allowed VLANs for the specified trunk ports, ensure that you are configuring the correct interfaces and that the interfaces are trunks.

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | switch# configure terminal | Enters global configuration mode. |
| Step 2 | switch(config)# interface { <i>type slot/port</i> port-channel number } | Specifies an interface to configure, and enters interface configuration mode. Note If this is a 10G breakout port, the <i>slot/port</i> syntax is <i>slot/QSFP-module/port</i> . |
| Step 3 | switch(config-if)# switchport trunk allowed vlan { <i>vlan-list all</i> none [add except none remove { <i>vlan-list</i> }]} | Sets allowed VLANs for the trunk interface. The default is to allow all VLANs on the trunk interface: 1 to 3967 and 4048 to 4094. VLANs 3968 to 4047 are the default VLANs reserved for internal use by default; this group of VLANs is configurable. By default, all VLANs are allowed on all trunk interfaces. Note You cannot add internally allocated VLANs as allowed VLANs on trunk ports. The system returns a message if you attempt to list an internally allocated VLAN as an allowed VLAN. |

This example shows how to add VLANs to the list of allowed VLANs on an Ethernet trunk port:

```
switch# configure terminal
switch(config)# interface ethernet 1/3
switch(config-if)# switchport trunk allow vlan 15-20
```

Configuring Native 802.1Q VLANs

Typically, you configure 802.1Q trunks with a native VLAN ID, which strips tagging from all packets on that VLAN. This configuration allows all untagged traffic and control traffic to transit the Cisco Nexus device. Packets that enter the switch with 802.1Q tags that match the native VLAN ID value are similarly stripped of tagging.

To maintain the tagging on the native VLAN and drop untagged traffic, enter the **vlan dot1q tag native** command. The switch will tag the traffic received on the native VLAN and admit only 802.1Q-tagged frames, dropping any untagged traffic, including untagged traffic in the native VLAN.

Control traffic continues to be accepted untagged on the native VLAN on a trunked port, even when the **vlan dot1q tag native** command is enabled.



Note

The **vlan dot1q tag native** command is enabled on global basis.

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | switch# configure terminal | Enters global configuration mode. |
| Step 2 | switch(config)# vlan dot1q tag native [tx-only] | Enables dot1q (IEEE 802.1Q) tagging for all native VLANs on all trunked ports on the Cisco Nexus device. By default, this feature is disabled. |
| Step 3 | switch(config)# no vlan dot1q tag native [tx-only] | (Optional) Disables dot1q (IEEE 802.1Q) tagging for all native VLANs on all trunked ports on the switch. |
| Step 4 | switch# show vlan dot1q tag native | (Optional) Displays the status of tagging on the native VLANs. |

This example shows how to enable 802.1Q tagging on the switch:

```
switch# configure terminal
switch(config)# vlan dot1q tag native
switch(config)# exit
switch# show vlan dot1q tag native
vlan dot1q native tag is enabled
```

Verifying the Interface Configuration

Use the following commands to display access and trunk interface configuration information.

| Command | Purpose |
|--|--|
| switch# show interface | Displays the interface configuration |
| switch# show interface switchport | Displays information for all Ethernet interfaces, including access and trunk interfaces. |
| switch# show interface brief | Displays interface configuration information. |

Configuring Ethernet Interfaces

The section includes the following topics:

Configuring Unified Ports

Before You Begin

Confirm that you have a supported Cisco Nexus switch. Unified Ports are available on the following Cisco Nexus switches:

- Cisco Nexus 5672UP
- Cisco Nexus 56128P with N56-M24UP2Q LEMs
- Cisco Nexus 5696Q with N5696-M20UP LEMs
- Cisco Nexus 6000
- Cisco Nexus 6004 Unified 20 x 10GE Eth/FCoE or 8/4/2Gbps Fibre Channel
- Cisco Nexus 6004 with M6004X-20UP LEMs

If you're configuring a unified port as Fibre Channel or FCoE, confirm that you have enabled the **feature fcoe** command.

Procedure

| | Command or Action | Purpose |
|---------------|--|------------------------------------|
| Step 1 | switch# configure terminal | Enters global configuration mode. |
| Step 2 | switch(config) # slot slot number | Identifies the slot on the switch. |

| | Command or Action | Purpose |
|---------------|--|--|
| Step 3 | <code>switch(config-slot) # port port number type {ethernet fc}</code> | <p>Configures a unified port as a native Fibre Channel port and an Ethernet port.</p> <ul style="list-style-type: none"> • type—Specifies the type of port to configure on a slot in a chassis. • ethernet—Specifies an Ethernet port. • fc—Specifies a Fibre Channel (FC) port. <p>Note Changing unified ports on an expansion module (GEM) requires that you power cycle the GEM card. You do not have to reboot the entire switch for changes to take effect.</p> <p>Note When configuring an FC port on N5672-16G, the fabric mode should be in the 40-G mode to support 16-G. When the ports are changed from Ethernet to FC, the fabric mode changes to 40-G on the next reload.</p> <p>When the ports are changed to FC for the first time, the following message is displayed: "Port type is changed. Fabric mode is also changed. Please copy configuration and reload the switch."</p> |
| Step 4 | <code>switch(config-slot) # copy running-config startup-config</code> | Copies the running configuration to the startup configuration. |
| Step 5 | <code>switch(config-slot) # reload</code> | Reboots the switch. |
| Step 6 | <code>switch(config) # no port port number type fc</code> | Removes the unified port. |

This example shows how to configure a unified port on a Cisco Nexus 5000 and Cisco Nexus 6000 series Switches:

```
switch# configure terminal
switch(config)# slot 1
switch(config-slot)# port 32 type fc
switch(config-slot)# copy running-config startup-config
switch(config-slot)# reload
```

This example shows how to configure 20 ports as Ethernet ports and 12 as FC ports:

```
switch# configure terminal
switch(config)# slot 1
switch(config-slot)# port 21-32 type fc
switch(config-slot)# copy running-config startup-config
switch(config-slot)# reload
```

This example shows how to configure a unified port on a Cisco N55-M16UP expansion module:

```
switch# configure terminal
switch(config)# slot 2
switch(config-slot)# port 16 type fc
switch(config-slot)# copy running-config startup-config
switch(config-slot)# poweroff module 2
switch(config-slot)# no poweroff module 2
```

Configuring the UDLD Mode

You can configure normal or aggressive unidirectional link detection (UDLD) modes for Ethernet interfaces on devices configured to run UDLD. Before you can enable a UDLD mode for an interface, you must make sure that UDLD is already enabled on the device that includes the interface. UDLD must also be enabled on the other linked interface and its device.

To use the normal UDLD mode, you must configure one of the ports for normal mode and configure the other port for the normal or aggressive mode. To use the aggressive UDLD mode, you must configure both ports for the aggressive mode.


Note

Before you begin, UDLD must be enabled for the other linked port and its device.

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | switch# configure terminal | Enters global configuration mode. |
| Step 2 | switch(config)# feature udld | Enables UDLD for the device. |
| Step 3 | switch(config)# no feature udld | Disables UDLD for the device. |
| Step 4 | switch(config)# show udld global | Displays the UDLD status for the device. |
| Step 5 | switch(config)# interface <i>type slot/port</i> | Specifies an interface to configure, and enters interface configuration mode. Note If this is a 10G breakout port, the <i>slot/port</i> syntax is <i>slot/QSFP-module/port</i> . |
| Step 6 | switch(config-if)# udld { enable disable aggressive } | Enables the normal UDLD mode, disables UDLD, or enables the aggressive UDLD mode. |
| Step 7 | switch(config-if)# show udld interface | Displays the UDLD status for the interface. |

This example shows how to enable UDLD for the switch:

```
switch# configure terminal
switch(config)# feature udld
```

This example shows how to enable the normal UDLD mode for an Ethernet port:

```
switch# configure terminal
switch(config)# interface ethernet 1/4
switch(config-if)# udld enable
```

This example shows how to enable the aggressive UDLD mode for an Ethernet port:

```
switch# configure terminal
switch(config)# interface ethernet 1/4
```

```
switch(config-if)# udld aggressive
```

This example shows how to disable UDLD for an Ethernet port:

```
switch# configure terminal
switch(config)# interface ethernet 1/4
switch(config-if)# udld disable
```

This example shows how to disable UDLD for the switch:

```
switch# configure terminal
switch(config)# no feature udld
```

Disabling Link Negotiation

You can disable link negotiation using the **no negotiate auto** command. By default, auto-negotiation is enabled on 1-Gigabit ports and disabled on 10-Gigabit ports.

This command is equivalent to the Cisco IOS **speed non-negotiate** command.



Note

The auto-negotiation configuration is not applicable on 10-Gigabit Ethernet ports. When auto-negotiation is configured on a 10-Gigabit port, the following error message is displayed:

```
ERROR: Ethernet1/40: Configuration does not match the port capability
```

Procedure

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | switch# configure terminal | Enters global configuration mode. |
| Step 2 | switch(config)# interface ethernet slot/port | Selects the interface and enters interface mode. Note If this is a 10G breakout port, the <i>slot/port</i> syntax is <i>slot/QSFP-module/port</i> . |
| Step 3 | switch(config-if)# no negotiate auto | Disables link negotiation on the selected Ethernet interface (1-Gigabit port). |
| Step 4 | switch(config-if)# negotiate auto | (Optional) Enables link negotiation on the selected Ethernet interface. The default for 1-Gigabit Ethernet ports is enabled. Note This command is not applicable for 10GBASE-T ports. It should not be used on 10-GBASE-T ports. |

This example shows how to disable auto-negotiation on a specified Ethernet interface (1-Gigabit port):

```
switch# configure terminal
switch(config)# interface ethernet 1/1
switch(config-if)# no negotiate auto
switch(config-if)#
```

This example shows how to enable auto-negotiation on a specified Ethernet interface (1-Gigabit port):

```
switch# configure terminal
switch(config)# interface ethernet 1/5
switch(config-if)# negotiate auto
switch(config-if)#
```

Configuring the CDP Characteristics

You can configure the frequency of Cisco Discovery Protocol (CDP) updates, the amount of time to hold the information before discarding it, and whether or not to send Version-2 advertisements.

Procedure

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | switch# configure terminal | Enters global configuration mode. |
| Step 2 | switch(config)# [no] cdp advertise {v1 v2 } | (Optional) Configures the version to use to send CDP advertisements. Version-2 is the default state. Use the no form of the command to return to its default setting. |
| Step 3 | switch(config)# [no] cdp format device-id {mac-address serial-number system-name } | (Optional) Configures the format of the CDP device ID. The default is the system name, which can be expressed as a fully qualified domain name. Use the no form of the command to return to its default setting. |
| Step 4 | switch(config)# [no] cdp holdtime <i>seconds</i> | (Optional) Specifies the amount of time a receiving device should hold the information sent by your device before discarding it. The range is 10 to 255 seconds; the default is 180 seconds. Use the no form of the command to return to its default setting. |
| Step 5 | switch(config)# [no] cdp timer <i>seconds</i> | (Optional) Sets the transmission frequency of CDP updates in seconds. The range is 5 to 254; the default is 60 seconds. Use the no form of the command to return to its default setting. |

This example shows how to configure CDP characteristics:

```
switch# configure terminal
switch(config)# cdp timer 50
switch(config)# cdp holdtime 120
switch(config)# cdp advertise v2
```

Enabling or Disabling CDP

You can enable or disable CDP for Ethernet interfaces. This protocol works only when you have it enabled on both interfaces on the same link.

Procedure

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | switch# configure terminal | Enters global configuration mode. |
| Step 2 | switch(config)# interface type slot/port | Enters interface configuration mode for the specified interface. Note If this is a 10G breakout port, the <i>slot/port</i> syntax is <i>slot/QSFP-module/port</i> . |
| Step 3 | switch(config-if)# cdp enable | Enables CDP for the interface. To work correctly, this parameter must be enabled for both interfaces on the same link. |
| Step 4 | switch(config-if)# no cdp enable | Disables CDP for the interface. |

This example shows how to enable CDP for an Ethernet port:

```
switch# configure terminal
switch(config)# interface ethernet 1/4
switch(config-if)# cdp enable
```

This command can only be applied to a physical Ethernet interface.

Enabling the Error-Disabled Detection

You can enable error-disable (err-disabled) detection in an application. As a result, when a cause is detected on an interface, the interface is placed in an err-disabled state, which is an operational state that is similar to the link-down state.

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | switch# configure terminal | Enters global configuration mode. |
| Step 2 | switch(config)# errdisable detect cause {all link-flap loopback} | Specifies a condition under which to place the interface in an err-disabled state. The default is enabled. |
| Step 3 | switch(config)# shutdown | Brings the interface down administratively. To manually recover the interface from the err-disabled state, enter this command first. |

| | Command or Action | Purpose |
|---------------|---|---|
| Step 4 | switch(config)# no shutdown | Brings the interface up administratively and enables the interface to recover manually from the err-disabled state. |
| Step 5 | switch(config)# show interface status err-disabled | Displays information about err-disabled interfaces. |
| Step 6 | switch(config)# copy running-config startup-config | (Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration. |

This example shows how to enable the err-disabled detection in all cases:

```
switch# configure terminal
switch(config)# errdisable detect cause all
switch(config)# shutdown
switch(config)# no shutdown
switch(config)# show interface status err-disabled
switch(config)# copy running-config startup-config
```

Enabling the Error-Disabled Recovery

You can specify the application to bring the interface out of the error-disabled (err-disabled) state and retry coming up. It retries after 300 seconds, unless you configure the recovery timer (see the **errdisable recovery interval** command).

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | switch# configure terminal | Enters global configuration mode. |
| Step 2 | switch(config)# errdisable recovery cause {all udld bpduguard link-flap failed-port-state pause-rate-limit} | Specifies a condition under which the interface automatically recovers from the err-disabled state, and the device retries bringing the interface up. The device waits 300 seconds to retry. The default is disabled. |
| Step 3 | switch(config)# show interface status err-disabled | Displays information about err-disabled interfaces. |
| Step 4 | switch(config)# copy running-config startup-config | (Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration. |

This example shows how to enable err-disabled recovery under all conditions:

```
switch# configure terminal
switch(config)# errdisable recovery cause all
switch(config)# show interface status err-disabled
switch(config)# copy running-config startup-config
```

Configuring the Error-Disabled Recovery Interval

You can use this procedure to configure the err-disabled recovery timer value. The range is from 30 to 65535 seconds. The default is 300 seconds.

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | switch# configure terminal | Enters global configuration mode. |
| Step 2 | switch(config)# errdisable recovery interval interval | Specifies the interval for the interface to recover from the err-disabled state. The range is from 30 to 65535 seconds. The default is 300 seconds. |
| Step 3 | switch(config)# show interface status err-disabled | Displays information about err-disabled interfaces. |
| Step 4 | switch(config)# copy running-config startup-config | (Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration. |

This example shows how to enable err-disabled recovery under all conditions:

```
switch# configure terminal
switch(config)# errdisable recovery interval 32
switch(config)# show interface status err-disabled
switch(config)# copy running-config startup-config
```

Port Profiles

Creating a Port Profile

You can create a port profile on the switch. Each port profile must have a unique name across interface types and the network.

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | configure terminal Example: switch# configure terminal switch(config)# | Enters configuration mode. |
| Step 2 | port-profile [type {ethernet interface-vlan port channel}] name Example: switch(config)# port-profile type ethernet test switch(config-port-prof)# | Creates and names a port profile for the specified type of interface and enters the port profile configuration mode. |
| Step 3 | exit Example: switch(config-port-prof)# exit switch(config)# | Exits port profile configuration mode. |
| Step 4 | show port-profile Example: switch(config)# show port-profile name | (Optional) Displays the port profile configuration. |
| Step 5 | copy running-config startup-config Example: switch(config)# copy running-config startup-config | (Optional) Copies the running configuration to the startup configuration. |

This example shows how to create a port profile named test for Ethernet interfaces:

```
switch# configure terminal
switch(config)# port-profile type ethernet test
switch(config-port-prof)#
```

This example shows how to add the interface commands to a port profile named ppEth configured for Ethernet interfaces:

```
switch# configure terminal
switch(config)# port-profile ppEth
switch(config-port-prof)# switchport mode trunk
switch(config-port-prof)# switchport trunk allowed vlan 300-400
switch(config-port-prof)# flowcontrol receive on
switch(config-port-prof)# speed 10000
switch(config-port-prof)#
```

Modifying a Port Profile

You can modify a port profile in port-profile configuration mode.

You can remove commands from a port profile using the **no** form of the command. When you remove a command from the port profile, the corresponding command is removed from the interface that is attached to the port profile.

Procedure

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | configure terminal Example: switch# configure terminal switch(config)# | Enters configuration mode. |
| Step 2 | port-profile [type {ethernet interface-vlan port channel}] name Example: switch(config)# port-profile type ethernet test switch(config-port-prof)# | Enters the port profile configuration mode for the specified port profile and allows you to add or remove configurations to the profile. |
| Step 3 | exit Example: switch(config-port-prof)# exit switch(config)# | Exits the port profile configuration mode. |
| Step 4 | show port-profile Example: switch(config)# show port-profile name | (Optional) Displays the port profile configuration. |
| Step 5 | copy running-config startup-config Example: switch(config)# copy running-config startup-config | (Optional) Copies the running configuration to the startup configuration. |

This example shows how to remove commands from the port profile named ppEth configured for an Ethernet interface:

```
switch# configure terminal
switch(config)# port-profile ppEth
switch(config-port-prof)# switchport mode trunk
switch(config-port-prof)# switchport trunk allowed vlan 300-400
switch(config-port-prof)# flowcontrol receive on
switch(config-port-prof)# no speed 10000
switch(config-port-prof)#
```

Enabling a Specific Port Profile

Procedure

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | configure terminal Example: switch# configure terminal switch(config)# | Enters configuration mode. |
| Step 2 | port-profile [type {ethernet interface-vlan port channel}] name Example: switch(config)# port-profile type ethernet test switch(config-port-prof)# no shutdown switch(config-port-prof)# | Enters the port profile configuration mode for the specified port profile. |
| Step 3 | state enabled name Example: switch(config-port-prof)# state enabled switch(config-port-prof)# | Enables the port profile. |
| Step 4 | exit Example: switch(config-port-prof)# exit switch(config)# | Exits the port profile configuration mode. |
| Step 5 | show port-profile Example: switch(config)# show port-profile name | (Optional) Displays the port profile configuration. |
| Step 6 | copy running-config startup-config Example: switch(config)# copy running-config startup-config | (Optional) Copies the running configuration to the startup configuration. |

This example shows how to enter port profile configuration mode and enable the port profile:

```
switch# configure terminal
switch(config)# port-profile type ethernet test
switch(config-port-prof)# state enabled
switch(config-port-prof)#
```

Inheriting a Port Profile

You can inherit a port profile onto an existing port profile. The switch supports four levels of inheritance.

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | configure terminal Example: switch# configure terminal switch(config)# | Enters configuration mode. |
| Step 2 | port-profile <i>name</i> Example: switch(config)# port-profile test switch(config-port-prof)# | Enters port profile configuration mode for the specified port profile. |
| Step 3 | inherit port-profile <i>name</i> Example: switch(config-port-prof)# inherit port-profile adam switch(config-port-prof)# | Inherits another port profile onto the existing one. The original port profile assumes all the configurations of the inherited port profile. |
| Step 4 | exit Example: switch(config-port-prof)# exit switch(config)# | Exits the port profile configuration mode. |
| Step 5 | show port-profile Example: switch(config)# show port-profile <i>name</i> | (Optional) Displays the port profile configuration. |
| Step 6 | copy running-config startup-config Example: switch(config)# copy running-config startup-config | (Optional) Copies the running configuration to the startup configuration. |

This example shows how to inherit the port profile named adam onto the port profile named test:

```
switch# configure terminal
switch(config)# port-profile test
switch(config-ppm)# inherit port-profile adam
switch(config-ppm)#
```

This example shows how to add the interface commands to a port profile named ppEth configured for Ethernet interfaces:

```
switch# configure terminal
switch(config)# port-profile ppEth
switch(config-port-prof)# switchport mode trunk
switch(config-port-prof)# switchport trunk allowed vlan 300-400
switch(config-port-prof)# flowcontrol receive on
switch(config-port-prof)# speed 10000
switch(config-port-prof)#
```

This example shows how to inherit a port profile named ppEth configured for Ethernet interfaces into an existing port profile named test:

```
switch# configure terminal
switch(config)# port-profile test
switch(config-port-prof)# inherit port-profile ppEth
switch(config-port-prof)#
```

This example shows how to assign a port profile named ppEth configured for Ethernet interfaces to a range of Ethernet interfaces:

```
switch# configure terminal
switch(config)# interface ethernet 1/2-5
switch(config-if)# inherit port-profile ppEth
switch(config-if)#
```

This example shows how to remove an inherited port profile named ppEth from an existing port profile named test:

```
switch# configure terminal
switch(config)# port-profile test
switch(config-port-prof)# no inherit port-profile ppEth
switch(config-port-prof)#
```

Removing an Inherited Port Profile

You can remove an inherited port profile.

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | configure terminal Example: switch# configure terminal switch(config)# | Enters configuration mode. |
| Step 2 | port-profile <i>name</i> Example: switch(config)# port-profile test switch(config-port-prof)# | Enters port profile configuration mode for the specified port profile. |
| Step 3 | no inherit port-profile <i>name</i> Example: switch(config-port-prof)# no inherit port-profile adam switch(config-port-prof)# | Removes an inherited port profile from this port profile. |
| Step 4 | exit Example: switch(config-port-prof)# exit switch(config)# | Exits the port profile configuration mode. |
| Step 5 | show port-profile Example: switch(config)# show port-profile <i>name</i> | (Optional) Displays the port profile configuration. |

| | Command or Action | Purpose |
|---------------|--|--|
| Step 6 | copy running-config startup-config Example: switch(config)# copy running-config startup-config | (Optional) Copies the running configuration to the startup configuration. |

This example shows how to remove the inherited port profile named adam from the port profile named test:

```
switch# configure terminal
switch(config)# port-profile test
switch(config-ppm)# no inherit port-profile adam
switch(config-ppm)#
```

Assigning a Port Profile to a Range of Interfaces

You can assign a port profile to an interface or to a range of interfaces. All of the interfaces must be the same type.

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | switch# configure terminal | Enters global configuration mode. |
| Step 2 | interface [ethernet <i>slot/port</i> interface-vlan <i>vlan-id</i> port-channel <i>number</i>] | Selects the range of interfaces. Note If this is a 10G breakout port, the <i>slot/port</i> syntax is <i>slot/QSFP-module/port</i> . |
| Step 3 | inherit port-profile <i>name</i> | Assigns the specified port profile to the selected interfaces. |
| Step 4 | exit | Exits port profile configuration mode. |
| Step 5 | show port-profile <i>name</i> | (Optional) Displays the port profile configuration. |
| Step 6 | switch(config)# copy running-config startup-config | (Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration. |

This example shows how to assign the port profile named adam to Ethernet interfaces 2/3 to 2/5, 3/2, and 1/20 to 1/25:

```
switch# configure terminal
switch(config)# interface ethernet 2/3 to 2/5, 3/2, and 1/20 to 1/25
switch(config-if)# inherit port-profile adam
switch(config-if)# exit
switch(config)# show port-profile adam
switch(config)# copy running-config startup-config
```

Removing a Port Profile from a Range of Interfaces

You can remove a port profile from some or all of the interfaces to which you have applied the profile.

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | <code>switch# configure terminal</code> | Enters global configuration mode. |
| Step 2 | <code>interface [ethernet slot/port interface-vlan vlan-id port-channel number]</code> | Selects the range of interfaces. Note If this is a 10G breakout port, the <i>slot/port</i> syntax is <i>slot/QSFP-module/port</i> . |
| Step 3 | <code>no inherit port-profile name</code> | Removes the specified port profile from the selected interfaces. |
| Step 4 | <code>exit</code> | Exits port profile configuration mode. |
| Step 5 | <code>show port-profile</code> | (Optional) Displays the port profile configuration. |
| Step 6 | <code>switch(config)# copy running-config startup-config</code> | (Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration. |

This example shows how to remove the port profile named adam from Ethernet interfaces 1/3-5:

```
switch# configure terminal
switch(config)# interface ethernet 1/3-5
switch(config-if)# no inherit port-profile adam
switch(config-if)# exit
switch(config)# show port-profile
switch(config)# copy running-config startup-config
```

Configuration Examples for Port Profiles

The following example shows how to configure a port profile, inherit the port profile on an Ethernet interface, and enabling the port profile.

```
switch(config)#
switch(config)# show running-config interface Ethernet1/14

!Command: show running-config interface Ethernet1/14
!Time: Thu Aug 26 07:01:32 2010

version 5.0(2)N1(1)

interface Ethernet1/14

switch(config)# port-profile type ethernet alpha
switch(config-port-prof)# switchport mode trunk
switch(config-port-prof)# switchport trunk allowed vlan 10-15
switch(config-port-prof)#
switch(config-port-prof)# show running-config port-profile alpha
```

```

!Command: show running-config port-profile alpha
!Time: Thu Aug 26 07:02:29 2010

version 5.0(2)N1(1)
port-profile type ethernet alpha
  switchport mode trunk
  switchport trunk allowed vlan 10-15

switch(config-port-prof)# int eth 1/14
switch(config-if)# inherit port-profile alpha
switch(config-if)#
switch(config-if)# port-profile type ethernet alpha
switch(config-port-prof)# state enabled
switch(config-port-prof)#
switch(config-port-prof)# sh running-config interface ethernet 1/14

!Command: show running-config interface Ethernet1/14
!Time: Thu Aug 26 07:03:17 2010

version 5.0(2)N1(1)

interface Ethernet1/14
  inherit port-profile alpha

switch(config-port-prof)# sh running-config interface ethernet 1/14 expand-port-profile

!Command: show running-config interface Ethernet1/14 expand-port-profile
!Time: Thu Aug 26 07:03:21 2010

version 5.0(2)N1(1)

interface Ethernet1/14
  switchport mode trunk
  switchport trunk allowed vlan 10-15

switch(config-port-prof)#

```

Configuring a Default Interface

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | switch# configure terminal | Enters global configuration mode. |
| Step 2 | switch(config)# default interface <i>int-if</i> [checkpoint name] | <p>Deletes the configuration of the interface and restores the default configuration. The value of <i>int-if</i> can be one of the following:</p> <ul style="list-style-type: none"> • ethernet • loopback • mgmt • port-channel • vlan <p>Use the checkpoint keyword to store a copy of the running configuration of the interface before clearing the configuration.</p> |

| | Command or Action | Purpose |
|---------------|-----------------------------|--|
| Step 3 | <code>exit</code> | Exits the configuration mode. |
| Step 4 | <code>show interface</code> | (Optional) Displays the interface status and information. |

This example shows how to delete the configuration of an Ethernet interface while saving a checkpoint of the running configuration for rollback purposes:

```
switch# configure terminal
switch(config)# show running-config interface e1/10
!Command: show running-config interface Ethernet1/10
!Time: Tue Jul 2 10:23:50 2013

version 6.0(2)N2(1)

interface Ethernet1/10
switchport mode trunk
channel-group 1

default interface ethernet 3/1 checkpoint chk1
.....Done
switch(config)# show running-config interface e1/10
!Command: show running-config interface Ethernet1/10
!Time: Tue Jul 2 10:24:41 2013

version 6.0(2)N2(1)

interface Ethernet1/10

switch(config)#
```

Configuring Default Interface Mode

Procedure

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | <code>switch# configure terminal</code> | Enters global configuration mode. |
| Step 2 | <code>switch(config)# system default switchport [shutdown]</code> | Sets default interface mode. Note When the system default switchport shutdown command is issued, any switchports (including FEX HIFs) that are not configured with no shutdown command are shut down. To avoid the shutdown, configure the switchports with no shutdown command. |

This example shows how to set the default interface mode:

```
switch# configure terminal
switch(config)# system default switchport
```

Configuring the Description Parameter

You can provide textual interface descriptions for the Ethernet ports.

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | switch# configure terminal | Enters global configuration mode. |
| Step 2 | switch(config)# interface <i>type slot/port</i> | Enters interface configuration mode for the specified interface. Note If this is a 10G breakout port, the <i>slot/port</i> syntax is <i>slot/QSFP-module/port</i> . |
| Step 3 | switch(config-if)# description <i>test</i> | Specifies the description for the interface. |

This example shows how to set the interface description to Server 3 interface:

```
switch# configure terminal
switch(config)# interface ethernet 1/3
switch(config-if)# description Server 3 Interface
```

Disabling and Restarting Ethernet Interfaces

You can shut down and restart an Ethernet interface. This action disables all of the interface functions and marks the interface as being down on all monitoring displays.

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | switch# configure terminal | Enters global configuration mode. |
| Step 2 | switch(config)# interface <i>type slot/port</i> | Enters interface configuration mode for the specified interface. Note If this is a 10G breakout port, the <i>slot/port</i> syntax is <i>slot/QSFP-module/port</i> . |
| Step 3 | switch(config-if)# shutdown | Disables the interface. |
| Step 4 | switch(config-if)# no shutdown | Restarts the interface. |

This example shows how to disable an Ethernet port:

```
switch# configure terminal
switch(config)# interface ethernet 1/4
switch(config-if)# shutdown
```

This example shows how to restart an Ethernet interface:

```
switch# configure terminal
switch(config)# interface ethernet 1/4
switch(config-if)# no shutdown
```

Displaying Interface Information

To view configuration information about the defined interfaces, perform one of these tasks:

| Command | Purpose |
|--|---|
| switch# show interface <i>type slot/port</i> | Displays the detailed configuration of the specified interface. Note If this is a 10G breakout port, the <i>slot/port</i> syntax is <i>slot/QSFP-module/port</i> . |
| switch# show interface <i>type slot/port capabilities</i> | Displays detailed information about the capabilities of the specified interface. This option is available only for physical interfaces. Note If this is a 10G breakout port, the <i>slot/port</i> syntax is <i>slot/QSFP-module/port</i> . |
| switch# show interface <i>type slot/port transceiver</i> | Displays detailed information about the transceiver connected to the specified interface. This option is available only for physical interfaces. Note If this is a 10G breakout port, the <i>slot/port</i> syntax is <i>slot/QSFP-module/port</i> . |
| switch# show interface brief | Displays the status of all interfaces. |
| switch# show interface flowcontrol | Displays the detailed listing of the flow control settings on all interfaces. |
| switch# show interface debounce | Displays the debounce status of all interfaces. |

The **show interface** command is invoked from EXEC mode and displays the interface configurations. Without any arguments, this command displays the information for all the configured interfaces in the switch.

This example shows how to display the physical Ethernet interface:

```
switch# show interface ethernet 1/1
Ethernet1/1 is up
Hardware is 1000/10000 Ethernet, address is 000d.eca3.5f08 (bia 000d.eca3.5f08)
MTU 1500 bytes, BW 10000000 Kbit, DLY 10 usec,
    reliability 255/255, txload 190/255, rxload 192/255
Encapsulation ARPA
Port mode is trunk
full-duplex, 10 Gb/s, media type is 1/10g
Input flow-control is off, output flow-control is off
Auto-mdix is turned on
Rate mode is dedicated
```

```

Switchport monitor is off
Last clearing of "show interface" counters never
5 minute input rate 942201806 bytes/sec, 14721892 packets/sec
5 minute output rate 935840313 bytes/sec, 14622492 packets/sec
Rx
 129141483840 input packets 0 unicast packets 129141483847 multicast packets
 0 broadcast packets 0 jumbo packets 0 storm suppression packets
 8265054965824 bytes
 0 No buffer 0 runt 0 Overrun
 0 crc 0 Ignored 0 Bad etype drop
 0 Bad proto drop
Tx
 119038487241 output packets 119038487245 multicast packets
 0 broadcast packets 0 jumbo packets
 7618463256471 bytes
 0 output CRC 0 ecc
 0 underrun 0 if down drop      0 output error 0 collision 0 deferred
 0 late collision 0 lost carrier 0 no carrier
 0 babble
 0 Rx pause 8031547972 Tx pause 0 reset

```

This example shows how to display the physical Ethernet capabilities:

```

switch# show interface ethernet 1/1 capabilities
Ethernet1/1
  Model:                734510033
  Type:                 10Gbase-(unknown)
  Speed:                1000,10000
  Duplex:               full
  Trunk encap. type:   802.1Q
  Channel:              yes
  Broadcast suppression: percentage(0-100)
  Flowcontrol:         rx-(off/on),tx-(off/on)
  Rate mode:            none
  QOS scheduling:       rx-(6qlt),tx-(1p6q0t)
  CoS rewrite:         no
  ToS rewrite:         no
  SPAN:                 yes
  UDLD:                 yes
  Link Debounce:       yes
  Link Debounce Time:  yes
  MDIX:                 no
  FEX Fabric:          yes

```

This example shows how to display the physical Ethernet transceiver:

```

switch# show interface ethernet 1/1 transceiver
Ethernet1/1
  sfp is present
  name is CISCO-EXCELIGHT
  part number is SPP5101SR-C1
  revision is A
  serial number is ECL120901AV
  nominal bitrate is 10300 Mbits/sec
  Link length supported for 50/125mm fiber is 82 m(s)
  Link length supported for 62.5/125mm fiber is 26 m(s)
  cisco id is --
  cisco extended id number is 4

```

This example shows how to display a brief interface status (some of the output has been removed for brevity):

```
switch# show interface brief
```

```

-----
Ethernet      VLAN   Type Mode   Status Reason                               Speed   Port
Interface                                           -----
Eth1/1        200    eth trunk up      none                               10G(D)  --
Eth1/2         1      eth trunk up      none                               10G(D)  --
Eth1/3         300    eth access down  SFP not inserted                  10G(D)  --
Eth1/4         300    eth access down  SFP not inserted                  10G(D)  --
Eth1/5         300    eth access down  Link not connected                 1000(D) --
Eth1/6         20     eth access down  Link not connected                 10G(D)  --
-----

```

```
Eth1/7      300   eth  access down   SFP not inserted      10G(D) --
...
```

This example shows how to display the link debounce status (some of the output has been removed for brevity):

```
switch# show interface debounce
```

```
-----
Port          Debounce time  Value(ms)
-----
...
Eth1/1        enable         100
Eth1/2        enable         100
Eth1/3        enable         100
...
```

This example shows how to display the CDP neighbors:

```
switch# show cdp neighbors
Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute

Device ID         Local Intrfce  Hldtme  Capability  Platform  Port ID
dl3-dist-1       mgmt0         148     S I         WS-C2960-24TC  Fas0/9
n5k(FLC12080012) Eth1/5        8       S I s      N5K-C5020P-BA  Eth1/5
```

Default Physical Ethernet Settings

The following table lists the default settings for all physical Ethernet interfaces:

| Parameter | Default Setting |
|------------------|--------------------------|
| Debounce | Enable, 100 milliseconds |
| Duplex | Auto (full-duplex) |
| Encapsulation | ARPA |
| MTU ¹ | 1500 bytes |
| Port Mode | Access |
| Speed | Auto (10000) |

¹ MTU cannot be changed per-physical Ethernet interface. You modify MTU by selecting maps of QoS classes.

