



# Interface and Hardware Commands

---

- [client vlan, page 4](#)
- [debug ilpower, page 5](#)
- [debug interface, page 7](#)
- [debug lldp packets, page 8](#)
- [debug nmsp, page 9](#)
- [debug platform poe, page 10](#)
- [duplex, page 11](#)
- [errdisable detect cause, page 13](#)
- [errdisable recovery cause, page 15](#)
- [errdisable recovery interval, page 18](#)
- [interface, page 19](#)
- [interface range, page 21](#)
- [ip mtu, page 22](#)
- [ipv6 mtu, page 24](#)
- [lldp \(interface configuration\), page 26](#)
- [logging event power-inline-status, page 28](#)
- [mdix auto, page 29](#)
- [mode \(power-stack configuration\), page 30](#)
- [network-policy, page 32](#)
- [network-policy profile \(global configuration\), page 34](#)
- [nmsp attachment suppress, page 36](#)
- [power efficient-ethernet auto, page 37](#)
- [power-priority, page 38](#)
- [power inline, page 40](#)

- power inline police, page 44
- power supply, page 47
- show CAPWAP summary, page 49
- show controllers cpu-interface, page 50
- show controllers ethernet-controller, page 52
- show controllers utilization, page 62
- show eee, page 64
- show env, page 67
- show errdisable detect, page 70
- show errdisable recovery, page 72
- show interfaces, page 74
- show interfaces counters, page 78
- show interfaces switchport, page 81
- show interfaces transceiver, page 85
- show mgmt-infra trace messages ilpower, page 88
- show mgmt-infra trace messages ilpower-ha, page 90
- show mgmt-infra trace messages platform-mgr-poe, page 91
- show network-policy profile, page 93
- show platform CAPWAP summary, page 94
- show power inline, page 95
- show stack-power , page 101
- show system mtu, page 102
- show wireless interface summary, page 103
- speed, page 104
- stack-power , page 106
- switchport backup interface, page 108
- switchport block, page 111
- system mtu, page 113
- voice-signaling vlan (network-policy configuration), page 114
- voice vlan (network-policy configuration), page 116
- wireless ap-manager interface, page 118
- wireless exclusionlist, page 119
- wireless linktest, page 120

- [wireless management interface, page 121](#)
- [wireless peer-blocking forward-upstream, page 122](#)

# client vlan

To configure a WLAN interface or an interface group, use the **client vlan** command. To disable the WLAN interface, use the **no** form of this command.

**client vlan** *interface-id-name-or-group-name*

**no client vlan**

## Syntax Description

<i>interface--id-name-or-group-name</i>	Interface ID, name, or VLAN group name.
---	---

## Command Default

The default interface is configured.

## Command Modes

WLAN configuration

## Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

## Usage Guidelines

You must disable the WLAN before using this command. See Related Commands section for more information on how to disable a WLAN.

## Examples

This example shows how to enable a client VLAN on a WLAN:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# client vlan client-vlan1
Switch(config-wlan)# end
```

This example shows how to disable a client association limit on a WLAN:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# no client vlan
Switch(config-wlan)# end
```

# debug ilpower

To enable debugging of the power controller and Power over Ethernet (PoE) system, use the **debug ilpower** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

```
debug ilpower {cdp| controller| event| ha| ipc| police| port| powerman| registries| scp | sense| upoe}
no debug ilpower {cdp| controller| event| ha| ipc| police| port| powerman| registries| scp | sense| upoe}
```

## Syntax Description

<b>cdp</b>	Displays PoE Cisco Discovery Protocol (CDP) debug messages.
<b>controller</b>	Displays PoE controller debug messages.
<b>event</b>	Displays PoE event debug messages.
<b>ha</b>	Displays PoE high-availability messages.
<b>ipc</b>	Displays PoE Inter-Process Communication (IPC) debug messages.
<b>police</b>	Displays PoE police debug messages.
<b>port</b>	Displays PoE port manager debug messages.
<b>powerman</b>	Displays PoE power management debug messages.
<b>registries</b>	Displays PoE registries debug messages.
<b>scp</b>	Displays PoE SCP debug messages.
<b>sense</b>	Displays PoE sense debug messages.
<b>upoe</b>	Displays Cisco UPOE debug messages.

## Command Default

Debugging is disabled.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.
Cisco IOS XE 3.3SE	The <b>upoe</b> keyword was added.

**Usage Guidelines**

This command is supported only on PoE-capable switches.

When you enable debugging on a switch stack, it is enabled only on the active switch. To enable debugging on a stack member, you can start a session from the active switch by using the **session** *switch-number* EXEC command. Then enter the **debug** command at the command-line prompt of the stack member.

# debug interface

To enable debugging of interface-related activities, use the **debug interface** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

**debug interface** {*interface-id*} **counters** {**exceptions**|**protocol memory**}|**states**}

**no debug interface** {*interface-id*} **counters** {**exceptions**|**protocol memory**}|**states**}

## Syntax Description

<i>interface-id</i>	ID of the physical interface. Displays debug messages for the specified physical port, identified by type switch number/module number/port, for example, gigabitethernet 1/0/2.
<b>counters</b>	Displays counters debugging information.
<b>exceptions</b>	Displays debug messages when a recoverable exceptional condition occurs during the computation of the interface packet and data rate statistics.
<b>protocol memory</b>	Displays debug messages for memory operations of protocol counters.
<b>states</b>	Displays intermediary debug messages when an interface's state transitions.

## Command Default

Debugging is disabled.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

## Usage Guidelines

If you do not specify a keyword, all debug messages appear.

The **undebug interface** command is the same as the **no debug interface** command.

When you enable debugging on a switch stack, it is enabled only on the active switch. To enable debugging on a stack member, you can start a session from the active switch by using the **session switch-number** EXEC command. Then enter the **debug** command at the command-line prompt of the stack member.

## debug lldp packets

To enable debugging of Link Layer Discovery Protocol (LLDP) packets, use the **debug lldp packets** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

**debug lldp packets**

**no debug lldp packets**

**Syntax Description** This command has no arguments or keywords.

**Command Default** Debugging is disabled.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	Cisco IOS XE 3.2SE	This command was introduced.

**Usage Guidelines** The **undebug lldp packets** command is the same as the **no debug lldp packets** command. When you enable debugging on a switch stack, it is enabled only on the active switch. To enable debugging on a stack member, you can start a session from the active switch by using the **session switch-number** EXEC command.

## debug nmosp

To enable debugging of the Network Mobility Services Protocol (NMSP) on the switch, use the **debug nmosp** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

**debug nmosp** {**all**| **connection**| **detail**| **error**| **event**| **message** {**rx**| **tx**}| **packet**} [**switch** *switch-number*]

**no debug nmosp** {**all**| **connection**| **detail**| **error**| **event**| **message** {**rx**| **tx**}| **packet**} [**switch** *switch-number*]

### Syntax Description

<b>all</b>	Displays all NMSP debug messages.
<b>connection</b>	Displays debug messages for NMSP connection events.
<b>detail</b>	Displays detailed debug messages for NMSP.
<b>error</b>	Displays debugging information for NMSP error messages.
<b>event</b>	Displays debug messages for NMSP events.
<b>message</b>	Displays debugging information for NMSP messages.
<b>rx</b>	Displays debugging information for NMSP receive messages.
<b>tx</b>	Displays debugging information for NMSP transmit messages.
<b>packet</b>	Displays debug messages for NMSP packet events.
<b>switch</b> <i>switch-number</i>	(Optional) Specifies the switch number for which to display NMSP debugging information.

### Command Default

Debugging is disabled.

### Command Modes

Privileged EXEC

### Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

### Usage Guidelines

The **undebg nmosp** command is the same as the **no debug nmosp** command.

When you enable debugging on a switch stack, it is enabled only on the active switch. To enable debugging on a stack member, you can start a session from the active switch by using the **session** *switch-number* EXEC command. Then enter the **debug** command at the command-line prompt of the stack member.

## debug platform poe

To enable debugging of a Power over Ethernet (PoE) port, use the **debug platform poe** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

**debug platform poe** [**error**|**info**] [**switch** *switch-number*]

**no debug platform poe** [**error**|**info**] [**switch** *switch-number*]

### Syntax Description

<b>error</b>	(Optional) Displays PoE-related error debug messages.
<b>info</b>	(Optional) Displays PoE-related information debug messages.
<b>switch</b> <i>switch-number</i>	(Optional) Specifies the stack member. This keyword is supported only on stacking-capable switches.

### Command Default

Debugging is disabled.

### Command Modes

Privileged EXEC

### Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

### Usage Guidelines

The **undebug platform poe** command is the same as the **no debug platform poe** command.

# duplex

To specify the duplex mode of operation for a port, use the **duplex** command in interface configuration mode. To return to the default value, use the **no** form of this command.

**duplex** {**auto**| **full**| **half**}

**no duplex** {**auto**| **full**| **half**}

## Syntax Description

<b>auto</b>	Enables automatic duplex configuration. The port automatically detects whether it should run in full- or half-duplex mode, depending on the attached device mode.
<b>full</b>	Enables full-duplex mode.
<b>half</b>	Enables half-duplex mode (only for interfaces operating at 10 or 100 Mb/s). You cannot configure half-duplex mode for interfaces operating at 1000 or 10,000 Mb/s.

## Command Default

The default is **auto** for Gigabit Ethernet ports.

You cannot configure the duplex mode on 10-Gigabit Ethernet ports; it is always **full**.

Duplex options are not supported on the 1000BASE-*x* or 10GBASE-*x* (where *x* is -BX, -CWDM, -LX, -SX, or -ZX) small form-factor pluggable (SFP) modules.

## Command Modes

Interface configuration

## Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

## Usage Guidelines

For Gigabit Ethernet ports, setting the port to **auto** has the same effect as specifying **full** if the attached device does not autonegotiate the duplex parameter.



### Note

Half-duplex mode is supported on Gigabit Ethernet interfaces if the duplex mode is **auto** and the connected device is operating at half duplex. However, you cannot configure these interfaces to operate in half-duplex mode.

Certain ports can be configured to be either full duplex or half duplex. How this command is applied depends on the device to which the switch is attached.

If both ends of the line support autonegotiation, we highly recommend using the default autonegotiation settings. If one interface supports autonegotiation and the other end does not, configure duplex and speed on both interfaces, and use the **auto** setting on the supported side.

If the speed is set to **auto**, the switch negotiates with the device at the other end of the link for the speed setting and then forces the speed setting to the negotiated value. The duplex setting remains as configured on each end of the link, which could result in a duplex setting mismatch.

You can configure the duplex setting when the speed is set to **auto**.



#### Caution

Changing the interface speed and duplex mode configuration might shut down and reenables the interface during the reconfiguration.

You can verify your setting by entering the **show interfaces** privileged EXEC command.

#### Examples

This example shows how to configure an interface for full-duplex operation:

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# duplex full
```

#### Related Commands

Command	Description
<a href="#">show interfaces</a>	Displays the administrative and operational status of all interfaces or a specified interface.

## errdisable detect cause

To enable error-disable detection for a specific cause or for all causes, use the **errdisable detect cause** command in global configuration mode. To disable the error-disable detection feature, use the **no** form of this command.

```
errdisable detect cause {all| arp-inspection| bpduguard shutdown vlan| dhcp-rate-limit| dtp-flap|
gbic-invalid| inline-power| l2ptguard| link-flap| loopback| pagp-flap| pppoe-ia-rate-limit |
security-violation shutdown vlan| sfp-config-mismatch}
```

```
no errdisable detect cause {all| arp-inspection| bpduguard shutdown vlan| dhcp-rate-limit| dtp-flap|
gbic-invalid| inline-power| l2ptguard| link-flap| loopback| pagp-flap| pppoe-ia-rate-limit |
security-violation shutdown vlan| sfp-config-mismatch}
```

### Syntax Description

<b>all</b>	Enables error detection for all error-disabled causes.
<b>arp-inspection</b>	Enables error detection for dynamic Address Resolution Protocol (ARP) inspection.
<b>bpduguard shutdown vlan</b>	Enables per-VLAN error-disable for BPDU guard.
<b>dhcp-rate-limit</b>	Enables error detection for DHCP snooping.
<b>dtp-flap</b>	Enables error detection for the Dynamic Trunking Protocol (DTP) flapping.
<b>gbic-invalid</b>	Enables error detection for an invalid Gigabit Interface Converter (GBIC) module.  <b>Note</b> This error refers to an invalid small form-factor pluggable (SFP) module.
<b>inline-power</b>	Enables error detection for the Power over Ethernet (PoE) error-disabled cause.  <b>Note</b> This keyword is supported only on switches with PoE ports.
<b>l2ptguard</b>	Enables error detection for a Layer 2 protocol-tunnel error-disabled cause.
<b>link-flap</b>	Enables error detection for link-state flapping.
<b>loopback</b>	Enables error detection for detected loopbacks.
<b>pagp-flap</b>	Enables error detection for the Port Aggregation Protocol (PAgP) flap error-disabled cause.
<b>pppoe-ia-rate-limit</b>	Enables error detection for the PPPoE Intermediate Agent rate-limit error-disabled cause.

---

<b>security-violation shutdown vlan</b>	Enables voice aware 802.1x security.
---	--------------------------------------

---

<b>sfp-config-mismatch</b>	Enables error detection on an SFP configuration mismatch.
----------------------------	---

---

**Command Default**

Detection is enabled for all causes. All causes, except per-VLAN error disabling, are configured to shut down the entire port.

**Command Modes**

Global configuration

**Command History****Release**

Cisco IOS XE 3.2SE

**Modification**

This command was introduced.

---

**Usage Guidelines**

A cause (such as a link-flap or dhcp-rate-limit) is the reason for the error-disabled state. When a cause is detected on an interface, the interface is placed in an error-disabled state, an operational state that is similar to a link-down state.

When a port is error-disabled, it is effectively shut down, and no traffic is sent or received on the port. For the bridge protocol data unit (BPDU) guard, voice-aware 802.1x security, and port-security features, you can configure the switch to shut down only the offending VLAN on the port when a violation occurs, instead of shutting down the entire port.

If you set a recovery mechanism for the cause by entering the **errdisable recovery** global configuration command, the interface is brought out of the error-disabled state and allowed to retry the operation when all causes have timed out. If you do not set a recovery mechanism, you must enter the **shutdown** and then the **no shutdown** commands to manually recover an interface from the error-disabled state.

To verify your settings, enter the **show errdisable detect** privileged EXEC command.

**Examples**

This example shows how to enable error-disabled detection for the link-flap error-disabled cause:

```
Switch(config)# errdisable detect cause link-flap
```

This command shows how to globally configure BPDU guard for a per-VLAN error-disabled state:

```
Switch(config)# errdisable detect cause bpduguard shutdown vlan
```

This command shows how to globally configure voice-aware 802.1x security for a per-VLAN error-disabled state:

```
Switch(config)# errdisable detect cause security-violation shutdown vlan
```

You can verify your setting by entering the **show errdisable detect** privileged EXEC command.

**Related Commands****Command**

[show errdisable detect](#)

**Description**

Displays error-disabled detection status.

---

## errdisable recovery cause

To enable the error-disabled mechanism to recover from a specific cause, use the **errdisable recovery cause** command in global configuration mode. To return to the default setting, use the **no** form of this command.

```
errdisable recovery cause {all| arp-inspection| bpduguard| channel-misconfig| dhcp-rate-limit| dtp-flap|
gbic-invalid| inline-power| l2ptguard| link-flap| loopback| mac-limit| pagp-flap| port-mode-failure|
pppoe-ia-rate-limit| psecure-violation| security-violation| sfp-config-mismatch| storm-control| udd|
vmps}
```

```
no errdisable recovery cause {all| arp-inspection| bpduguard| channel-misconfig| dhcp-rate-limit|
dtp-flap| gbic-invalid| inline-power| l2ptguard| link-flap| loopback| mac-limit| pagp-flap|
port-mode-failure| pppoe-ia-rate-limit| psecure-violation| security-violation| sfp-config-mismatch|
storm-control| udd| vmps}
```

### Syntax Description

<b>all</b>	Enables the timer to recover from all error-disabled causes.
<b>arp-inspection</b>	Enables the timer to recover from the Address Resolution Protocol (ARP) inspection error-disabled state.
<b>bpduguard</b>	Enables the timer to recover from the bridge protocol data unit (BPDU) guard error-disabled state.
<b>channel-misconfig</b>	Enables the timer to recover from the EtherChannel misconfiguration error-disabled state.
<b>dhcp-rate-limit</b>	Enables the timer to recover from the DHCP snooping error-disabled state.
<b>dtp-flap</b>	Enables the timer to recover from the Dynamic Trunking Protocol (DTP) flap error-disabled state.
<b>gbic-invalid</b>	Enables the timer to recover from an invalid Gigabit Interface Converter (GBIC) module error-disabled state.  <b>Note</b> This error refers to an invalid small form-factor pluggable (SFP) error-disabled state.
<b>inline-power</b>	Enables the timer to recover from the Power over Ethernet (PoE) error-disabled state.  This keyword is supported only on switches with PoE ports.
<b>l2ptguard</b>	Enables the timer to recover from a Layer 2 protocol tunnel error-disabled state.
<b>link-flap</b>	Enables the timer to recover from the link-flap error-disabled state.
<b>loopback</b>	Enables the timer to recover from a loopback error-disabled state.
<b>mac-limit</b>	Enables the timer to recover from the mac limit error-disabled state.

<b>pagp-flap</b>	Enables the timer to recover from the Port Aggregation Protocol (PAgP)-flap error-disabled state.
<b>port-mode-failure</b>	Enables the timer to recover from the port mode change failure error-disabled state.
<b>pppoe-ia-rate-limit</b>	Enables the timer to recover from the PPPoE IA rate limit error-disabled state.
<b>psecure-violation</b>	Enables the timer to recover from a port security violation disable state.
<b>security-violation</b>	Enables the timer to recover from an IEEE 802.1x-violation disabled state.
<b>sfp-config-mismatch</b>	Enables error detection on an SFP configuration mismatch.
<b>storm-control</b>	Enables the timer to recover from a storm control error.
<b>udld</b>	Enables the timer to recover from the UniDirectional Link Detection (UDLD) error-disabled state.
<b>vmmps</b>	Enables the timer to recover from the VLAN Membership Policy Server (VMPS) error-disabled state.

**Command Default** Recovery is disabled for all causes.

**Command Modes** Global configuration

#### Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

#### Usage Guidelines

A cause (such as all or BPDU guard) is defined as the reason that the error-disabled state occurred. When a cause is detected on an interface, the interface is placed in the error-disabled state, an operational state similar to link-down state.

When a port is error-disabled, it is effectively shut down, and no traffic is sent or received on the port. For the BPDU guard and port-security features, you can configure the switch to shut down only the offending VLAN on the port when a violation occurs, instead of shutting down the entire port.

If you do not enable the recovery for the cause, the interface stays in the error-disabled state until you enter the **shutdown** and the **no shutdown** interface configuration commands. If you enable the recovery for a cause, the interface is brought out of the error-disabled state and allowed to retry the operation again when all the causes have timed out.

Otherwise, you must enter the **shutdown** and then the **no shutdown** commands to manually recover an interface from the error-disabled state.

You can verify your settings by entering the **show errdisable recovery** privileged EXEC command.

### Examples

This example shows how to enable the recovery timer for the BPDUGuard error-disabled cause:

```
Switch(config)# errdisable recovery cause bpduguard
```

### Related Commands

Command	Description
<a href="#">errdisable recovery interval</a>	Specifies the time to recover from an error-disabled state.
<a href="#">show errdisable recovery</a>	Displays the error-disabled recovery timer information.
<a href="#">show interfaces</a>	Displays the administrative and operational status of all interfaces or a specified interface.

# errdisable recovery interval

To specify the time to recover from an error-disabled state, use the **errdisable recovery interval** command in global configuration mode. To return to the default setting, use the **no** form of this command.

**errdisable recovery interval** *timer-interval*

**no errdisable recovery interval** *timer-interval*

## Syntax Description

<i>timer-interval</i>	Time to recover from the error-disabled state. The range is 30 to 86400 seconds. The same interval is applied to all causes. The default interval is 300 seconds.
-----------------------	---

## Command Default

The default recovery interval is 300 seconds.

## Command Modes

Global configuration

## Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

## Usage Guidelines

The error-disabled recovery timer is initialized at a random differential from the configured interval value. The difference between the actual timeout value and the configured value can be up to 15 percent of the configured interval.

You can verify your settings by entering the **show errdisable recovery** privileged EXEC command.

## Examples

This example shows how to set the timer to 500 seconds:

```
Switch(config)# errdisable recovery interval 500
```

## Related Commands

Command	Description
<a href="#">errdisable recovery cause</a>	Enables the error-disabled mechanism to recover from a specific cause.
<a href="#">show errdisable recovery</a>	Displays the error-disabled recovery timer information.
<a href="#">show interfaces</a>	Displays the administrative and operational status of all interfaces or a specified interface.

# interface

To configure an interface, use the **interface** command.

**interface** {**Auto-Template** *Auto-Template interface-number* | **Capwap** *Capwap interface-number* | **Gigabit Ethernet** *Gigabit Ethernet interface number* | **Group VI** *Group VI interface number* **Internal Interface** *Internal Interface number* **Loopback** *Loopback interface number* **Null** *Null interface number* **Port-channel** *interface number* **Port-channel** *interface number* **TenGigabit Ethernet** *interface number* **Tunnel** *interface number* **Vlan** *interface number*}

## Syntax Description

<b>Auto-Template</b> <i>Auto-template interface-number</i>	Enables you to configure auto-template interface. Values range from 1 to 999.
<b>Capwap</b> <i>Capwap interface number</i>	Enables you to configure CAPWAP tunnel interface. Values range from 0 to 2147483647.
<b>GigabitEthernet</b> <i>Gigabit Ethernet interface number</i>	Enables you to configure Gigabit Ethernet IEEE 802.3z interface. Values range from 0 to 9.
<b>Group VI</b> <i>Group VI interface number</i>	Enables you to configure the internal interface. Values range from 0 to 9.
<b>Internal Interface</b> <i>Internal Interface</i>	Enables you to configure internal interface.
<b>Loopback</b> <i>Loopback Interface number</i>	Enables you to configure loopback interface. Values range from 0 to 2147483647.
<b>Null</b> <i>Null interface number</i>	Enables you to configure null interface. Value is 0.
<b>Port-channel</b> <i>interface number</i>	Enables you to configure Ethernet channel interfaces. Values range from 1 to 128.
<b>TenGigabitEthernet</b> <i>interface number</i>	Enables you to configure a 10-Gigabit Ethernet interface. Values range from 0 to 9.
<b>Tunnel</b> <i>interface number</i>	Enables you to configure the tunnel interface. Values range from 0 to 2147483647.
<b>Vlan</b> <i>interface number</i>	Enables you to configure switch VLAN interfaces. Values range from 0 to 4098.

**Command Default** None

**Command Modes** Global configuration

**Command History**

<b>Release</b>	<b>Modification</b>
Cisco IOS XE 3.2SE	This command was introduced.

**Usage Guidelines**

You can not use the "no" form of this command.

**Examples**

This example shows how you can configure interface:

```
Switch# interface Tunnel 15
```

# interface range

To configure an interface range, use the **interface range** command.

**interface range** {**Gigabit Ethernet** *interface-number* | **Loopback** *interface-number* | **Port Channel** *interface-number* | **TenGigabit Ethernet** *interface-number* **Tunnel** *interface-number* **Vlan** *interface-number* **Macro** *WORD*}

## Syntax Description

<b>GigabitEthernet</b> <i>interface-number</i>	Configures the Gigabit Ethernet IEEE 802.3z interface. Values range from 1 to 9.
<b>Loopback</b> <i>interface-number</i>	Configures the loopback interface. Values range from 0 to 2147483647.
<b>Port-Channel</b> <i>interface-number</i>	Configures 10-Gigabit Ethernet channel of interfaces. Values range from 1 to 128.
<b>TenGigabit Ethernet</b> <i>interface-number</i>	Configures 10-Gigabit Ethernet interfaces. Values range from 0 to 9.
<b>Tunnel</b> <i>interface-number</i>	Configures the tunnel interface. Values range from 0 to 2147483647.
<b>VLAN</b> <i>interface-number</i>	Configures the switch VLAN interfaces. Values range from 1 to 4095.
<b>Macro</b> <i>WORD</i>	Configures the keywords to interfaces. Support up to 32 characters.

## Command Default

None

## Command Modes

Global configuration

## Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

## Examples

This example shows how you can configure interface range:

```
Switch(config)# interface range vlan 1
```

# ip mtu

To set the IP maximum transmission unit (MTU) size of routed packets on all routed ports of the switch or switch stack, use the **ip mtu** command in interface configuration mode. To restore the default IP MTU size, use the **no** form of this command.

**ip mtu** *bytes*

**no ip mtu** *bytes*

## Syntax Description

*bytes* MTU size, in bytes. The range is from 68 up to the system MTU value (in bytes).

## Command Default

The default IP MTU size for frames received and sent on all switch interfaces is 1500 bytes.

## Command Modes

Interface configuration

## Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

## Usage Guidelines

The upper limit of the IP value is based on the switch or switch stack configuration and refers to the currently applied system MTU value. For more information about setting the MTU sizes, see the **system mtu** global configuration command.

To return to the default IP MTU setting, you can apply the **default ip mtu** command or the **no ip mtu** command on the interface.

You can verify your setting by entering the **show ip interface** *interface-id* or **show interfaces** *interface-id* privileged EXEC command.

## Examples

The following example sets the maximum IP packet size for VLAN 200 to 1000 bytes:

```
Switch(config)# interface vlan 200
Switch(config-if)# ip mtu 1000
```

The following example sets the maximum IP packet size for VLAN 200 to the default setting of 1500 bytes:

```
Switch(config)# interface vlan 200
Switch(config-if)# default ip mtu
```

This is an example of partial output from the **show ip interface** *interface-id* command. It displays the current IP MTU setting for the interface.

```
Switch# show ip interface gigabitethernet4/0/1
GigabitEthernet4/0/1 is up, line protocol is up
Internet address is 18.0.0.1/24
Broadcast address is 255.255.255.255
```

```
Address determined by setup command
MTU is 1500 bytes
Helper address is not set
```

<output truncated>

**Related Commands**

Command	Description
<a href="#">show interfaces</a>	Displays the administrative and operational status of all interfaces or a specified interface.
<a href="#">system mtu</a>	Sets the global maximum packet size or MTU size for switched packets on Gigabit Ethernet and 10-Gigabit Ethernet ports.

# ipv6 mtu

To set the IPv6 maximum transmission unit (MTU) size of routed packets on all routed ports of the switch or switch stack, use the **ipv6 mtu** command in interface configuration mode. To restore the default IPv6 MTU size, use the **no** form of this command.

**ipv6 mtu** *bytes*

**no ipv6 mtu** *bytes*

## Syntax Description

*bytes* MTU size, in bytes. The range is from 1280 up to the system MTU value (in bytes).

## Command Default

The default IPv6 MTU size for frames received and sent on all switch interfaces is 1500 bytes.

## Command Modes

Interface configuration

## Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

## Usage Guidelines

The upper limit of the IPv6 MTU value is based on the switch or switch stack configuration and refers to the currently applied system MTU value. For more information about setting the MTU sizes, see the **system mtu** global configuration command.

To return to the default IPv6 MTU setting, you can apply the **default ipv6 mtu** command or the **no ipv6 mtu** command on the interface.

You can verify your setting by entering the **show ipv6 interface** *interface-id* or **show interface** *interface-id* privileged EXEC command.

## Examples

The following example sets the maximum IPv6 packet size for an interface to 2000 bytes:

```
Switch(config)# interface gigabitethernet4/0/1
Switch(config-if)# ipv6 mtu 2000
```

The following example sets the maximum IPv6 packet size for an interface to the default setting of 1500 bytes:

```
Switch(config)# interface gigabitethernet4/0/1
Switch(config-if)# default ipv6 mtu
```

This is an example of partial output from the **show ipv6 interface** *interface-id* command. It displays the current IPv6 MTU setting for the interface.

```
Switch# show ipv6 interface gigabitethernet4/0/1
GigabitEthernet4/0/1 is up, line protocol is up
Internet address is 18.0.0.1/24
Broadcast address is 255.255.255.255
```

```
Address determined by setup command
MTU is 1500 bytes
Helper address is not set
```

<output truncated>

**Related Commands**

Command	Description
<a href="#">show interfaces</a>	Displays the administrative and operational status of all interfaces or a specified interface.
<a href="#">system mtu</a>	Sets the global maximum packet size or MTU size for switched packets on Gigabit Ethernet and 10-Gigabit Ethernet ports.

## lldp (interface configuration)

To enable Link Layer Discovery Protocol (LLDP) on an interface, use the **lldp** command in interface configuration mode. To disable LLDP on an interface, use the **no** form of this command.

**lldp** {**med-tlv-select** *tlv*| **receive**| **tlv-select power-management**| **transmit**}

**no lldp** {**med-tlv-select** *tlv*| **receive**| **tlv-select power-management**| **transmit**}

### Syntax Description

<b>med-tlv-select</b>	Selects an LLDP Media Endpoint Discovery (MED) time-length-value (TLV) element to send.
<i>tlv</i>	String that identifies the TLV element. Valid values are the following: <ul style="list-style-type: none"> <li>• <b>inventory-management</b>— LLDP MED Inventory Management TLV.</li> <li>• <b>location</b>— LLDP MED Location TLV.</li> <li>• <b>network-policy</b>— LLDP MED Network Policy TLV.</li> <li>• <b>power-management</b>— LLDP MED Power Management TLV.</li> </ul>
<b>receive</b>	Enables the interface to receive LLDP transmissions.
<b>tlv-select</b>	Selects the LLDP TLVs to send.
<b>power-management</b>	Sends the LLDP Power Management TLV.
<b>transmit</b>	Enables LLDP transmission on the interface.

### Command Default

LLDP is enabled on supported interfaces.

### Command Modes

Interface configuration

### Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

### Usage Guidelines

This command is supported on 802.1 media types.

If the interface is configured as a tunnel port, LLDP is automatically disabled.

**Examples**

The following example shows how to disable LLDP transmission on an interface:

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# no lldp transmit
```

The following example shows how to enable LLDP transmission on an interface:

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# lldp transmit
```

# logging event power-inline-status

To enable the logging of Power over Ethernet (PoE) events, use the **logging event power-inline-status** command in interface configuration mode. To disable the logging of PoE status events, use the **no** form of this command.

**logging event power-inline-status**

**no logging event power-inline-status**

**Syntax Description** This command has no arguments or keywords.

**Command Default** Logging of PoE events is enabled.

**Command Modes** Interface configuration

Command History	Release	Modification
	Cisco IOS XE 3.2SE	This command was introduced.

**Usage Guidelines** The **no** form of this command does not disable PoE error events.

**Examples** This example shows how to enable logging of PoE events on a port:

```
Switch(config-if) # interface gigabitethernet1/0/1
Switch(config-if) # logging event power-inline-status
Switch(config-if) #
```

Related Commands	Command	Description
	<a href="#">power inline</a>	Configures the power management mode on PoE ports.
	<a href="#">show power inline</a>	Displays the PoE status for the specified PoE port, the specified stack member, or for all PoE ports in the switch stack.

# mdix auto

To enable the automatic medium-dependent interface crossover (auto-MDIX) feature on the interface, use the **mdix auto** command in interface configuration mode. To disable auto-MDIX, use the **no** form of this command.

**mdix auto**

**no mdix auto**

**Syntax Description** This command has no arguments or keywords.

**Command Default** Auto-MDIX is enabled.

**Command Modes** Interface configuration

Command History	Release	Modification
	Cisco IOS XE 3.2SE	This command was introduced.

**Usage Guidelines**

When auto-MDIX is enabled, the interface automatically detects the required cable connection type (straight-through or crossover) and configures the connection appropriately.

When you enable auto-MDIX on an interface, you must also set the interface speed and duplex to **auto** so that the feature operates correctly.

When auto-MDIX (and autonegotiation of speed and duplex) is enabled on one or both of the connected interfaces, link up occurs, even if the cable type (straight-through or crossover) is incorrect.

You can verify the operational state of auto-MDIX on the interface by entering the **show controllers ethernet-controller interface-id phy** privileged EXEC command.

**Examples** This example shows how to enable auto-MDIX on a port:

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# speed auto
Switch(config-if)# duplex auto
Switch(config-if)# mdix auto
Switch(config-if)# end
```

Related Commands	Command	Description
	<a href="#">show controllers ethernet-controller</a>	Displays per-interface send and receive statistics read from the hardware with keywords.

## mode (power-stack configuration)

To configure power stack mode for the power stack, use the **mode** command in power-stack configuration mode. To return to the default settings, use the **no** form of the command.

**mode** {power-shared|redundant} [strict]

**no mode**

### Syntax Description

<b>power-shared</b>	Sets the power stack to operate in power-shared mode. This is the default.
<b>redundant</b>	Sets the power stack to operate in redundant mode. The largest power supply is removed from the power pool to be used as backup power in case one of the other power supplies fails.
<b>strict</b>	(Optional) Configures the power stack mode to run a strict power budget. The stack power needs cannot exceed the available power.

### Command Default

The default modes are **power-shared** and nonstrict.

### Command Modes

Power-stack configuration

### Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

### Usage Guidelines

This command is available only on switch stacks running the IP Base or IP Services feature set.

To access power-stack configuration mode, enter the **stack-power stack** *power stack name* global configuration command.

Entering the **no mode** command sets the switch to the defaults of **power-shared** and non-strict mode.



#### Note

For stack power, available power is the total power available for PoE from all power supplies in the power stack, available power is the power allocated to all powered devices connected to PoE ports in the stack, and consumed power is the actual power consumed by the powered devices.

In **power-shared** mode, all of the input power can be used for loads, and the total available power appears as one large power supply. The power budget includes all power from all supplies. No power is set aside for power supply failures. If a power supply fails, load shedding (shutting down of powered devices or switches) might occur.

In **redundant** mode, the largest power supply is removed from the power pool to use as backup power in case one of the other power supplies fails. The available power budget is the total power minus the largest power supply. This reduces the available power in the pool for switches and powered devices, but in case of a failure or an extreme power load, there is less chance of having to shut down switches or powered devices.

In **strict** mode, when a power supply fails and the available power drops below the budgeted power, the system balances the budget through load shedding of powered devices, even if the actual power is less than the available power. In nonstrict mode, the power stack can run in an over-allocated state and is stable as long as the actual power does not exceed the available power. In this mode, a powered device drawing more than normal power could cause the power stack to start shedding loads. This is normally not a problem because most devices do not run at full power. The chances of multiple powered devices in the stack requiring maximum power at the same time is small.

In both strict and nonstrict modes, power is denied when there is no power available in the power budget.

### Examples

This is an example of setting the power stack mode for the stack named power1 to power-shared with strict power budgeting. All power in the stack is shared, but when the total available power is allotted, no more devices are allowed power.

```
Switch(config)# stack-power stack power1
Switch(config-stackpower)# mode power-shared strict
Switch(config-stackpower)# exit
```

This is an example of setting the power stack mode for the stack named power2 to redundant. The largest power supply in the stack is removed from the power pool to provide redundancy in case one of the other supplies fails.

```
Switch(config)# stack-power stack power2
Switch(config-stackpower)# mode redundant
Switch(config-stackpower)# exit
```

### Related Commands

Command	Description
<a href="#">stack-power</a>	Configures StackPower parameters for the power stack or for a switch in the power stack.

# network-policy

To apply a network-policy profile to an interface, use the **network-policy** command in interface configuration mode. To remove the policy, use the **no** form of this command.

**network-policy** *profile-number*

**no network-policy**

## Syntax Description

<i>profile-number</i>	The network-policy profile number to apply to the interface.
-----------------------	--

## Command Default

No network-policy profiles are applied.

## Command Modes

Interface configuration

## Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

## Usage Guidelines

Use the **network-policy** *profile number* interface configuration command to apply a profile to an interface.

You cannot apply the **switchport voice vlan** command on an interface if you first configure a network-policy profile on it. However, if **switchport voice vlan** *vlan-id* is already configured on the interface, you can apply a network-policy profile on the interface. The interface then has the voice or voice-signaling VLAN network-policy profile applied.

## Examples

This example shows how to apply network-policy profile 60 to an interface:

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# network-policy 60
```

## Related Commands

Command	Description
<a href="#">network-policy profile (global configuration)</a>	Creates a network-policy profile and enters network-policy configuration mode.
<a href="#">show network-policy profile</a>	Displays the network-policy profiles.
<a href="#">voice-signaling vlan (network-policy configuration)</a>	Creates a network-policy profile for the voice-signaling application type.

Command	Description
<a href="#">voice vlan (network-policy configuration)</a>	Creates a network-policy profile for the voice application type.

## network-policy profile (global configuration)

To create a network-policy profile and to enter network-policy configuration mode, use the **network-policy profile** command in global configuration mode. To delete the policy and to return to global configuration mode, use the **no** form of this command.

**network-policy profile** *profile-number*

**no network-policy profile** *profile-number*

### Syntax Description

<i>profile-number</i>	Network-policy profile number. The range is 1 to 4294967295.
-----------------------	--

### Command Default

No network-policy profiles are defined.

### Command Modes

Global configuration

### Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

### Usage Guidelines

Use the **network-policy profile** global configuration command to create a profile and to enter network-policy profile configuration mode.

To return to privileged EXEC mode from the network-policy profile configuration mode, enter the **exit** command.

When you are in network-policy profile configuration mode, you can create the profile for voice and voice signaling by specifying the values for VLAN, class of service (CoS), differentiated services code point (DSCP), and tagging mode.

These profile attributes are contained in the Link Layer Discovery Protocol for Media Endpoint Devices (LLDP-MED) network-policy time-length-value (TLV).

### Examples

This example shows how to create network-policy profile 60:

```
Switch(config)# network-policy profile 60
Switch(config-network-policy)#
```

### Related Commands

Command	Description
<a href="#">network-policy</a>	Applies a network-policy profile to an interface.

Command	Description
<a href="#">show network-policy profile</a>	Displays the network-policy profiles.
<a href="#">voice-signaling vlan (network-policy configuration)</a>	Creates a network-policy profile for the voice-signaling application type.
<a href="#">voice vlan (network-policy configuration)</a>	Creates a network-policy profile for the voice application type.

## nmsp attachment suppress

To suppress the reporting of attachment information from a specified interface, use the **nmsp attachment suppress** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

**nmsp attachment suppress**

**no nmsp attachment suppress**

**Syntax Description** This command has no arguments or keywords.

**Command Default** None

**Command Modes** Interface configuration

Command History	Release	Modification
	Cisco IOS XE 3.2SE	This command was introduced.

**Usage Guidelines** Use the **nmsp attachment suppress** interface configuration command to configure an interface to not send location and attachment notifications to a Cisco Mobility Services Engine (MSE).

**Examples** This example shows how to configure an interface to not send attachment information to the MSE:

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# nmsp attachment suppress
```

Related Commands	Command	Description
	show nmsp	Displays the NMSP information for the switch.

# power efficient-ethernet auto

To enable Energy Efficient Ethernet (EEE) for an interface, use the **power efficient-ethernet auto** command in interface configuration mode. To disable EEE on an interface, use the **no** form of this command.

**power efficient-ethernet auto**

**no power efficient-ethernet auto**

**Syntax Description** This command has no arguments or keywords.

**Command Default** EEE is disabled.

**Command Modes** Interface configuration

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE 3.2SE	This command was introduced.

**Usage Guidelines** You can enable EEE on devices that support low power idle (LPI) mode. Such devices can save power by entering LPI mode during periods of low utilization. In LPI mode, systems on both ends of the link can save power by shutting down certain services. EEE provides the protocol needed to transition into and out of LPI mode in a way that is transparent to upper layer protocols and applications.

The **power efficient-ethernet auto** command is available only if the interface is EEE capable. To check if an interface is EEE capable, use the **show eee capabilities EXEC** command.

When EEE is enabled, the switch advertises and autonegotiates EEE to its link partner. To view the current EEE status for an interface, use the **show eee status EXEC** command.

This command does not require a license.

**Examples** This example shows how to enable EEE for an interface:

```
Switch(config-if) # power efficient-ethernet auto
Switch(config-if) #
```

This example shows how to disable EEE for an interface:

```
Switch(config-if) # no power efficient-ethernet auto
Switch(config-if) #
```

## power-priority

To configure Cisco StackPower power-priority values for a switch in a power stack and for its high-priority and low-priority PoE ports, use the **power-priority** command in switch stack-power configuration mode. To return to the default setting, use the **no** form of the command.

**power-priority** {**high** *value*| **low** *value*| **switch** *value*}

**no power-priority** {**high**| **low**| **switch**}

### Syntax Description

<b>high</b> <i>value</i>	Sets the power priority for the ports configured as high-priority ports. The range is 1 to 27, with 1 as the highest priority. The <b>high</b> value must be lower than the value set for the low-priority ports and higher than the value set for the switch.
<b>low</b> <i>value</i>	Sets the power priority for the ports configured as low-priority ports. The range is 1 to 27. The <b>low</b> value must be higher than the value set for the high-priority ports and the value set for the switch.
<b>switch</b> <i>value</i>	Sets the power priority for the switch. The range is 1 to 27. The <b>switch</b> value must be lower than the values set for the low and high-priority ports.

### Command Default

If no values are configured, the power stack randomly determines a default priority.

The default ranges are 1 to 9 for switches, 10 to 18 for high-priority ports, 19 to 27 for low-priority ports.

On non-PoE switches, the high and low values (for port priority) have no effect.

### Command Modes

Switch stack-power configuration

### Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

### Usage Guidelines

To access switch stack-power configuration mode, enter the **stack-power switch** *switch-number* global configuration command.

Cisco StackPower power-priority values determine the order for shutting down switches and ports when power is lost and load shedding must occur. Priority values are from 1 to 27; the highest numbers are shut down first.

We recommend that you configure different priority values for each switch and for its high priority ports and low priority ports to limit the number of devices shut down at one time during a loss of power. If you try to configure the same priority value on different switches in a power stack, the configuration is allowed, but you receive a warning message.

**Note**

This command is available only on switch stacks running the IP Base or IP Services feature set.

**Examples**

This is an example of setting the power priority for switch 1 in power stack a to 7, for the high-priority ports to 11, and for the low-priority ports to 20.

```
Switch(config)# stack-power switch 1  
Switch(config-switch-stackpower) # stack-id power_stack_a  
Switch(config-switch-stackpower) # power-priority high 11  
Switch(config-switch-stackpower) # power-priority low 20  
Switch(config-switch-stackpower) # power-priority switch 7  
Switch(config-switch-stackpower) # exit
```

**Related Commands**

Command	Description
<a href="#">stack-power</a>	Configures StackPower parameters for the power stack or for a switch in the power stack.
<a href="#">show stack-power</a>	Displays information about StackPower stacks or switches in a power stack.

## power inline

To configure the power management mode on Power over Ethernet (PoE) ports, use the **power inline** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

**power inline** {**auto** [**max** *max-wattage*]| **four-pair forced**| **never**| **port priority** {**high** | **low**} | **static** [**max** *max-wattage*]}

**no power inline** {**auto**| **four-pair forced**| **never**| **port priority** {**high** | **low**}| **static** [**max** *max-wattage*]}

### Syntax Description

<b>auto</b>	Enables powered-device detection. If enough power is available, automatically allocates power to the PoE port after device detection. Allocation is first-come, first-serve.
<b>max</b> <i>max-wattage</i>	(Optional) Limits the power allowed on the port. The range is 4000 to 30000 mW. If no value is specified, the maximum is allowed.
<b>four-pair forced</b>	(Optional) Enable Four-pair PoE without L2 negotiation (Cisco UPOE switches only).
<b>never</b>	Disables device detection, and disables power to the port.
<b>port</b>	Configures the power priority of the port. The default priority is low.
<b>priority</b> { <b>high</b>   <b>low</b> }	Sets the power priority of the port. In case of a power supply failure, ports configured as low priority are turned off first and ports configured as high priority are turned off last. The default priority is low.
<b>static</b>	Enables powered-device detection. Pre-allocates (reserves) power for a port before the switch discovers the powered device. This action guarantees that the device connected to the interface receives enough power.

### Command Default

The default is **auto** (enabled).

The maximum wattage is 30,000 mW.

The default port priority is low.

### Command Default

Interface configuration

### Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.
Cisco IOS XE 3.3SE	The <b>four-pair forced</b> keywords were added.

### Usage Guidelines

This command is supported only on PoE-capable ports. If you enter this command on a port that does not support PoE, this error message appears:

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# power inline auto
                        ^
% Invalid input detected at '^' marker.
```

In a switch stack, this command is supported on all ports in the stack that support PoE.

Cisco Universal Power Over Ethernet (Cisco UPOE) is a Cisco proprietary technology that extends the IEEE 802.3at PoE standard to provide the capability to source up to 60 W of power over standard Ethernet cabling infrastructure (Class D or better) by using the spare pair of an RJ-45 cable (wires 4,5,7,8) with the signal pair (wires 1,2,3,6). Power on the spare pair is enabled when the switch port and end device mutually identify themselves as Cisco UPOE-capable using CDP or LLDP and the end device requests for power to be enabled on the spare pair. When the spare pair is powered, the end device can negotiate up to 60 W of power from the switch using CDP or LLDP. Use the **power inline four-pair forced** command when the end device is PoE-capable on both signal and spare pairs, but does not support the CDP or LLDP extensions required for Cisco UPOE.

Use the **max max-wattage** option to disallow higher-power powered devices. With this configuration, when the powered device sends Cisco Discovery Protocol (CDP) messages requesting more power than the maximum wattage, the switch removes power from the port. If the powered-device IEEE class maximum is greater than the maximum wattage, the switch does not power the device. The power is reclaimed into the global power budget.



#### Note

The switch never powers any class 0 or class 3 device if the **power inline max max-wattage** command is configured for less than 30 W.

If the switch denies power to a powered device (the powered device requests more power through CDP messages or if the IEEE class maximum is greater than the maximum wattage), the PoE port is in a power-deny state. The switch generates a system message, and the Oper column in the **show power inline** privileged EXEC command output shows *power-deny*.

Use the **power inline static max max-wattage** command to give a port high priority. The switch allocates PoE to a port configured in static mode before allocating power to a port configured in auto mode. The switch

reserves power for the static port when it is configured rather than upon device discovery. The switch reserves the power on a static port even when there is no connected device and whether or not the port is in a shutdown or in a no shutdown state. The switch allocates the configured maximum wattage to the port, and the amount is never adjusted through the IEEE class or by CDP messages from the powered device. Because power is pre-allocated, any powered device that uses less than or equal to the maximum wattage is guaranteed power when it is connected to a static port. However, if the powered device IEEE class is greater than the maximum wattage, the switch does not supply power to it. If the switch learns through CDP messages that the powered device needs more than the maximum wattage, the powered device is shut down.

If the switch cannot pre-allocate power when a port is in static mode (for example, because the entire power budget is already allocated to other auto or static ports), this message appears: Command rejected: power inline static: pwr not available. The port configuration remains unchanged.

When you configure a port by using the **power inline auto** or the **power inline static** interface configuration command, the port autonegotiates by using the configured speed and duplex settings. This is necessary to determine the power requirements of the connected device (whether or not it is a powered device). After the power requirements have been determined, the switch hardcodes the interface by using the configured speed and duplex settings without resetting the interface.

When you configure a port by using the **power inline never** command, the port reverts to the configured speed and duplex settings.

If a port has a Cisco powered device connected to it, you should not use the **power inline never** command to configure the port. A false link-up can occur, placing the port in an error-disabled state.

Use the **power inline port priority {high | low}** command to configure the power priority of a PoE port. Powered devices connected to ports with low port priority are shut down first in case of a power shortage.

You can verify your settings by entering the **show power inline EXEC** command.

## Examples

This example shows how to enable detection of a powered device and to automatically power a PoE port on a switch:

```
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# power inline auto
```

This example shows how to automatically enable power on both signal and spare pairs from switch port Gigabit Ethernet 1/0/1:

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# power inline four-pair forced
```

This example shows how to configure a PoE port on a switch to allow a class 1 or a class 2 powered device:

```
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# power inline auto max 7000
```

This example shows how to disable powered-device detection and to not power a PoE port on a switch:

```
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# power inline never
```

This example shows how to set the priority of a port to high, so that it would be one of the last ports to be shut down in case of power supply failure:

```
Switch(config)# interface gigabitethernet1/0/2
```

```
Switch(config-if)# power inline port priority high
```

**Related Commands**

Command	Description
<a href="#">logging event power-inline-status</a>	Enables the logging of PoE events.
<a href="#">show power inline</a>	Displays the PoE status for the specified PoE port, the specified stack member, or for all PoE ports in the switch stack.

# power inline police

To enable policing of real-time power consumption on a powered device, use the **power inline police** command in interface configuration mode. To disable this feature, use the **no** form of this command

**power inline police** [**action** {**errdisable**|**log**}]

**no power inline police**

## Syntax Description

<b>action errdisable</b>	(Optional) Configures the switch to turn off power to the port if the real-time power consumption exceeds the maximum power allocation on the port. This is the default action.
<b>action log</b>	(Optional) Configures the switch to generate a syslog message while still providing power to a connected device if the real-time power consumption exceeds the maximum power allocation on the port.

## Command Default

Policing of the real-time power consumption of the powered device is disabled.

## Command Modes

Interface configuration

## Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

## Usage Guidelines

This command is supported only on the LAN Base image.

This command is supported only on Power over Ethernet (PoE)-capable ports. If you enter this command on a switch or port that does not support PoE, an error message appears.

In a switch stack, this command is supported on all switches or ports in the stack that support PoE and real-time power-consumption monitoring.

When policing of the real-time power consumption is enabled, the switch takes action when a powered device consumes more power than the allocated maximum amount.

When PoE is enabled, the switch senses the real-time power consumption of the powered device. This feature is called *power monitoring* or *power sensing*. The switch also polices the power usage with the *power policing* feature.

When power policing is enabled, the switch uses one of the these values as the cutoff power on the PoE port in this order:

- 1 The user-defined power level that limits the power allowed on the port when you enter the **power inline auto max** *max-wattage* or the **power inline static max** *max-wattage* interface configuration command

- The switch automatically sets the power usage of the device by using CDP power negotiation or by the IEEE classification and LLDP power negotiation.

If you do not manually configure the cutoff-power value, the switch automatically determines it by using CDP power negotiation or the device IEEE classification and LLDP power negotiation. If CDP or LLDP are not enabled, the default value of 30 W is applied. However without CDP or LLDP, the switch does not allow devices to consume more than 15.4 W of power because values from 15400 to 30000 mW are only allocated based on CDP or LLDP requests. If a powered device consumes more than 15.4 W without CDP or LLDP negotiation, the device might be in violation of the maximum current *I<sub>max</sub>* limitation and might experience an *I<sub>cut</sub>* fault for drawing more current than the maximum. The port remains in the fault state for a time before attempting to power on again. If the port continuously draws more than 15.4 W, the cycle repeats.

When a powered device connected to a PoE+ port restarts and sends a CDP or LLDP packet with a power TLV, the switch locks to the power-negotiation protocol of that first packet and does not respond to power requests from the other protocol. For example, if the switch is locked to CDP, it does not provide power to devices that send LLDP requests. If CDP is disabled after the switch has locked on it, the switch does not respond to LLDP power requests and can no longer power on any accessories. In this case, you should restart the powered device.

If power policing is enabled, the switch polices power usage by comparing the real-time power consumption to the maximum power allocated on the PoE port. If the device uses more than the maximum power allocation (or *cutoff power*) on the port, the switch either turns power off to the port, or the switch generates a syslog message and updates the LEDs (the port LEDs are blinking amber) while still providing power to the device.

- To configure the switch to turn off power to the port and put the port in the error-disabled state, use the **power inline police** interface configuration command.
- To configure the switch to generate a syslog message while still providing power to the device, use the **power inline police action log** command.

If you do not enter the **action log** keywords, the default action is to shut down the port, turn off power to it, and put the port in the PoE error-disabled state. To configure the PoE port to automatically recover from the error-disabled state, use the **errdisable detect cause inline-power** global configuration command to enable error-disabled detection for the PoE cause and the **errdisable recovery cause inline-power interval interval** global configuration command to enable the recovery timer for the PoE error-disabled cause.



#### Caution

If policing is disabled, no action occurs when the powered device consumes more than the maximum power allocation on the port, which could adversely affect the switch.

You can verify your settings by entering the **show power inline police** privileged EXEC command.

#### Examples

This example shows how to enable policing of the power consumption and configuring the switch to generate a syslog message on the PoE port on a switch:

```
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# power inline police action log
```

#### Related Commands

Command	Description
<a href="#">power inline</a>	Configures the power management mode on PoE ports.

Command	Description
<a href="#">show power inline</a>	Displays the PoE status for the specified PoE port, the specified stack member, or for all PoE ports in the switch stack.

# power supply

To configure and manage the internal power supplies on a switch, use the **power supply** command in privileged EXEC mode.

**power supply** *stack-member-number* **slot** {A| B} {off| on}

## Syntax Description

<i>stack-member-number</i>	Stack member number for which to configure the internal power supplies. The range is 1 to 9, depending on the number of switches in the stack.  This parameter is available only on stacking-capable switches.
<b>slot</b>	Selects the switch power supply to set.
<b>A</b>	Selects the power supply in slot A.
<b>B</b>	Selects the power supply in slot B.  <b>Note</b> Power supply slot B is the closest slot to the outer edge of the switch.
<b>off</b>	Sets the switch power supply to off.
<b>on</b>	Sets the switch power supply to on.

## Command Default

The switch power supply is on.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.
Cisco IOS XE 3.3SE	The <b>slot</b> keyword replaced the <b>frufep</b> keyword.

## Usage Guidelines

The **power supply** command applies to a switch or to a switch stack where all switches are the same platform. In a switch stack with the same platform switches, you must specify the stack member before entering the **slot** {A | B} **off** or **on** keywords.

To return to the default setting, use the **power supply** *stack-member-number* **on** command.

You can verify your settings by entering the **show env power** privileged EXEC command.

**Examples**

This example shows how to set the power supply in slot A to off:

```
Switch> power supply 2 slot A off
Disabling Power supply A may result in a power loss to PoE devices and/or switches ...
Continue? (yes/[no]): yes
Switch
Jun 10 04:52:54.389: %PLATFORM_ENV-6-FRU_PS_OIR: FRU Power Supply 1 powered off
Jun 10 04:52:56.717: %PLATFORM_ENV-1-FAN_NOT_PRESENT: Fan is not present
```

This example shows how to set the power supply in slot A to on:

```
Switch> power supply 1 slot B on
Jun 10 04:54:39.600: %PLATFORM_ENV-6-FRU_PS_OIR: FRU Power Supply 1 powered on
```

This example shows the output of the show env power command:

```
Switch> show env power
SW  PID                Serial#      Status          Sys Pwr  PoE Pwr  Watts
--  -
1A  PWR-1RUC2-640WAC     DCB1705B05B OK           Good     Good     250/390
1B  Not Present
```

**Related Commands**

Command	Description
<a href="#">show env</a>	Displays fan, temperature, RPS availability, and power information.

# show CAPWAP summary

To display all the CAPWAP tunnels established by the controller to access points and other mobility controllers use the **show CAPWAP summary** command.

**show CAPWAP summary**

**Syntax Description** This command has no arguments or keywords.

**Command Default** None

**Command Modes** Global configuration

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE 3.2SE	This command was introduced.

**Examples** This example shows how to display CAPWAP tunnels established by the controllers to the access points and other controllers.

```
Switch# show capwap summary
CAPWAP Tunnels General Statistics:
Number of Capwap Data Tunnels = 8
Number of Capwap Mobility Tunnels = 0
Number of Capwap Multicast Tunnels = 0
Name APName Type PhyPortIf Mode McastIf
-----
Ca4 AP-Behind-Router data - unicast -
Ca0 AP1142-kat data - unicast -
Ca5 APRFCHAMBER2-EDISON data - unicast -
Ca6 KATANA_2_RF data - unicast -
Ca1 AP-1040-RF data - unicast -
Ca7 KATANA_1_RF data - unicast -
Ca2 AP3500-2027 data - unicast -
Ca3 AP-1040-out data - unicast -
```

# show controllers cpu-interface

To display the state of the CPU network interface ASIC and the send and receive statistics for packets reaching the CPU, use the **show controllers cpu-interface** command in privileged EXEC mode.

**show controllers cpu-interface** [*switch stack-member-number*]

## Syntax Description

<b>switch</b> <i>stack-member-number</i>	(Optional) Specifies the stack member number.
--	---

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

## Usage Guidelines

This display provides information that might be useful for Cisco technical support representatives troubleshooting the switch.

## Examples

This is a partial output example from the **show controllers cpu-interface** command:

```
Switch# show controllers cpu-interface switch 1
cpu-queue-frames  retrieved dropped invalid hol-block
```

```
-----
Routing Protocol          0          0          0          0
L2 Protocol               241567         0          0          0
sw forwarding             0            0          0          0
broadcast                 68355         0          0          0
icmp                      0            0          0          0
icmp redirect             0            0          0          0
logging                   0            0          0          0
rpf-fail                   0            0          0          0
DOT1X authentication 328174  0            0          0
Forus Traffic              0            0          0          0
Forus Resolution          0            0          0          0
Wireless q5                0            0          0          0
Wireless q1                0            0          0          0
Wireless q2                0            0          0          0
Wireless q3                0            0          0          0
Wireless q4                0            0          0          0
Learning cache             0            0          0          0
Topology control          820408         0          0          0
Proto snooping             0            0          0          0
BFD Low latency            0            0          0          0
Transit Traffic            0            0          0          0
Multi End station          0            0          0          0
```

Health Check	0	0	0	0
Crypto control	0	0	0	0
Exception	0	0	0	0
General Punt	0	0	0	0
NFL sampled data	0	0	0	0
STG cache	0	0	0	0
EGR exception	0	0	0	0
show forward	0	0	0	0
Multicast data	0	0	0	0
Gold packet	0	0	0	0

**Related Commands**

Command	Description
<a href="#">show controllers ethernet-controller</a>	Displays per-interface send and receive statistics read from the hardware with keywords.
<a href="#">show interfaces</a>	Displays the administrative and operational status of all interfaces or a specified interface.

## show controllers ethernet-controller

To display per-interface send and receive statistics read from the hardware with keywords, use the **show controllers ethernet-controller** command in EXEC mode.

```
show controllers ethernet-controller [interface-id] [down-when-looped|phy [detail]] [port-asic statistics
{exceptions|interface interface-id {I2|I3}|I3-ifid if-id|port-ifid if-id|vlan-ifid if-id} [switch
stack-member-number] [asic asic-number]
```

### Syntax Description

<i>interface-id</i>	(Optional) ID of the physical interface.
<b>down-when-looped</b>	(Optional) Displays states related to down-when-looped detection.
<b>phy</b>	(Optional) Displays the status of the internal registers on the switch physical layer device (PHY) for the device or the interface. This display includes the operational state of the automatic medium-dependent interface crossover (auto-MDIX) feature on an interface.
<b>detail</b>	(Optional) Displays details about the PHY internal registers.
<b>port-asic</b>	(Optional) Displays information about the port ASIC internal registers.
<b>statistics</b>	Displays port ASIC statistics, including the Rx/Sup Queue and miscellaneous statistics.
<b>exceptions</b>	Displays port ASIC exception statistics.
<b>interface</b> <i>interface-id</i>	Specifies the interface for which to display port ASIC statistics.
<b>I2</b>	Displays statistics for the Layer 2 interface.
<b>I3</b>	Displays statistics for the Layer 3 interface.
<b>I3-ifid</b> <i>if-id</i>	Specifies the Layer 3 IF interface ID for which to display port ASIC statistics.
<b>port-ifid</b> <i>if-id</i>	Specifies the PortIF interface ID for which to display port ASIC statistics.
<b>vlan-ifid</b> <i>if-id</i>	Specifies the VLANIF interface ID for which to display port ASIC statistics.
<b>switch</b> <i>stack-member-number</i>	(Optional) Specifies the stack member number for which to display send and receive statistics.
<b>asic</b> <i>asic-number</i>	(Optional) Specifies the ASIC number.

### Command Modes

User EXEC (only supported with the *interface-id* keywords in user EXEC mode)

Privileged EXEC

### Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

### Usage Guidelines

Without keywords, this command provides the RMON statistics for all interfaces or for the specified interface. To display the interface internal registers, use the **phy** keyword. To display information about the port ASIC, use the **port-asic** keyword.

When you enter the **phy** or **port-asic** keywords, the displayed information is useful primarily for Cisco technical support representatives troubleshooting the switch.

### Examples

This is an example of output from the **show controllers ethernet-controller** command for an interface:

```
Switch# show controllers ethernet-controller gigabitEthernet1/0/1
Transmit          GigabitEthernet1/0/1          Receive
19216827 Total bytes          0 Total bytes
   41935 Unicast frames        0 Unicast frames
2683840 Unicast bytes         0 Unicast bytes
   216662 Multicast frames     0 Multicast frames
16532987 Multicast bytes      0 Multicast bytes
   0 Broadcast frames         0 Broadcast frames
   0 Broadcast bytes          0 Broadcast bytes
   0 System FCS error frames   0 IpgViolation frames
   0 MacUnderrun frames       0 MacOverrun frames
   0 Pause frames             0 Pause frames
   0 Cos 0 Pause frames        0 Cos 0 Pause frames
   0 Cos 1 Pause frames        0 Cos 1 Pause frames
   0 Cos 2 Pause frames        0 Cos 2 Pause frames
   0 Cos 3 Pause frames        0 Cos 3 Pause frames
   0 Cos 4 Pause frames        0 Cos 4 Pause frames
   0 Cos 5 Pause frames        0 Cos 5 Pause frames
   0 Cos 6 Pause frames        0 Cos 6 Pause frames
   0 Cos 7 Pause frames        0 Cos 7 Pause frames
   0 Oam frames                0 OamProcessed frames
   0 Oam frames                0 OamDropped frames
251598 Minimum size frames    0 Minimum size frames
   0 65 to 127 byte frames     0 65 to 127 byte frames
   0 128 to 255 byte frames    0 128 to 255 byte frames
6999 256 to 511 byte frames   0 256 to 511 byte frames
   0 512 to 1023 byte frames   0 512 to 1023 byte frames
   0 1024 to 1518 byte frames  0 1024 to 1518 byte frames
   0 1519 to 2047 byte frames  0 1519 to 2047 byte frames
   0 2048 to 4095 byte frames  0 2048 to 4095 byte frames
   0 4096 to 8191 byte frames  0 4096 to 8191 byte frames
   0 8192 to 16383 byte frames 0 8192 to 16383 byte frames
   0 16384 to 32767 byte frame 0 16384 to 32767 byte frame
   0 > 32768 byte frames      0 > 32768 byte frames
   0 Late collision frames     0 SymbolErr frames
   0 Excess Defer frames       0 Collision fragments
   0 Good (1 coll) frames      0 ValidUnderSize frames
   0 Good (>1 coll) frames    0 InvalidOverSize frames
   0 Deferred frames          0 ValidOverSize frames
   0 Gold frames dropped       0 FcsErr frames
   0 Gold frames truncated
   0 Gold frames successful
   0 1 collision frames
   0 2 collision frames
   0 3 collision frames
   0 4 collision frames
```

```

0 5 collision frames
0 6 collision frames
0 7 collision frames
0 8 collision frames
0 9 collision frames
0 10 collision frames
0 11 collision frames
0 12 collision frames
0 13 collision frames
0 14 collision frames
0 15 collision frames
0 Excess collision frames

```

LAST UPDATE 850 msec AGO

**Table 1: Transmit Field Descriptions**

Field	Description
Total bytes	The total number of bytes sent on an interface.
Unicast Frames	The total number of frames sent to unicast addresses.
Unicast bytes	The total number of bytes sent to unicast addresses.
Multicast frames	The total number of frames sent to multicast addresses.
Multicast bytes	The total number of bytes sent to multicast addresses.
Broadcast frames	The total number of frames sent to broadcast addresses.
Broadcast bytes	The total number of bytes sent to broadcast addresses.
System FCS error frames	The total number of frames that fail the Frame Check Sequence (FCS).
MacUnderrun frames	The total number of frames that have MAC Underrun errors.
Pause frames	The total number of pause frames sent on an interface.
Cos x Pause frames	The total number of class of service (CoS) x pause frames sent on an interface.
Oam frames	The total number of Ethernet Operations, Administration, and Maintenance (OAM) frames sent on an interface.
Minimum size frames	The number of frames that are the minimum allowed frame size.
65 to 127 byte frames	The total number of frames sent on an interface that are 65 to 127 bytes.
128 to 255 byte frames	The total number of frames sent on an interface that are 128 to 255 bytes.
256 to 511 byte frames	The total number of frames sent on an interface that are 256 to 511 bytes.
512 to 1023 byte frames	The total number of frames sent on an interface that are 512 to 1023 bytes.

Field	Description
1024 to 1518 byte frames	The total number of frames sent on an interface that are 1024 to 1518 bytes.
1519 to 2047 byte frames	The total number of frames sent on an interface that are 1519 to 2047 bytes.
2048 to 4095 byte frames	The total number of frames sent on an interface that are 2048 to 4095 bytes.
4096 to 8191 byte frames	The total number of frames sent on an interface that are 4096 to 8191 bytes.
8192 to 16383 byte frames	The total number of frames sent on an interface that are 8192 to 16383 bytes.
16384 to 32767 byte frames	The total number of frames sent on an interface that are 16384 to 32767 bytes.
> 32768 byte frames	The total number of frames sent on an interface that are greater than 32768 bytes.
Late collision frames	After a frame is sent, the number of frames dropped because late collisions were detected while the frame was sent.
Excess defer frames	The number of frames that are not sent after the time exceeds the maximum-packet time.
Good (1 coll) frames	The number of frames that are successfully sent on an interface after one collision occurs. This value does not include the number of frames that are not successfully sent after one collision occurs.
Good (>1 coll) frames	The number of frames that are successfully sent on an interface after more than one collision occurs. This value does not include the number of frames that are not successfully sent after more than one collision occurs.
Deferred frames	The number of frames that are not sent after the time exceeds 2*maximum-packet time.
Gold frames dropped	The number of gold frames that are dropped.
Gold frames truncated	The number of gold frames that are truncated.
Gold frames successful	The number of gold frames that are successful.
1 collision frames	The number of frames that are successfully sent on an interface after one collision occurs.
2 collision frames	The number of frames that are successfully sent on an interface after two collisions occur.
3 collision frames	The number of frames that are successfully sent on an interface after three collisions occur.

Field	Description
4 collision frames	The number of frames that are successfully sent on an interface after four collisions occur.
5 collision frames	The number of frames that are successfully sent on an interface after five collisions occur.
6 collision frames	The number of frames that are successfully sent on an interface after six collisions occur.
7 collision frames	The number of frames that are successfully sent on an interface after seven collisions occur.
8 collision frames	The number of frames that are successfully sent on an interface after eight collisions occur.
9 collision frames	The number of frames that are successfully sent on an interface after nine collisions occur.
10 collision frames	The number of frames that are successfully sent on an interface after ten collisions occur.
11 collision frames	The number of frames that are successfully sent on an interface after 11 collisions occur.
12 collision frames	The number of frames that are successfully sent on an interface after 12 collisions occur.
13 collision frames	The number of frames that are successfully sent on an interface after 13 collisions occur.
14 collision frames	The number of frames that are successfully sent on an interface after 14 collisions occur.
15 collision frames	The number of frames that are successfully sent on an interface after 15 collisions occur.
Excess collisions	The number of frames that could not be sent on an interface after 16 collisions occur.

**Table 2: Transmit Field Descriptions**

Field	Description
Bytes	The total number of bytes sent on an interface.
Unicast Frames	The total number of frames sent to unicast addresses.

Field	Description
Multicast frames	The total number of frames sent to multicast addresses.
Broadcast frames	The total number of frames sent to broadcast addresses.
Too old frames	The number of frames dropped on the egress port because the packet aged out.
Deferred frames	The number of frames that are not sent after the time exceeds 2*maximum-packet time.
MTU exceeded frames	The number of frames that are larger than the maximum allowed frame size.
1 collision frames	The number of frames that are successfully sent on an interface after one collision occurs.
2 collision frames	The number of frames that are successfully sent on an interface after two collisions occur.
3 collision frames	The number of frames that are successfully sent on an interface after three collisions occur.
4 collision frames	The number of frames that are successfully sent on an interface after four collisions occur.
5 collision frames	The number of frames that are successfully sent on an interface after five collisions occur.
6 collision frames	The number of frames that are successfully sent on an interface after six collisions occur.
7 collision frames	The number of frames that are successfully sent on an interface after seven collisions occur.
8 collision frames	The number of frames that are successfully sent on an interface after eight collisions occur.
9 collision frames	The number of frames that are successfully sent on an interface after nine collisions occur.
10 collision frames	The number of frames that are successfully sent on an interface after ten collisions occur.
11 collision frames	The number of frames that are successfully sent on an interface after 11 collisions occur.

Field	Description
12 collision frames	The number of frames that are successfully sent on an interface after 12 collisions occur.
13 collision frames	The number of frames that are successfully sent on an interface after 13 collisions occur.
14 collision frames	The number of frames that are successfully sent on an interface after 14 collisions occur.
15 collision frames	The number of frames that are successfully sent on an interface after 15 collisions occur.
Excessive collisions	The number of frames that could not be sent on an interface after 16 collisions occur.
Late collisions	After a frame is sent, the number of frames dropped because late collisions were detected while the frame was sent.
VLAN discard frames	The number of frames dropped on an interface because the CFI <sup>1</sup> bit is set.
Excess defer frames	The number of frames that are not sent after the time exceeds the maximum-packet time.
64 byte frames	The total number of frames sent on an interface that are 64 bytes.
127 byte frames	The total number of frames sent on an interface that are from 65 to 127 bytes.
255 byte frames	The total number of frames sent on an interface that are from 128 to 255 bytes.
511 byte frames	The total number of frames sent on an interface that are from 256 to 511 bytes.
1023 byte frames	The total number of frames sent on an interface that are from 512 to 1023 bytes.
1518 byte frames	The total number of frames sent on an interface that are from 1024 to 1518 bytes.
Too large frames	The number of frames sent on an interface that are larger than the maximum allowed frame size.

Field	Description
Good (1 coll) frames	The number of frames that are successfully sent on an interface after one collision occurs. This value does not include the number of frames that are not successfully sent after one collision occurs.

<sup>1</sup> CFI = Canonical Format Indicator

**Table 3: Receive Field Descriptions**

Field	Description
Total Bytes	The total amount of memory (in bytes) used by frames received on an interface, including the FCS <sup>2</sup> value and the incorrectly formed frames. This value excludes the frame header bits.
Unicast frames	The total number of frames successfully received on the interface that are directed to unicast addresses.
Unicast bytes	The total amount of memory (in bytes) used by unicast frames received on an interface, including the FCS value and the incorrectly formed frames. This value excludes the frame header bits.
Multicast frames	The total amount of memory (in bytes) used by multicast frames received on an interface, including the FCS value and the incorrectly formed frames. This value excludes the frame header bits.
Multicast bytes	The total number of bytes successfully received on the interface that are directed to multicast addresses.
Broadcast frames	The total number of frames successfully received on an interface that are directed to broadcast addresses.
Broadcast bytes	The total amount of memory (in bytes) used by broadcast frames received on an interface, including the FCS value and the incorrectly formed frames. This value excludes the frame header bits.
IpgViolation frames	The total number of frames with an interpacket gap (IPG) violation.
MacOverrun frames	The total number of frames with MacOverrun errors.
Pause frames	The total number of pause frames received on an interface.
Cos x Pause frames	The total number of class of service (CoS) x pause frames received on an interface.
OamProcessed	The total number of Ethernet Operations, Administration, and Maintenance (OAM) frames that are processed on an interface.

Field	Description
OamDropped	The total number of Ethernet Operations, Administration, and Maintenance (OAM) frames that are dropped on an interface.
Minimum size frames	The total number of frames that are the minimum frame size.
65 to 127 byte frames	The total number of frames that are from 65 to 127 bytes.
128 to 255 byte frames	The total number of frames that are from 128 to 255 bytes.
256 to 511 byte frames	The total number of frames that are from 256 to 511 bytes.
512 to 1023 byte frames	The total number of frames that are from 512 to 1023 bytes.
1024 to 1518 byte frames	The total number of frames that are from 1024 to 1518 bytes.
1519 to 2047 byte frames	The total number of frames that are from 1519 to 2047 bytes.
2048 to 4095 byte frames	The total number of frames that are from 2048 to 4095 bytes.
4096 to 8191 byte frames	The total number of frames that are from 4096 to 8191 bytes.
8192 to 16383 byte frames	The total number of frames that are from 8192 to 16383 bytes.
16384 to 32767 byte frames	The total number of frames that are from 16384 to 32767 bytes.
> 32768 byte frames	The total number of frames that are greater than 32768 bytes.
Symbol error frames	The number of frames received on an interface that have symbol errors.
Collision fragments	The number of collision fragments received on an interface.
Valid undersize frames	The number of frames received on an interface that are smaller than 64 bytes (or 68 bytes for VLAN-tagged frames) and that have valid FCS values. The frame size includes the FCS bits but excludes the frame header bits.
Invalid oversize frames	The number of frames received that were larger than maximum allowed maximum transmission unit (MTU) size (including the FCS bits and excluding the frame header) and that have either an FCS error or an alignment error.
Valid oversize frames	The number of frames received on an interface that are larger than the maximum allowed frame size and have valid FCS values. The frame size includes the FCS value but does not include the VLAN tag.
FcsErr frames	The total number of frames received on an interface that have a valid length (in bytes) but do not have the correct FCS values.

<sup>2</sup> FCS = frame check sequence

This is an example of output from the **show controllers ethernet-controller phy** command for a specific interface:

```
Switch# show controllers ethernet-controller gigabitethernet1/0/2 phy
Gi1/0/2 (gpn: 2, port-number: 2)
-----
0000 : 1140 Control Register           : 0001 0001 0100 0000
0001 : 7949 Control STATUS           : 0111 1001 0100 1001
0002 : 0141 Phy ID 1                 : 0000 0001 0100 0001
0003 : 0EE0 Phy ID 2                 : 0000 1110 1110 0000
0004 : 03E1 Auto-Negotiation Advertisement : 0000 0011 1110 0001
0005 : 0000 Auto-Negotiation Link Partner : 0000 0000 0000 0000
0006 : 0004 Auto-Negotiation Expansion Reg : 0000 0000 0000 0100
0007 : 2001 Next Page Transmit Register : 0010 0000 0000 0001
0008 : 0000 Link Partner Next page Register : 0000 0000 0000 0000
0010 : 3B60 PHY Specific Control      : 0011 1011 0110 0000
0011 : 8010 PHY Specific Status      : 1000 0000 0001 0000
0012 : 6404 PHY Specific Interrupt Enable : 0110 0100 0000 0100
0013 : 0000 PHY Specific Interrupt Status : 0000 0000 0000 0000
```

### Related Commands

Command	Description
<a href="#">show controllers cpu-interface</a>	Displays the state of the CPU network interface ASIC and the send and receive statistics for packets reaching the CPU.

# show controllers utilization

To display bandwidth utilization, use the **show controllers utilization** command in EXEC mode.

**show controllers** [*interface-id*] **utilization**

<b>Syntax Description</b>	<i>interface-id</i>	(Optional) ID of the physical interface.
<b>Command Default</b>	None	
<b>Command Modes</b>	User EXEC Privileged EXEC	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE 3.2SE	This command was introduced.

## Examples

This is an example of output from the **show controllers utilization** command:

```
Switch> show controllers utilization
Port      Receive Utilization  Transmit Utilization
Gi1/0/1   0                    0
Gi1/0/2   0                    0
Gi1/0/3   0                    0
Gi1/0/4   0                    0
Gi1/0/5   0                    0
Gi1/0/6   0                    0
Gi1/0/7   0                    0
<output truncated>
Gi2/0/1   0                    0
Gi2/0/2   0                    0
<output truncated>
Total Ports : 48
Switch Receive Bandwidth Percentage Utilization : 0
Switch Transmit Bandwidth Percentage Utilization : 0

Average Switch Percentage Utilization : 0
```

This is an example of output from the **show controllers utilization** command on a specific port:

```
Switch> show controllers gigabitethernet1/0/1 utilization
Receive Bandwidth Percentage Utilization : 0
Transmit Bandwidth Percentage Utilization : 0
```

**Table 4: Show controllers utilization Field Descriptions**

<b>Field</b>	<b>Description</b>
Receive Bandwidth Percentage Utilization	Displays the received bandwidth usage of the switch, which is the sum of the received traffic on all the ports divided by the switch receive capacity.
Transmit Bandwidth Percentage Utilization	Displays the transmitted bandwidth usage of the switch, which is the sum of the transmitted traffic on all the ports divided it by the switch transmit capacity.
Average Switch Percentage Utilization	Displays the average of the transmitted and received bandwidth usage of the switch.

# show eee

To display Energy Efficient Ethernet (EEE) information for an interface, use the **show eee** command in EXEC mode.

**show eee** {capabilities| status} interface *interface-id*

## Syntax Description

<b>capabilities</b>	Displays EEE capabilities for the specified interface.
<b>status</b>	Displays EEE status information for the specified interface.
<b>interface</b> <i>interface-id</i>	Specifies the interface for which to display EEE capabilities or status information.

## Command Default

None

## Command Modes

User EXEC  
Privileged EXEC

## Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

## Usage Guidelines

You can enable EEE on devices that support low power idle (LPI) mode. Such devices can save power by entering LPI mode during periods of low power utilization. In LPI mode, systems on both ends of the link can save power by shutting down certain services. EEE provides the protocol needed to transition into and out of LPI mode in a way that is transparent to upper layer protocols and applications.

To check if an interface is EEE capable, use the **show eee capabilities** command. You can enable EEE on an interface that is EEE capable by using the **power efficient-ethernet auto** interface configuration command.

To view the EEE status, LPI status, and wake error count information for an interface, use the **show eee status** command.

## Examples

This is an example of output from the **show eee capabilities** command on an interface where EEE is enabled:

```
Switch# show eee capabilities interface gigabitethernet1/0/1
Gi1/0/1
    EEE(efficient-ethernet):  yes (100-Tx and 1000T auto)
    Link Partner              :  yes (100-Tx and 1000T auto)
```

This is an example of output from the **show eee capabilities** command on an interface where EEE is not enabled:

```
Switch# show eee capabilities interface gigabitethernet2/0/1
Gi2/0/1
  EEE(efficient-ethernet): not enabled
  Link Partner             : not enabled
```

This is an example of output from the **show eee status** command on an interface where EEE is enabled and operational. The table that follows describes the fields in the display.

```
Switch# show eee status interface gigabitethernet1/0/4
Gi1/0/4 is up
  EEE(efficient-ethernet): Operational
  Rx LPI Status           : Received
  Tx LPI Status           : Received
```

This is an example of output from the **show eee status** command on an interface where EEE operational and the ports are in low power save mode:

```
Switch# show eee status interface gigabitethernet1/0/3
Gi1/0/3 is up
  EEE(efficient-ethernet): Operational
  Rx LPI Status           : Low Power
  Tx LPI Status           : Low Power
  Wake Error Count        : 0
```

This is an example of output from the **show eee status** command on an interface where EEE is not enabled because a remote link partner is incompatible with EEE:

```
Switch# show eee status interface gigabitethernet1/0/3
Gi1/0/3 is down
  EEE(efficient-ethernet): Disagreed
  Rx LPI Status           : None
  Tx LPI Status           : None
  Wake Error Count        : 0
```

Table 5: show eee status Field Descriptions

Field	Description
EEE (efficient-ethernet)	<p>The EEE status for the interface. This field can have any of the following values:</p> <ul style="list-style-type: none"> <li>• N/A—The port is not capable of EEE.</li> <li>• Disabled—The port EEE is disabled.</li> <li>• Disagreed—The port EEE is not set because a remote link partner might be incompatible with EEE; either it is not EEE capable, or its EEE setting is incompatible.</li> <li>• Operational—The port EEE is enabled and operating.</li> </ul> <p>If the interface speed is configured as 10 Mbps, EEE is disabled internally. When the interface speed moves back to auto, 100 Mbps or 1000 Mbps, EEE becomes active again.</p>
Rx/Tx LPI Status	<p>The Low Power Idle (LPI) status for the link partner. These fields can have any of the following values:</p> <ul style="list-style-type: none"> <li>• N/A—The port is not capable of EEE.</li> <li>• Interrupted—The link partner is in the process of moving to low power mode.</li> <li>• Low Power—The link partner is in low power mode.</li> <li>• None— EEE is disabled or not capable at the link partner side.</li> <li>• Received—The link partner is in low power mode and there is traffic activity.</li> </ul> <p>If an interface is configured as half-duplex, the LPI status is None, which means the interface cannot be in low power mode until it is configured as full-duplex.</p>
Wake Error Count	<p>The number of PHY wake-up faults that have occurred. A wake-up fault can occur when EEE is enabled and the connection to the link partner is broken.</p> <p>This information is useful for PHY debugging.</p>

# show env

To display fan, temperature, and power information, use the **show env** command in EXEC mode.

```
show env {all|fan|power [all|switch [stack-member-number]]|stack [stack-member-number] | temperature [status]}
```

## Syntax Description

<b>all</b>	Displays the fan and temperature environmental status and the status of the internal power supplies.
<b>fan</b>	Displays the switch fan status.
<b>power</b>	Displays the internal power status of the active switch.
<b>all</b>	(Optional) Displays the status of all the internal power supplies in a standalone switch when the command is entered on the switch, or in all the stack members when the command is entered on the active switch.
<b>switch</b>	(Optional) Displays the status of the internal power supplies for each switch in the stack or for the specified switch.  This keyword is available only on stacking-capable switches.
<i>stack-member-number</i>	(Optional) Number of the stack member for which to display the status of the internal power supplies or the environmental status.  The range is 1 to 9.
<b>stack</b>	Displays all environmental status for each switch in the stack or for the specified switch.  This keyword is available only on stacking-capable switches.
<b>temperature</b>	Displays the switch temperature status.
<b>status</b>	(Optional) Displays the switch internal temperature (not the external temperature) and the threshold values.

## Command Default

None

## Command Modes

User EXEC  
Privileged EXEC

**Command History**

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

**Usage Guidelines**

Use the **show env EXEC** command to display the information for the switch being accessed—a standalone switch or the active switch. Use this command with the **stack** and **switch** keywords to display all information for the stack or for the specified stack member.

If you enter the **show env temperature status** command, the command output shows the switch temperature state and the threshold level.

You can also use the **show env temperature** command to display the switch temperature status. The command output shows the green and yellow states as *OK* and the red state as *FAULTY*. If you enter the **show env all** command, the command output is the same as the **show env temperature status** command output.

**Examples**

This is an example of output from the **show env all** command:

```
Switch>show env all
Switch 1 FAN 1 is OK
Switch 1 FAN 2 is OK
Switch 1 FAN 3 is OK
FAN PS-1 is NOT PRESENT
FAN PS-2 is OK
Switch 1: SYSTEM TEMPERATURE is OK
SW  PID              Serial#      Status      Sys Pwr  PoE Pwr  Watts
--  -
1A  Not Present
1B  PWR-C1-715WAC      LIT150119Z1 OK          Good     Good     715
```

This is an example of output from the **show env fan** command:

```
Switch>show env fan
Switch 1 FAN 1 is OK
Switch 1 FAN 2 is OK
Switch 1 FAN 3 is OK
FAN PS-1 is NOT PRESENT
FAN PS-2 is OK
```

This is an example of output from the **show env power** command:

```
Switch>show env power
SW  PID              Serial#      Status      Sys Pwr  PoE Pwr  Watts
--  -
1A  Not Present
1B  PWR-C1-715WAC      LIT150119Z1 OK          Good     Good     715
```

This is an example of output from the **show env power all** command on the active switch:

```
Switch# show env power all
SW  PID              Serial#      Status      Sys Pwr  PoE Pwr  Watts
--  -
1A  Not Present
1B  PWR-C1-715WAC      LIT150119Z1 OK          Good     Good     715
```

This is an example of output from the **show env stack** command on the active switch:

```
Switch> show env stack
SWITCH: 1
Switch 1 FAN 1 is OK
Switch 1 FAN 2 is OK
Switch 1 FAN 3 is OK
FAN PS-1 is NOT PRESENT
FAN PS-2 is OK
Switch 1: SYSTEM TEMPERATURE is OK
Temperature Value: 28 Degree Celsius
Temperature State: GREEN
Yellow Threshold : 41 Degree Celsius
Red Threshold    : 56 Degree Celsius
```

This example shows how to display the temperature value, state, and the threshold values on a standalone switch. The table describes the temperature states in the command output.

```
Switch> show env temperature status
Temperature Value: 33 Degree Celsius
Temperature State: GREEN
Yellow Threshold : 65 Degree Celsius
Red Threshold    : 75 Degree Celsius
```

**Table 6: States in the show env temperature status Command Output**

State	Description
Green	The switch temperature is in the <i>normal</i> operating range.
Yellow	The temperature is in the <i>warning</i> range. You should check the external temperature around the switch.
Red	The temperature is in the <i>critical</i> range. The switch might not run properly if the temperature is in this range.

# show errdisable detect

To display error-disabled detection status, use the **show errdisable detect** command in EXEC mode.

## show errdisable detect

**Syntax Description** This command has no arguments or keywords.

**Command Default** None

**Command Modes** User EXEC  
Privileged EXEC

Command History	Release	Modification
	Cisco IOS XE 3.2SE	This command was introduced.

## Usage Guidelines

A gbic-invalid error reason refers to an invalid small form-factor pluggable (SFP) module.

The error-disable reasons in the command output are listed in alphabetical order. The mode column shows how error-disable is configured for each feature.

You can configure error-disabled detection in these modes:

- port mode—The entire physical port is error-disabled if a violation occurs.
- vlan mode—The VLAN is error-disabled if a violation occurs.
- port/vlan mode—The entire physical port is error-disabled on some ports and is per-VLAN error-disabled on other ports.

## Examples

This is an example of output from the **show errdisable detect** command:

```
Switch> show errdisable detect
ErrDisable Reason    Detection    Mode
-----
arp-inspection       Enabled     port
bpduguard            Enabled     vlan
channel-misconfig    Enabled     port
community-limit      Enabled     port
dhcp-rate-limit      Enabled     port
dtp-flap             Enabled     port
gbic-invalid         Enabled     port
inline-power         Enabled     port
invalid-policy       Enabled     port
l2ptguard            Enabled     port
link-flap            Enabled     port
loopback             Enabled     port
```

lsgroup	Enabled	port
pagp-flap	Enabled	port
psecure-violation	Enabled	port/vlan
security-violatio	Enabled	port
sfp-config-mismat	Enabled	port
storm-control	Enabled	port
udld	Enabled	port
vmps	Enabled	port

**Related Commands**

Command	Description
<a href="#">errdisable detect cause</a>	Enables error-disabled detection for a specific cause or all causes.
<a href="#">show errdisable recovery</a>	Displays the error-disabled recovery timer information.

# show errdisable recovery

To display the error-disabled recovery timer information, use the **show errdisable recovery** command in EXEC mode.

**show errdisable recovery**

**Syntax Description** This command has no arguments or keywords.

**Command Default** None

**Command Modes** User EXEC  
Privileged EXEC

Command History	Release	Modification
	Cisco IOS XE 3.2SE	This command was introduced.

**Usage Guidelines** A gbic-invalid error-disable reason refers to an invalid small form-factor pluggable (SFP) module interface.



**Note** Though visible in the output, the unicast-flood field is not valid.

**Examples** This is an example of output from the **show errdisable recovery** command:

```
Switch> show errdisable recovery
ErrDisable Reason      Timer Status
-----
udld                   Disabled
bpduguard              Disabled
security-violatio     Disabled
channel-misconfig     Disabled
vmps                   Disabled
pagp-flap              Disabled
dtp-flap               Disabled
link-flap              Enabled
l2ptguard              Disabled
psecure-violation     Disabled
gbic-invalid           Disabled
dhcp-rate-limit       Disabled
unicast-flood         Disabled
storm-control         Disabled
arp-inspection        Disabled
loopback               Disabled
Timer interval:300 seconds
Interfaces that will be enabled at the next timeout:
Interface  Errdisable reason  Time left(sec)
```

```
-----  
Gi1/0/2      link-flap      279
```

**Related Commands**

Command	Description
<a href="#">errdisable recovery cause</a>	Enables the error-disabled mechanism to recover from a specific cause.
<a href="#">errdisable recovery interval</a>	Specifies the time to recover from an error-disabled state.
<a href="#">show errdisable detect</a>	Displays error-disabled detection status.

## show interfaces

To display the administrative and operational status of all interfaces or for a specified interface, use the **show interfaces** command in privileged EXEC mode.

**show interfaces** [*interface-id*] **vlan** *vlan-id*] [**accounting**] **capabilities** [*module number*] **debounce** **description** **etherchannel** **flowcontrol** **pruning** **stats** **status** [**err-disabled**] **inactive**] **trunk**]

### Syntax Description

<i>interface-id</i>	(Optional) ID of the interface. Valid interfaces include physical ports (including type, stack member for stacking-capable switches, module, and port number) and port channels. The port channel range is 1 to 48.
<b>vlan</b> <i>vlan-id</i>	(Optional) VLAN identification. The range is 1 to 4094.
<b>accounting</b>	(Optional) Displays accounting information on the interface, including active protocols and input and output packets and octets. <b>Note</b> The display shows only packets processed in software; hardware-switched packets do not appear.
<b>capabilities</b>	(Optional) Displays the capabilities of all interfaces or the specified interface, including the features and options that you can configure on the interface. Though visible in the command line help, this option is not available for VLAN IDs.
<b>module number</b>	(Optional) Displays capabilities of all interfaces on the switch or specified stack member. The range is 1 to 9. This option is not available if you entered a specific interface ID.
<b>debounce</b>	(Optional) Displays port debounce timer information for an interface.
<b>description</b>	(Optional) Displays the administrative status and description set for an interface.
<b>etherchannel</b>	(Optional) Displays interface EtherChannel information.
<b>flowcontrol</b>	(Optional) Displays interface flow control information.
<b>mtu</b>	(Optional) Displays the MTU for each interface or for the specified interface.
<b>pruning</b>	(Optional) Displays trunk VTP pruning information for the interface.
<b>stats</b>	(Optional) Displays the input and output packets by switching the path for the interface.

<b>status</b>	(Optional) Displays the status of the interface. A status of unsupported in the Type field means that a non-Cisco small form-factor pluggable (SFP) module is inserted in the module slot.
<b>err-disabled</b>	(Optional) Displays interfaces in an error-disabled state.
<b>inactive</b>	(Optional) Displays interfaces in an inactive state.
<b>trunk</b>	(Optional) Displays interface trunk information. If you do not specify an interface, only information for active trunking ports appears.

**Note**

Though visible in the command-line help strings, the **crb**, **fair-queue**, **irb**, **mac-accounting**, **precedence**, **random-detect**, and **rate-limit** keywords are not supported.

**Command Default**

None

**Command Modes**

Privileged EXEC

**Command History**

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

**Usage Guidelines**

The **show interfaces capabilities** command with different keywords has these results:

- Use the **show interface capabilities module number** command to display the capabilities of all interfaces on that switch in the stack. If there is no switch with that module number in the stack, there is no output.
- Use the **show interfaces interface-id capabilities** to display the capabilities of the specified interface.
- Use the **show interfaces capabilities** (with no module number or interface ID) to display the capabilities of all interfaces in the stack.

**Examples**

This is an example of output from the **show interfaces** command for an interface on stack member 3:

```
Switch# show interfaces gigabitethernet3/0/2
GigabitEthernet3/0/2 is down, line protocol is down (notconnect)
  Hardware is Gigabit Ethernet, address is 2037.064d.4381 (bia 2037.064d.4381)
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Auto-duplex, Auto-speed, media type is 10/100/1000BaseTX
  input flow-control is off, output flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
```

```

Last input never, output never, output hang never
Last clearing of "show interface" counters never
Input queue: 0/2000/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
  0 packets input, 0 bytes, 0 no buffer
  Received 0 broadcasts (0 multicasts)
  0 runts, 0 giants, 0 throttles
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
  0 watchdog, 0 multicast, 0 pause input
  0 input packets with dribble condition detected
  0 packets output, 0 bytes, 0 underruns
  0 output errors, 0 collisions, 1 interface resets
  0 unknown protocol drops
  0 babbles, 0 late collision, 0 deferred
  0 lost carrier, 0 no carrier, 0 pause output
  0 output buffer failures, 0 output buffers swapped out

```

This is an example of output from the **show interfaces accounting** command:

This is an example of output from the **show interfaces capabilities** command for an interface:

```

Switch# show interfaces gigabitethernet1/0/2 capabilities
GigabitEthernet1/0/2
  Model:                UA-3850-24-CR
  Type:                 10/100/1000BaseTX
  Speed:                10,100,1000,auto
  Duplex:                full,half,auto
  Trunk encap. type:    802.1Q
  Trunk mode:           on,off,desirable,nonegotiate
  Channel:              yes
  Fast Start:           yes
  QoS scheduling:       rx-(not configurable on per port basis),
                       tx-(4q3t) (3t: Two configurable values and one fixed.)
  CoS rewrite:          yes
  ToS rewrite:          yes
  UDLD:                 yes
  Inline power:         no
  SPAN:                 source/destination
  PortSecure:           yes
  Dot1x:                yes

```

This is an example of output from the **show interfaces interface description** command when the interface has been described as *Connects to Marketing* by using the **description** interface configuration command:

```

Switch# show interfaces gigabitethernet1/0/2 description
Interface      Status      Protocol Description
Gi1/0/2        up          down      Connects to Marketing

```

This is an example of output from the **show interfaces etherchannel** command when port channels are configured on the switch:

```

Switch# show interfaces etherchannel
----
Port-channel34:
Age of the Port-channel   = 28d:18h:51m:46s
Logical slot/port         = 12/34           Number of ports = 0
GC                         = 0x00000000         HotStandBy port = null
Passive port list         =
Port state                 = Port-channel L3-Ag Ag-Not-Inuse
Protocol                   = -
Port security              = Disabled

```

This is an example of output from the **show interfaces interface-id pruning** command when pruning is enabled in the VTP domain:

```

Switch# show interfaces gigabitethernet1/0/2 pruning
Port      Vlans pruned for lack of request by neighbor
Gi1/0/2   3,4

```

```
Port      Vlans traffic requested of neighbor
Gi1/0/2   1-3
```

This is an example of output from the **show interfaces stats** command for a specified VLAN interface:

```
Switch# show interfaces vlan 1 stats
Switching path   Pkts In   Chars In   Pkts Out   Chars Out
Processor        1165354   136205310  570800     91731594
Route cache      0         0          0          0
Total            1165354   136205310  570800     91731594
```

This is an example of partial output from the **show interfaces status** command. It displays the status of all interfaces:

This is an example of output from the **show interfaces interface-id status** command:

```
Switch# show interfaces gigabitethernet1/0/20 status
Port      Name      Status      Vlan      Duplex  Speed      Type
Gi1/0/20          notconnect  1          auto     auto    10/100/1000Ba
seTX
```

This is an example of output from the **show interfaces status err-disabled** command. It displays the status of interfaces in the error-disabled state:

```
Switch# show interfaces status err-disabled
Port      Name      Status      Reason
Gi1/0/2          err-disabled  gbic-invalid
Gi2/0/3          err-disabled  dtp-flap
```

This is an example of output from the **show interfaces interface-id pruning** command:

```
Switch# show interfaces gigabitethernet1/0/2 pruning
Port Vlans pruned for lack of request by neighbor
```

This is an example of output from the **show interfaces interface-id trunk** command. It displays trunking information for the port.

```
Switch# show interfaces gigabitethernet1/0/1 trunk
Port      Mode      Encapsulation  Status      Native vlan
Gi1/0/1   on        802.1q         other       10

Port      Vlans allowed on trunk
Gi1/0/1   none

Port      Vlans allowed and active in management domain
Gi1/0/1   none

Port      Vlans in spanning tree forwarding state and not pruned
Gi1/0/1   none
```

## Related Commands

Command	Description
<a href="#">show interfaces counters</a>	Displays various counters for the switch or for a specific interface.
<a href="#">show interfaces switchport</a>	Displays the administrative and operational status of a switching (nonrouting) port.
<a href="#">show interfaces transceiver</a>	Displays the physical properties of a small form-factor pluggable (SFP) module interface.

# show interfaces counters

To display various counters for the switch or for a specific interface, use the **show interfaces counters** command in privileged EXEC mode.

**show interfaces** [*interface-id*] **counters** [**errors**] **etherchannel** | **module** *stack-member-number* | **protocol status** | **trunk**]

## Syntax Description

<i>interface-id</i>	(Optional) ID of the physical interface, including type, stack member (stacking-capable switches only) module, and port number.
<b>errors</b>	(Optional) Displays error counters.
<b>etherchannel</b>	(Optional) Displays EtherChannel counters, including octets, broadcast packets, multicast packets, and unicast packets received and sent.
<b>module</b> <i>stack-member-number</i>	(Optional) Displays counters for the specified stack member. The range is 1 to 9. <b>Note</b> In this command, the <b>module</b> keyword refers to the stack member number. The module number that is part of the interface ID is always zero.
<b>protocol status</b>	(Optional) Displays the status of protocols enabled on interfaces.
<b>trunk</b>	(Optional) Displays trunk counters.



### Note

Though visible in the command-line help string, the **vlan** *vlan-id* keyword is not supported.

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

## Usage Guidelines

If you do not enter any keywords, all counters for all interfaces are included.

**Examples**

This is an example of partial output from the **show interfaces counters** command. It displays all counters for the switch.

```
Switch# show interfaces counters
Port          InOctets      InUcastPkts    InMcastPkts    InBcastPkts
Gi1/0/1              0                0                0                0
Gi1/0/2              0                0                0                0
Gi1/0/3          95285341         43115           1178430         1950
Gi1/0/4              0                0                0                0
```

<output truncated>

This is an example of partial output from the **show interfaces counters module** command for stack member 2. It displays all counters for the specified switch in the stack.

```
Switch# show interfaces counters module 2
Port          InOctets      InUcastPkts    InMcastPkts    InBcastPkts
Gi1/0/1              520                2                0                0
Gi1/0/2              520                2                0                0
Gi1/0/3              520                2                0                0
Gi1/0/4              520                2                0                0
```

<output truncated>

This is an example of partial output from the **show interfaces counters protocol status** command for all interfaces:

```
Switch# show interfaces counters protocol status
Protocols allocated:
Vlan1: Other, IP
Vlan20: Other, IP, ARP
Vlan30: Other, IP, ARP
Vlan40: Other, IP, ARP
Vlan50: Other, IP, ARP
Vlan60: Other, IP, ARP
Vlan70: Other, IP, ARP
Vlan80: Other, IP, ARP
Vlan90: Other, IP, ARP
Vlan900: Other, IP, ARP
Vlan3000: Other, IP
Vlan3500: Other, IP
GigabitEthernet1/0/1: Other, IP, ARP, CDP
GigabitEthernet1/0/2: Other, IP
GigabitEthernet1/0/3: Other, IP
GigabitEthernet1/0/4: Other, IP
GigabitEthernet1/0/5: Other, IP
GigabitEthernet1/0/6: Other, IP
GigabitEthernet1/0/7: Other, IP
GigabitEthernet1/0/8: Other, IP
GigabitEthernet1/0/9: Other, IP
GigabitEthernet1/0/10: Other, IP, CDP
```

<output truncated>

This is an example of output from the **show interfaces counters trunk** command. It displays trunk counters for all interfaces.

```
Switch# show interfaces counters trunk
Port          TrunkFramesTx  TrunkFramesRx  WrongEncap
Gi1/0/1              0                0                0
Gi1/0/2              0                0                0
Gi1/0/3            80678            0                0
Gi1/0/4            82320            0                0
Gi1/0/5              0                0                0
```

<output truncated>

**Related Commands**

Command	Description
<a href="#">show interfaces</a>	Displays the administrative and operational status of all interfaces or a specified interface.

# show interfaces switchport

To display the administrative and operational status of a switching (nonrouting) port, including port blocking and port protection settings, use the **show interfaces switchport** command in privileged EXEC mode.

**show interfaces** [*interface-id*] **switchport** [**backup** [**detail**]] **module** *number*

## Syntax Description

<i>interface-id</i>	(Optional) ID of the interface. Valid interfaces include physical ports (including type, stack member for stacking-capable switches, module, and port number) and port channels. The port channel range is 1 to 48.
<b>backup</b>	(Optional) Displays Flex Link backup interface configuration for the specified interface or all interfaces.
<b>detail</b>	(Optional) Displays detailed backup information for the specified interface or all interfaces on the switch or the stack.
<b>module</b> <i>number</i>	(Optional) Displays switchport configuration of all interfaces on the switch or specified stack member.  The range is 1 to 9.  This option is not available if you entered a specific interface ID.

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

## Usage Guidelines

Use the **show interface switchport module** *number* command to display the switch port characteristics of all interfaces on that switch in the stack. If there is no switch with that module number in the stack, there is no output.

## Examples

This is an example of output from the **show interfaces switchport** command for a port. The table that follows describes the fields in the display.

**Note**

Private VLANs are not supported in this release, so those fields are not applicable.

```
Switch# show interfaces gigabitethernet1/0/1 switchport
Name: Gi1/0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 10 (VLAN0010)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: 11-20
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL

Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
```

Field	Description
Name	Displays the port name.
Switchport	Displays the administrative and operational status of the port. In this display, the port is in switchport mode.
Administrative Mode Operational Mode	Displays the administrative and operational modes.
Administrative Trunking Encapsulation Operational Trunking Encapsulation Negotiation of Trunking	Displays the administrative and operational encapsulation method and whether trunking negotiation is enabled.
Access Mode VLAN	Displays the VLAN ID to which the port is configured.
Trunking Native Mode VLAN Trunking VLANs Enabled Trunking VLANs Active	Lists the VLAN ID of the trunk that is in native mode. Lists the allowed VLANs on the trunk. Lists the active VLANs on the trunk.
Pruning VLANs Enabled	Lists the VLANs that are pruning-eligible.

Field	Description
Protected	Displays whether or not protected port is enabled (True) or disabled (False) on the interface.
Unknown unicast blocked Unknown multicast blocked	Displays whether or not unknown multicast and unknown unicast traffic is blocked on the interface.
Voice VLAN	Displays the VLAN ID on which voice VLAN is enabled.
Appliance trust	Displays the class of service (CoS) setting of the data packets of the IP phone.

This is an example of output from the **show interfaces switchport backup** command:

```
Switch# show interfaces switchport backup
Switch Backup Interface Pairs:
Active Interface      Backup Interface      State
-----
Gi1/0/1              Gi1/0/2              Active Up/Backup Standby
Gi3/0/3              Gi4/0/5              Active Down/Backup Up
Po1                  Po2                  Active Standby/Backup Up
```

In this example of output from the **show interfaces switchport backup** command, VLANs 1 to 50, 60, and 100 to 120 are configured on the switch:

```
Switch(config)# interface gigabitethernet 2/0/6
Switch(config-if)# switchport backup interface gigabitethernet 2/0/8
prefer vlan 60,100-120
```

When both interfaces are up, Gi2/0/8 forwards traffic for VLANs 60, 100 to 120, and Gi2/0/6 will forward traffic for VLANs 1 to 50.

```
Switch# show interfaces switchport backup

Switch Backup Interface Pairs:
Active Interface      Backup Interface      State
-----
GigabitEthernet2/0/6  GigabitEthernet2/0/8  Active Up/Backup Up
Vlans on Interface Gi 2/0/6: 1-50
Vlans on Interface Gi 2/0/8: 60, 100-120
```

When a Flex Link interface goes down (LINK\_DOWN), VLANs preferred on this interface are moved to the peer interface of the Flex Link pair. In this example, if interface Gi2/0/6 goes down, Gi2/0/8 carries all VLANs of the Flex Link pair.

```
Switch# show interfaces switchport backup

Switch Backup Interface Pairs:
Active Interface      Backup Interface      State
-----
GigabitEthernet2/0/6  GigabitEthernet2/0/8  Active Down/Backup Up
Vlans on Interface Gi 2/0/6:
Vlans on Interface Gi 2/0/8: 1-50, 60, 100-120
```

When a Flex Link interface comes up, VLANs preferred on this interface are blocked on the peer interface and moved to the forwarding state on the interface that has just come up. In this example, if interface Gi2/0/6

comes up, then VLANs preferred on this interface are blocked on the peer interface Gi2/0/8 and forwarded on Gi2/0/6.

```
Switch# show interfaces switchport backup
```

```
Switch Backup Interface Pairs:
Active Interface      Backup Interface      State
-----
GigabitEthernet2/0/6  GigabitEthernet2/0/8  Active Up/Backup Up
Vlans on Interface Gi 2/0/6: 1-50
Vlans on Interface Gi 2/0/8: 60, 100-120
```

## Related Commands

Command	Description
<a href="#">show interfaces</a>	Displays the administrative and operational status of all interfaces or a specified interface.

# show interfaces transceiver

To display the physical properties of a small form-factor pluggable (SFP) module interface, use the **show interfaces transceiver** command in EXEC mode.

**show interfaces** [*interface-id*] **transceiver** [**detail**| **module** *number*] **properties**| **supported-list**| **threshold-table**]

## Syntax Description

<i>interface-id</i>	(Optional) ID of the physical interface, including type, stack member (stacking-capable switches only) module, and port number.
<b>detail</b>	(Optional) Displays calibration properties, including high and low numbers and any alarm information for any Digital Optical Monitoring (DoM)-capable transceiver if one is installed in the switch.
<b>module</b> <i>number</i>	(Optional) Limits display to interfaces on module on the switch. The range is 1 to 9. This option is not available if you entered a specific interface ID.
<b>properties</b>	(Optional) Displays speed, duplex, and inline power settings on an interface.
<b>supported-list</b>	(Optional) Lists all supported transceivers.
<b>threshold-table</b>	(Optional) Displays alarm and warning threshold table.

## Command Modes

User EXEC  
Privileged EXEC

## Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

## Examples

This is an example of output from the **show interfaces *interface-id* transceiver properties** command:

```
Switch# show interfaces gigabitethernet1/1/1 transceiver properties
Name : Gil/1/1
Administrative Speed: auto
Operational Speed: auto
Administrative Duplex: auto
Administrative Power Inline: enable
Operational Duplex: auto
Administrative Auto-MDIX: off
Operational Auto-MDIX: off
```

This is an example of output from the **show interfaces interface-id transceiver detail** command:

```
Switch# show interfaces gigabitethernet1/1/1 transceiver detail
ITU Channel not available (Wavelength not available),
Transceiver is internally calibrated.
mA:milliamperes, dBm:decibels (milliwatts), N/A:not applicable.
++:high alarm, +:high warning, -:low warning, -- :low alarm.
A2D readouts (if they differ), are reported in parentheses.
The threshold values are uncalibrated.
```

Port	Temperature (Celsius)	High Alarm Threshold (Celsius)	High Warn Threshold (Celsius)	Low Warn Threshold (Celsius)	Low Alarm Threshold (Celsius)
Gil/1/1	29.9	74.0	70.0	0.0	-4.0

  

Port	Voltage (Volts)	High Alarm Threshold (Volts)	High Warn Threshold (Volts)	Low Warn Threshold (Volts)	Low Alarm Threshold (Volts)
Gil/1/1	3.28	3.60	3.50	3.10	3.00

  

Port	Optical Transmit Power (dBm)	High Alarm Threshold (dBm)	High Warn Threshold (dBm)	Low Warn Threshold (dBm)	Low Alarm Threshold (dBm)
Gil/1/1	1.8	7.9	3.9	0.0	-4.0

  

Port	Optical Receive Power (dBm)	High Alarm Threshold (dBm)	High Warn Threshold (dBm)	Low Warn Threshold (dBm)	Low Alarm Threshold (dBm)
Gil/1/1	-23.5	-5.0	-9.0	-28.2	-32.2

This is an example of output from the **show interfaces transceiver threshold-table** command:

```
Switch# show interfaces transceiver threshold-table
```

	Optical Tx	Optical Rx	Temp	Laser Bias current	Voltage
DWDM GBIC					
Min1	-4.00	-32.00	-4	N/A	4.65
Min2	0.00	-28.00	0	N/A	4.75
Max2	4.00	-9.00	70	N/A	5.25
Max1	7.00	-5.00	74	N/A	5.40
DWDM SFP					
Min1	-4.00	-32.00	-4	N/A	3.00
Min2	0.00	-28.00	0	N/A	3.10
Max2	4.00	-9.00	70	N/A	3.50
Max1	8.00	-5.00	74	N/A	3.60
RX only WDM GBIC					
Min1	N/A	-32.00	-4	N/A	4.65
Min2	N/A	-28.30	0	N/A	4.75
Max2	N/A	-9.00	70	N/A	5.25
Max1	N/A	-5.00	74	N/A	5.40
DWDM XENPAK					
Min1	-5.00	-28.00	-4	N/A	N/A
Min2	-1.00	-24.00	0	N/A	N/A
Max2	3.00	-7.00	70	N/A	N/A
Max1	7.00	-3.00	74	N/A	N/A
DWDM X2					
Min1	-5.00	-28.00	-4	N/A	N/A
Min2	-1.00	-24.00	0	N/A	N/A
Max2	3.00	-7.00	70	N/A	N/A
Max1	7.00	-3.00	74	N/A	N/A
DWDM XFP					
Min1	-5.00	-28.00	-4	N/A	N/A
Min2	-1.00	-24.00	0	N/A	N/A
Max2	3.00	-7.00	70	N/A	N/A
Max1	7.00	-3.00	74	N/A	N/A
CWDM X2					

Min1	N/A	N/A	0	N/A	N/A
Min2	N/A	N/A	0	N/A	N/A
Max2	N/A	N/A	0	N/A	N/A
Max1	N/A	N/A	0	N/A	N/A

<output truncated>

### Related Commands

Command	Description
<a href="#">show interfaces</a>	Displays the administrative and operational status of all interfaces or a specified interface.

# show mgmt-infra trace messages ilpower

To display inline power messages within a trace buffer, use the **show mgmt-infra trace messages ilpower** command in privileged EXEC mode.

**show mgmt-infra trace messages ilpower** [*switch stack-member-number*]

## Syntax Description

<b>switch</b> <i>stack-member-number</i>	(Optional) Specifies the stack member number for which to display inline power messages within a trace buffer.
--	--

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

## Examples

This is an output example from the **show mgmt-infra trace messages ilpower** command:

```
Switch# show mgmt-infra trace messages ilpower
[10/23/12 14:05:10.984 UTC 1 3] Initialized inline power system configuration fo
r slot 1.
[10/23/12 14:05:10.984 UTC 2 3] Initialized inline power system configuration fo
r slot 2.
[10/23/12 14:05:10.984 UTC 3 3] Initialized inline power system configuration fo
r slot 3.
[10/23/12 14:05:10.984 UTC 4 3] Initialized inline power system configuration fo
r slot 4.
[10/23/12 14:05:10.984 UTC 5 3] Initialized inline power system configuration fo
r slot 5.
[10/23/12 14:05:10.984 UTC 6 3] Initialized inline power system configuration fo
r slot 6.
[10/23/12 14:05:10.984 UTC 7 3] Initialized inline power system configuration fo
r slot 7.
[10/23/12 14:05:10.984 UTC 8 3] Initialized inline power system configuration fo
r slot 8.
[10/23/12 14:05:10.984 UTC 9 3] Initialized inline power system configuration fo
r slot 9.
[10/23/12 14:05:10.984 UTC a 3] Inline power subsystem initialized.
[10/23/12 14:05:18.908 UTC b 264] Create new power pool for slot 1
[10/23/12 14:05:18.909 UTC c 264] Set total inline power to 450 for slot 1
[10/23/12 14:05:20.273 UTC d 3] PoE is not supported on .
[10/23/12 14:05:20.288 UTC e 3] PoE is not supported on .
[10/23/12 14:05:20.299 UTC f 3] PoE is not supported on .
[10/23/12 14:05:20.311 UTC 10 3] PoE is not supported on .
[10/23/12 14:05:20.373 UTC 11 98] Inline power process post for switch 1
[10/23/12 14:05:20.373 UTC 12 98] PoE post passed on switch 1
[10/23/12 14:05:20.379 UTC 13 3] Slot #1: PoE initialization for board id 16387
[10/23/12 14:05:20.379 UTC 14 3] Set total inline power to 450 for slot 1
[10/23/12 14:05:20.379 UTC 15 3] Gi1/0/1 port config Initialized
```

```
[10/23/12 14:05:20.379 UTC 16 3] Interface Gi1/0/1 initialization done.
[10/23/12 14:05:20.380 UTC 17 3] Gi1/0/24 port config Initialized
[10/23/12 14:05:20.380 UTC 18 3] Interface Gi1/0/24 initialization done.
[10/23/12 14:05:20.380 UTC 19 3] Slot #1: initialization done.
[10/23/12 14:05:50.440 UTC 1a 3] Slot #1: PoE initialization for board id 16387
[10/23/12 14:05:50.440 UTC 1b 3] Duplicate init event
```

**Related Commands**

Command	Description
<a href="#">show mgmt-infra trace messages ilpower-ha</a>	Displays inline power high availability messages within a trace buffer.
<a href="#">show mgmt-infra trace messages platform-mgr-poe</a>	Displays platform manager Power over Ethernet messages within a trace buffer.

# show mgmt-infra trace messages ilpower-ha

To display inline power high availability messages within a trace buffer, use the **show mgmt-infra trace messages ilpower-ha** command in privileged EXEC mode.

**show mgmt-infra trace messages ilpower-ha** [*switch stack-member-number*]

## Syntax Description

<b>switch</b> <i>stack-member-number</i>	(Optional) Specifies the stack member number for which to display inline power messages within a trace buffer.
--	--

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

## Examples

This is an output example from the **show mgmt-infra trace messages ilpower-ha** command:

```
Switch# show mgmt-infra trace messages ilpower-ha
[10/23/12 14:04:48.087 UTC 1 3] NG3K_ILPOWER_HA: Created NGWC ILP CF client successfully.
```

## Related Commands

Command	Description
<a href="#">show mgmt-infra trace messages ilpower</a>	Displays inline power messages within a trace buffer.
<a href="#">show mgmt-infra trace messages platform-mgr-poe</a>	Displays platform manager Power over Ethernet messages within a trace buffer.

# show mgmt-infra trace messages platform-mgr-poe

To display platform manager Power over Ethernet (PoE) messages within a trace buffer, use the **show mgmt-infra trace messages platform-mgr-poe** privileged EXEC command.

**show mgmt-infra trace messages platform-mgr-poe** [*switch stack-member-number*]

<b>Syntax Description</b>	<b>switch</b> <i>stack-member-number</i>	(Optional) Specifies the stack member number for which to display messages within a trace buffer.
<b>Command Default</b>	None	
<b>Command Modes</b>	Privileged EXEC	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Cisco IOS XE 3.2SE	This command was introduced.

## Examples

This is an example of partial output from the **show mgmt-infra trace messages platform-mgr-poe** command:

```
Switch# show mgmt-infra trace messages platform-mgr-poe
[10/23/12 14:04:06.431 UTC 1 5495] PoE Info: get power controller param sent:
[10/23/12 14:04:06.431 UTC 2 5495] PoE Info: POE_SHUT sent for port 1 (0:0)
[10/23/12 14:04:06.431 UTC 3 5495] PoE Info: POE_SHUT sent for port 2 (0:1)
[10/23/12 14:04:06.431 UTC 4 5495] PoE Info: POE_SHUT sent for port 3 (0:2)
[10/23/12 14:04:06.431 UTC 5 5495] PoE Info: POE_SHUT sent for port 4 (0:3)
[10/23/12 14:04:06.431 UTC 6 5495] PoE Info: POE_SHUT sent for port 5 (0:4)
[10/23/12 14:04:06.431 UTC 7 5495] PoE Info: POE_SHUT sent for port 6 (0:5)
[10/23/12 14:04:06.431 UTC 8 5495] PoE Info: POE_SHUT sent for port 7 (0:6)
[10/23/12 14:04:06.431 UTC 9 5495] PoE Info: POE_SHUT sent for port 8 (0:7)
[10/23/12 14:04:06.431 UTC a 5495] PoE Info: POE_SHUT sent for port 9 (0:8)
[10/23/12 14:04:06.431 UTC b 5495] PoE Info: POE_SHUT sent for port 10 (0:9)
[10/23/12 14:04:06.431 UTC c 5495] PoE Info: POE_SHUT sent for port 11 (0:10)
[10/23/12 14:04:06.431 UTC d 5495] PoE Info: POE_SHUT sent for port 12 (0:11)
[10/23/12 14:04:06.431 UTC e 5495] PoE Info: POE_SHUT sent for port 13 (e:0)
[10/23/12 14:04:06.431 UTC f 5495] PoE Info: POE_SHUT sent for port 14 (e:1)
[10/23/12 14:04:06.431 UTC 10 5495] PoE Info: POE_SHUT sent for port 15 (e:2)
[10/23/12 14:04:06.431 UTC 11 5495] PoE Info: POE_SHUT sent for port 16 (e:3)
[10/23/12 14:04:06.431 UTC 12 5495] PoE Info: POE_SHUT sent for port 17 (e:4)
[10/23/12 14:04:06.431 UTC 13 5495] PoE Info: POE_SHUT sent for port 18 (e:5)
[10/23/12 14:04:06.431 UTC 14 5495] PoE Info: POE_SHUT sent for port 19 (e:6)
[10/23/12 14:04:06.431 UTC 15 5495] PoE Info: POE_SHUT sent for port 20 (e:7)
[10/23/12 14:04:06.431 UTC 16 5495] PoE Info: POE_SHUT sent for port 21 (e:8)
[10/23/12 14:04:06.431 UTC 17 5495] PoE Info: POE_SHUT sent for port 22 (e:9)
[10/23/12 14:04:06.431 UTC 18 5495] PoE Info: POE_SHUT sent for port 23 (e:10)
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<a href="#">show mgmt-infra trace messages ilpower</a>	Displays inline power messages within a trace buffer.
<a href="#">show mgmt-infra trace messages ilpower-ha</a>	Displays inline power high availability messages within a trace buffer.

# show network-policy profile

To display the network-policy profiles, use the **show network policy profile** command in privileged EXEC mode.

**show network-policy profile** [*profile-number*]

## Syntax Description

<i>profile-number</i>	(Optional) Displays the network-policy profile number. If no profile is entered, all network-policy profiles appear.
-----------------------	--

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

## Examples

This is an example of output from the **show network-policy profile** command:

```
Switch# show network-policy profile
Network Policy Profile 60
  Interface:
    none
```

## Related Commands

Command	Description
<a href="#">network-policy</a>	Applies a network-policy profile to an interface.
<a href="#">network-policy profile (global configuration)</a>	Creates a network-policy profile and enters network-policy configuration mode.

# show platform CAPWAP summary

To display the tunnel identifier and the type all the CAPWAP tunnels established by the controller to the access points and other mobility controllers, use the **show platform CAPWAP summary** command.

**show platform CAPWAP summary**

## Syntax Description

This command has no arguments or keywords.

## Command Default

## Command Modes

Global configuration

## Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

## Examples

This example displays the tunnel identifier and details:

```
Switch# show platform capwap summary
Tunnel ID | Type | Src IP | Dst IP | SPrt | DPrt | S | A
-----
0x0088498000000983 data 9.6.44.61 9.12.138.101 5247 41894 1 1
0x00966dc000000010 data 9.6.44.61 9.6.47.101 5247 62526 1 2
0x00938e800000095b data 9.6.44.61 9.12.138.100 5247 45697 1 1
0x00ab1a8000000bd1 data 9.6.44.61 9.12.139.101 5247 38906 1 0
0x00896e40000000bd data 9.6.44.61 9.12.136.100 5247 1836 1 1
```

# show power inline

To display the Power over Ethernet (PoE) status for the specified PoE port, the specified stack member, or for all PoE ports in the switch stack, use the **show power inline** command in EXEC mode.

**show power inline** [**police** | **priority**] [*interface-id* | **module** *stack-member-number*] [**detail**]

## Syntax Description

<b>police</b>	(Optional) Displays the power policing information about real-time power consumption.
<b>priority</b>	(Optional) Displays the power inline port priority for each port.
<i>interface-id</i>	(Optional) ID of the physical interface.
<b>module</b> <i>stack-member-number</i>	(Optional) Limits the display to ports on the specified stack member.  The range is 1 to 9.  This keyword is supported only on stacking-capable switches.
<b>detail</b>	(Optional) Displays detailed output of the interface or module.

## Command Modes

User EXEC  
Privileged EXEC

## Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

## Examples

This is an example of output from the **show power inline** command. The table that follows describes the output fields.

```
Switch> show power inline
Module   Available      Used      Remaining
         (Watts)        (Watts)   (Watts)
-----
1         n/a            n/a       n/a
2         n/a            n/a       n/a
3         1440.0         15.4      1424.6
4         720.0          6.3       713.7
Interface Admin   Oper      Power   Device      Class Max
         (Watts)
-----
Gi3/0/1  auto   off       0.0     n/a         n/a   30.0
Gi3/0/2  auto   off       0.0     n/a         n/a   30.0
Gi3/0/3  auto   off       0.0     n/a         n/a   30.0
```

## show power inline

```

Gi3/0/4 auto off 0.0 n/a n/a 30.0
Gi3/0/5 auto off 0.0 n/a n/a 30.0
Gi3/0/6 auto off 0.0 n/a n/a 30.0
Gi3/0/7 auto off 0.0 n/a n/a 30.0
Gi3/0/8 auto off 0.0 n/a n/a 30.0
Gi3/0/9 auto off 0.0 n/a n/a 30.0
Gi3/0/10 auto off 0.0 n/a n/a 30.0
Gi3/0/11 auto off 0.0 n/a n/a 30.0
Gi3/0/12 auto off 0.0 n/a n/a 30.0
<output truncated>

```

This is an example of output from the **show power inline interface-id** command on a switch port:

```

Switch> show power inline gigabitethernet1/0/1
Interface Admin Oper Power Device Class Max
              (Watts)
-----
Gi1/0/1 auto off 0.0 n/a n/a 30.0

```

This is an example of output from the **show power inline module switch-number** command on stack member 3. The table that follows describes the output fields.

```

Switch> show power inline module 3
Module Available Used Remaining
        (Watts) (Watts) (Watts)
-----
3 865.0 864.0 1.0
Interface Admin Oper Power Device Class Max
              (Watts)
-----
Gi3/0/1 auto power-deny 4.0 n/a n/a 15.4
Gi3/0/2 auto off 0.0 n/a n/a 15.4
Gi3/0/3 auto off 0.0 n/a n/a 15.4
Gi3/0/4 auto off 0.0 n/a n/a 15.4
Gi3/0/5 auto off 0.0 n/a n/a 15.4
Gi3/0/6 auto off 0.0 n/a n/a 15.4
Gi3/0/7 auto off 0.0 n/a n/a 15.4
Gi3/0/8 auto off 0.0 n/a n/a 15.4
Gi3/0/9 auto off 0.0 n/a n/a 15.4
Gi3/0/10 auto off 0.0 n/a n/a 15.4
<output truncated>

```

**Table 7: show power inline Field Descriptions**

Field	Description
Available	The total amount of configured power <sup>3</sup> on the PoE switch in watts (W).
Used	The amount of configured power that is allocated to PoE ports in watts.
Remaining	The amount of configured power in watts that is not allocated to ports in the system. (Available – Used = Remaining)
Admin	Administration mode: auto, off, static.

Field	Description
Oper	Operating mode: <ul style="list-style-type: none"> <li>• on—The powered device is detected, and power is applied.</li> <li>• off—No PoE is applied.</li> <li>• faulty—Device detection or a powered device is in a faulty state.</li> <li>• power-deny—A powered device is detected, but no PoE is available, or the maximum wattage exceeds the detected powered-device maximum.</li> </ul>
Power	The maximum amount of power that is allocated to the powered device in watts. This value is the same as the value in the <i>Cutoff Power</i> field in the <b>show power inline police</b> command output.
Device	The device type detected: n/a, unknown, Cisco powered-device, IEEE powered-device, or the name from CDP.
Class	The IEEE classification: n/a or a value from 0 to 4.
Max	The maximum amount of power allocated to the powered device in watts.
AdminPowerMax	The maximum amount power allocated to the powered device in watts when the switch polices the real-time power consumption. This value is the same as the <i>Max</i> field value.
AdminConsumption	The power consumption of the powered device in watts when the switch polices the real-time power consumption. If policing is disabled, this value is the same as the <i>AdminPowerMax</i> field value.

<sup>3</sup> The configured power is the power that you manually specify or that the switch specifies by using CDP power negotiation or the IEEE classification, which is different than the real-time power that is monitored with the power sensing feature.

This is an example of output from the **show power inline police** command on a stacking-capable switch:

```
Switch> show power inline police
Module   Available   Used         Remaining
         (Watts)    (Watts)     (Watts)
-----
1         370.0      0.0         370.0
3         865.0      864.0      1.0
         Admin Oper   Admin   Oper   Cutoff Oper
Interface State State   Police  Police Power  Power
-----
```

```

Gi1/0/1  auto  off      none      n/a      n/a      0.0
Gi1/0/2  auto  off      log       n/a      5.4     0.0
Gi1/0/3  auto  off      errdisable n/a      5.4     0.0
Gi1/0/4  off   off      none      n/a      n/a     0.0
Gi1/0/5  off   off      log       n/a      5.4     0.0
Gi1/0/6  off   off      errdisable n/a      5.4     0.0
Gi1/0/7  auto  off      none      n/a      n/a     0.0
Gi1/0/8  auto  off      log       n/a      5.4     0.0
Gi1/0/9  auto  on       none      n/a      n/a     5.1
Gi1/0/10 auto  on       log       ok       5.4     4.2
Gi1/0/11 auto  on       log       log      5.4     5.9
Gi1/0/12 auto  on       errdisable ok       5.4     4.2
Gi1/0/13 auto  errdisable errdisable n/a      5.4     0.0
<output truncated>

```

In the previous example:

- The Gi1/0/1 port is shut down, and policing is not configured.
- The Gi1/0/2 port is shut down, but policing is enabled with a policing action to generate a syslog message.
- The Gi1/0/3 port is shut down, but policing is enabled with a policing action is to shut down the port.
- Device detection is disabled on the Gi1/0/4 port, power is not applied to the port, and policing is disabled.
- Device detection is disabled on the Gi1/0/5 port, and power is not applied to the port, but policing is enabled with a policing action to generate a syslog message.
- Device detection is disabled on the Gi1/0/6 port, and power is not applied to the port, but policing is enabled with a policing action to shut down the port.
- The Gi1/0/7 port is up, and policing is disabled, but the switch does not apply power to the connected device.
- The Gi1/0/8 port is up, and policing is enabled with a policing action to generate a syslog message, but the switch does not apply power to the powered device.
- The Gi1/0/9 port is up and connected to a powered device, and policing is disabled.
- The Gi1/0/10 port is up and connected to a powered device, and policing is enabled with a policing action to generate a syslog message. The policing action does not take effect because the real-time power consumption is less than the cutoff value.
- The Gi1/0/11 port is up and connected to a powered device, and policing is enabled with a policing action to generate a syslog message.
- The Gi1/0/12 port is up and connected to a powered device, and policing is enabled with a policing action to shut down the port. The policing action does not take effect because the real-time power consumption is less than the cutoff value.
- The Gi1/0/13 port is up and connected to a powered device, and policing is enabled with a policing action to shut down the port.

This is an example of output from the **show power inline police interface-id** command on a standalone switch. The table that follows describes the output fields.

```

Switch> show power inline police gigabitethernet1/0/1
Interface Admin Oper Admin Oper Cutoff Oper
          State State Police Police Power Power
-----
Gi1/0/1  auto  off      none      n/a      n/a      0.0

```

**Table 8: show power inline police Field Descriptions**

Field	Description
Available	The total amount of configured power <sup>4</sup> on the switch in watts (W).
Used	The amount of configured power allocated to PoE ports in watts.
Remaining	The amount of configured power in watts that is not allocated to ports in the system. (Available – Used = Remaining)
Admin State	Administration mode: auto, off, static.
Oper State	<p>Operating mode:</p> <ul style="list-style-type: none"> <li>• errdisable—Policing is enabled.</li> <li>• faulty—Device detection on a powered device is in a faulty state.</li> <li>• off—No PoE is applied.</li> <li>• on—The powered device is detected, and power is applied.</li> <li>• power-deny—A powered device is detected, but no PoE is available, or the real-time power consumption exceeds the maximum power allocation.</li> </ul> <p><b>Note</b> The operating mode is the current PoE state for the specified PoE port, the specified stack member, or for all PoE ports on the switch.</p>
Admin Police	<p>Status of the real-time power-consumption policing feature:</p> <ul style="list-style-type: none"> <li>• errdisable—Policing is enabled, and the switch shuts down the port when the real-time power consumption exceeds the maximum power allocation.</li> <li>• log—Policing is enabled, and the switch generates a syslog message when the real-time power consumption exceeds the maximum power allocation.</li> <li>• none—Policing is disabled.</li> </ul>

Field	Description
Oper Police	Policing status: <ul style="list-style-type: none"> <li>errdisable—The real-time power consumption exceeds the maximum power allocation, and the switch shuts down the PoE port.</li> <li>log—The real-time power consumption exceeds the maximum power allocation, and the switch generates a syslog message.</li> <li>n/a—Device detection is disabled, power is not applied to the PoE port, or no policing action is configured.</li> <li>ok—Real-time power consumption is less than the maximum power allocation.</li> </ul>
Cutoff Power	The maximum power allocated on the port. When the real-time power consumption is greater than this value, the switch takes the configured policing action.
Oper Power	The real-time power consumption of the powered device.

<sup>4</sup> The configured power is the power that you manually specify or that the switch specifies by using CDP power negotiation or the IEEE classification, which is different than the real-time power that is monitored with the power sensing feature.

#### Related Commands

Command	Description
<a href="#">logging event power-inline-status</a>	Enables the logging of PoE events.
<a href="#">power inline</a>	Configures the power management mode on PoE ports.

# show stack-power

To display information about StackPower stacks or switches in a power stack, use the **show stack-power** command in EXEC mode.

**show stack-power** [*power-stack-name*]

## Syntax Description

<i>power-stack-name</i>	(Optional) Name of the power stack for which to display power information. The name can be up to 31 characters.
-------------------------	---

## Command Modes

User EXEC  
Privileged EXEC

## Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

## Usage Guidelines

This command is available only on switch stacks running the IP Base or IP Services image.

If a switch is shut down because of load shedding, the output of the **show stack-power** command still includes the MAC address of the shutdown neighbor switch. The command output shows the stack power topology even if there is not enough power to power a switch.

## Examples

This is an example of output from the **show stack-power** command:

```
Switch# show stack-power
Power Stack      Stack   Stack   Total   Rsvd    Alloc   Unused   Num   Num
Name            Mode    Topolgy Pwr (W) Pwr (W) Pwr (W) Pwr (W) SW    PS
-----
Powerstack-1    SP-PS   Stndaln 715     509     190     16      1    1
```

## Related Commands

Command	Description
<a href="#">mode (power-stack configuration)</a>	Configures power stack mode for the power stack.
<a href="#">power-priority</a>	Configures Cisco StackPower power-priority values for a switch in a power stack and for its high-priority and low-priority PoE.
<a href="#">stack-power</a>	Configures StackPower parameters for the power stack or for a switch in the power stack.

# show system mtu

To display the global maximum transmission unit (MTU) or maximum packet size set for the switch, use the **show system mtu** command in privileged EXEC mode.

**show system mtu**

**Syntax Description** This command has no arguments or keywords.

**Command Default** None

**Command Modes** Privileged EXEC

Command History	Release	Modification
	Cisco IOS XE 3.2SE	This command was introduced.

**Usage Guidelines** For information about the MTU values and the stack configurations that affect the MTU values, see the **system mtu** command.

**Examples** This is an example of output from the **show system mtu** command:

```
Switch# show system mtu
Global Ethernet MTU is 1500 bytes.
```

Related Commands	Command	Description
	<a href="#">system mtu</a>	Sets the global maximum packet size or MTU size for switched packets on Gigabit Ethernet and 10-Gigabit Ethernet ports.

# show wireless interface summary

To display the wireless interface status and configuration, use the **show wireless interface summary** privileged EXEC command.

```
show wireless interface summary
```

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

## Usage Guidelines

### Examples

This example shows how to display the summary of wireless interfaces:

```
Switch# show wireless interface summary
```

# speed

To specify the speed of a 10/100 Mb/s or 10/100/1000 Mb/s port, use the **speed** command in interface configuration mode. To return to the default value, use the **no** form of this command.

```
speed {10| 100| 1000} auto [10| 100| 1000] nonegotiate}
```

```
no speed
```

## Syntax Description

<b>10</b>	Specifies that the port runs at 10 Mb/s.
<b>100</b>	Specifies that the port runs at 100 Mb/s.
<b>1000</b>	Specifies that the port runs at 1000 Mb/s. This option is valid and visible only on 10/100/1000 Mb/s ports.
<b>auto</b>	Automatically detects the speed the port should run at based on the port at the other end of the link. If you use the <b>10</b> , <b>100</b> , or <b>1000</b> keywords with the <b>auto</b> keyword, the port only autonegotiates at the specified speeds.
<b>nonegotiate</b>	Disables autonegotiation, and the port runs at 1000 Mb/s.

## Command Default

The default is **auto**.

## Command Modes

Interface configuration

## Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

## Usage Guidelines

You cannot configure speed on the 10-Gigabit Ethernet ports.

Except for the 1000BASE-T small form-factor pluggable (SFP) modules, you can configure the speed to not negotiate (**nonegotiate**) when an SFP module port is connected to a device that does not support autonegotiation.

If the speed is set to **auto**, the switch negotiates with the device at the other end of the link for the speed setting and then forces the speed setting to the negotiated value. The duplex setting remains as configured on each end of the link, which could result in a duplex setting mismatch.

If both ends of the line support autonegotiation, we highly recommend the default autonegotiation settings. If one interface supports autonegotiation and the other end does not, do use the **auto** setting on the supported side, but set the duplex and speed on the other side.

**Caution**

Changing the interface speed and duplex mode configuration might shut down and reenable the interface during the reconfiguration.

For guidelines on setting the switch speed and duplex parameters, see the “Configuring Interface Characteristics” chapter in the software configuration guide for this release.

You can verify your settings by entering the **show interfaces** privileged EXEC command.

**Examples**

This example shows how to set speed on a port to 100 Mb/s:

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# speed 100
```

This example shows how to set a port to autonegotiate at only 10 Mb/s:

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# speed auto 10
```

This example shows how to set a port to autonegotiate at only 10 or 100 Mb/s:

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# speed auto 10 100
```

**Related Commands**

Command	Description
<a href="#">duplex</a>	Specifies the duplex mode of operation for a port.
<a href="#">show interfaces</a>	Displays the administrative and operational status of all interfaces or a specified interface.

# stack-power

To configure StackPower parameters for the power stack or for a switch in the power stack, use the **stack power** command in global configuration mode. To return to the default setting, use the **no** form of the command,

**stack-power** {**stack** *power-stack-name*| **switch** *stack-member-number*}

**no stack-power** {**stack** *power-stack-name*| **switch** *stack-member-number*}

## Syntax Description

<b>stack</b> <i>power-stack-name</i>	Specifies the name of the power stack. The name can be up to 31 characters. Entering these keywords followed by a carriage return enters power stack configuration mode.
<b>switch</b> <i>stack-member-number</i>	Specifies the switch number in the stack (1 to 4) to enter switch stack-power configuration mode for the switch.

## Command Default

There is no default.

## Command Modes

Global configuration

## Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

## Usage Guidelines

When you enter the **stack-power stack** *power stack name* command, you enter power stack configuration mode, and these commands are available:

- **default**—Returns a command to its default setting.
- **exit**—Exits ARP access-list configuration mode.
- **mode**—Sets the power mode for the power stack. See the **mode** command.
- **no**—Negates a command or returns to default settings.

If you enter the **stack-power switch** *switch-number* command with a switch number that is not participating in StackPower, you receive an error message.

When you enter the **stack-power switch** *switch-number* command with the number of a switch participating in StackPower, you enter switch stack power configuration mode, and these commands are available:

- **default**—Returns a command to its default setting.
- **exit**—Exits switch stack power configuration mode.

- **no**—Negates a command or returns to default settings.
- **power-priority**—Sets the power priority for the switch and the switch ports. See the **power-priority** command.
- **stack-id name**—Enters the name of the power stack to which the switch belongs. If you do not enter the power stack-ID, the switch does not inherit the stack parameters. The name can be up to 31 characters.
- **standalone**—Forces the switch to operate in standalone power mode. This mode shuts down both stack power ports.

### Examples

This example removes switch 2, which is connected to the power stack, from the power pool and shutting down both power ports:

```
Switch(config)# stack-power switch 2
Switch(config-switch-stackpower)# standalone
Switch(config-switch-stackpower)# exit
```

### Related Commands

Command	Description
<a href="#">mode (power-stack configuration)</a>	Configures power stack mode for the power stack.
<a href="#">power-priority</a>	Configures Cisco StackPower power-priority values for a switch in a power stack and for its high-priority and low-priority PoE.
<a href="#">show stack-power</a>	Displays information about StackPower stacks or switches in a power stack.

## switchport backup interface

To configure Flex Links, use the **switchport backup interface** command in interface configuration mode on a Layer 2 interface on the switch stack or on a standalone switch. To remove the Flex Links configuration, use the **no** form of this command.

```
switchport backup interface interface-id [mmu primary vlan vlan-id| multicast fast-convergence|
preemption {delay seconds| mode {bandwidth| forced| off}}| prefer vlan vlan-id]
```

```
no switchport backup interface interface-id [mmu primary vlan| multicast fast-convergence| preemption
{delay| mode}]| prefer vlan]
```

### Syntax Description

<i>interface-id</i>	ID of the physical interface.
<b>mmu</b>	(Optional) Configures the MAC move update (MMU) for a backup interface pair.
<b>primary vlan</b> <i>vlan-id</i>	(Optional) VLAN ID of the primary VLAN. The range is 1 to 4094.
<b>multicast fast-convergence</b>	(Optional) Configures multicast fast convergence on the backup interface.
<b>preemption</b>	(Optional) Configures a preemption scheme for a backup interface pair.
<b>delay</b> <i>seconds</i>	Specifies a preemption delay. The range is 1 to 300 seconds. The default is 35 seconds.
<b>mode</b>	Specifies the preemption mode.
<b>bandwidth</b>	Specifies that a higher bandwidth interface is preferred.
<b>forced</b>	Specifies that an active interface is preferred.
<b>off</b>	Specifies that no preemption occurs from backup to active.
<b>prefer vlan</b> <i>vlan-id</i>	(Optional) Specifies that VLANs are carried on the backup interfaces of a Flex Link pair. VLAN ID range is 1 to 4094.

### Command Default

The default is to have no Flex Links defined. The preemption mode is off. No preemption occurs. Preemption delay is set to 35 seconds.

### Command Modes

Interface configuration

### Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

## Usage Guidelines

Flex Links are a pair of interfaces that provide backup to each other. With Flex Links configured, one link acts as the primary interface and forwards traffic, while the other interface is in standby mode, ready to begin forwarding traffic if the primary link shuts down. The interface being configured is referred to as the active link; the specified interface is identified as the backup link. The feature provides an alternative to the Spanning Tree Protocol (STP), allowing users to turn off STP and still retain basic link redundancy.

This command is available only for Layer 2 interfaces.

You can configure only one Flex Link backup link for any active link, and it must be a different interface from the active interface.

- An interface can belong to only one Flex Link pair. An interface can be a backup link for only one active link. An active link cannot belong to another Flex Link pair.
- A backup link does not have to be the same type (Fast Ethernet or Gigabit Ethernet, for instance) as the active link. However, you should configure both Flex Links with similar characteristics so that there are no loops or changes in behavior if the standby link begins to forward traffic.
- Neither of the links can be a port that belongs to an EtherChannel. However, you can configure two port channels (EtherChannel logical interfaces) as Flex Links, and you can configure a port channel and a physical interface as Flex Links, with either the port channel or the physical interface as the active link.
- If STP is configured on the switch, Flex Links do not participate in STP in all valid VLANs. If STP is not running, be sure that there are no loops in the configured topology.

## Examples

This example shows how to configure two interfaces as Flex Links:

```
Switch# configure terminal
Switch(conf)# interface gigabitethernet1/0/1
Switch(conf-if)# switchport backup interface gigabitethernet1/0/2
Switch(conf-if)# end
```

This example shows how to configure the Gigabit Ethernet interface to always preempt the backup:

```
Switch# configure terminal
Switch(conf)# interface gigabitethernet1/0/1
Switch(conf-if)# switchport backup interface gigabitethernet1/0/2 preemption forced
Switch(conf-if)# end
```

This example shows how to configure the Gigabit Ethernet interface preemption delay time:

```
Switch# configure terminal
Switch(conf)# interface gigabitethernet1/0/1
Switch(conf-if)# switchport backup interface gigabitethernet1/0/2 preemption delay 150
Switch(conf-if)# end
```

This example shows how to configure the Gigabit Ethernet interface as the MMU primary VLAN:

```
Switch# configure terminal
Switch(conf)# interface gigabitethernet1/0/1
Switch(conf-if)# switchport backup interface gigabitethernet1/0/2 mmu primary vlan 1021
Switch(conf-if)# end
```

You can verify your setting by entering the **show interfaces switchport backup** privileged EXEC command.

**Related Commands**

<b>Command</b>	<b>Description</b>
<a href="#">show interfaces switchport</a>	Displays the administrative and operational status of a switching (nonrouting) port.

# switchport block

To prevent unknown multicast or unicast packets from being forwarded, use the **switchport block** command in interface configuration mode. To allow forwarding unknown multicast or unicast packets, use the **no** form of this command.

**switchport block** {multicast| unicast}

**no switchport block** {multicast| unicast}

## Syntax Description

<b>multicast</b>	Specifies that unknown multicast traffic should be blocked.  <b>Note</b> Only pure Layer 2 multicast traffic is blocked. Multicast packets that contain IPv4 or IPv6 information in the header are not blocked.
<b>unicast</b>	Specifies that unknown unicast traffic should be blocked.

## Command Default

Unknown multicast and unicast traffic is not blocked.

## Command Modes

Interface configuration

## Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

## Usage Guidelines

By default, all traffic with unknown MAC addresses is sent to all ports. You can block unknown multicast or unicast traffic on protected or nonprotected ports. If unknown multicast or unicast traffic is not blocked on a protected port, there could be security issues.

With multicast traffic, the port blocking feature blocks only pure Layer 2 packets. Multicast packets that contain IPv4 or IPv6 information in the header are not blocked.

Blocking unknown multicast or unicast traffic is not automatically enabled on protected ports; you must explicitly configure it.

For more information about blocking packets, see the software configuration guide for this release.

## Examples

This example shows how to block unknown unicast traffic on an interface:

```
Switch(config-if)# switchport block unicast
```

You can verify your setting by entering the **show interfaces interface-id switchport** privileged EXEC command.

**Related Commands**

Command	Description
<a href="#">show interfaces switchport</a>	Displays the administrative and operational status of a switching (nonrouting) port.

## system mtu

To set the global maximum packet size or MTU size for switched packets on Gigabit Ethernet and 10-Gigabit Ethernet ports, use the **system mtu** command in global configuration mode. To restore the global MTU value to its default value use the **no** form of this command.

**system mtu** *bytes*

**no system mtu**

### Syntax Description

<i>bytes</i>	The global MTU size in bytes. The range is 1500 to 9198 bytes; the default is 1500 bytes.
--------------	---

### Command Default

The default MTU size for all ports is 1500 bytes.

### Command Modes

Global configuration

### Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

### Usage Guidelines

You can verify your setting by entering the **show system mtu** privileged EXEC command.

The switch does not support the MTU on a per-interface basis.

If you enter a value that is outside the allowed range for the specific type of interface, the value is not accepted.

### Examples

This example shows how to set the global system MTU size to 6000 bytes:

```
Switch(config)# system mtu 6000
Global Ethernet MTU is set to 6000 bytes.
Note: this is the Ethernet payload size, not the total
Ethernet frame size, which includes the Ethernet
header/trailer and possibly other tags, such as ISL or
802.1q tags.
```

### Related Commands

Command	Description
<a href="#">show system mtu</a>	Displays the global MTU or maximum packet size set for the switch.

## voice-signaling vlan (network-policy configuration)

To create a network-policy profile for the voice-signaling application type, use the **voice-signaling vlan** command in network-policy configuration mode. To delete the policy, use the **no** form of this command.

```
voice-signaling vlan {vlan-id [cos cos-value| dscp dscp-value]| dot1p [cos l2-priority| dscp dscp]| none| untagged}
```

### Syntax Description

<b>vlan-id</b>	(Optional) The VLAN for voice traffic. The range is 1 to 4094.
<b>cos</b> <i>cos-value</i>	(Optional) Specifies the Layer 2 priority class of service (CoS) for the configured VLAN. The range is 0 to 7; the default is 5.
<b>dscp</b> <i>dscp-value</i>	(Optional) Specifies the differentiated services code point (DSCP) value for the configured VLAN. The range is 0 to 63; the default is 46.
<b>dot1p</b>	(Optional) Configures the phone to use IEEE 802.1p priority tagging and to use VLAN 0 (the native VLAN).
<b>none</b>	(Optional) Does not instruct the Cisco IP phone about the voice VLAN. The phone uses the configuration from the phone key pad.
<b>untagged</b>	(Optional) Configures the phone to send untagged voice traffic. This is the default for the phone.

### Command Default

No network-policy profiles for the voice-signaling application type are defined.

The default CoS value is 5.

The default DSCP value is 46.

The default tagging mode is untagged.

### Command Modes

Network-policy profile configuration

### Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

### Usage Guidelines

Use the **network-policy profile** global configuration command to create a profile and to enter network-policy profile configuration mode.

The voice-signaling application type is for network topologies that require a different policy for voice signaling than for voice media. This application type should not be advertised if all of the same network policies apply as those advertised in the voice policy TLV.

When you are in network-policy profile configuration mode, you can create the profile for voice-signaling by specifying the values for VLAN, class of service (CoS), differentiated services code point (DSCP), and tagging mode.

These profile attributes are contained in the Link Layer Discovery Protocol for Media Endpoint Devices (LLDP-MED) network-policy time-length-value (TLV).

To return to privileged EXEC mode from the network-policy profile configuration mode, enter the **exit** command.

### Examples

This example shows how to configure voice-signaling for VLAN 200 with a priority 2 CoS:

```
Switch(config)# network-policy profile 1
Switch(config-network-policy)# voice-signaling vlan 200 cos 2
```

This example shows how to configure voice-signaling for VLAN 400 with a DSCP value of 45:

```
Switch(config)# network-policy profile 1
Switch(config-network-policy)# voice-signaling vlan 400 dscp 45
```

This example shows how to configure voice-signaling for the native VLAN with priority tagging:

```
Switch(config-network-policy)# voice-signaling vlan dot1p cos 4
```

### Related Commands

Command	Description
<a href="#">network-policy</a>	Applies a network-policy profile to an interface.
<a href="#">network-policy profile (global configuration)</a>	Creates a network-policy profile and enters network-policy configuration mode.
<a href="#">voice vlan (network-policy configuration)</a>	Creates a network-policy profile for the voice application type.

## voice vlan (network-policy configuration)

To create a network-policy profile for the voice application type, use the **voice vlan** command in network-policy configuration mode. To delete the policy, use the **no** form of this command.

```
voice vlan {vlan-id [cos cos-value] dscp dscp-value} dot1p [cos l2-priority] dscp dscp} none| untagged}
```

### Syntax Description

<i>vlan-id</i>	(Optional) The VLAN for voice traffic. The range is 1 to 4094.
<b>cos</b> <i>cos-value</i>	(Optional) Specifies the Layer 2 priority class of service (CoS) for the configured VLAN. The range is 0 to 7; the default is 5.
<b>dscp</b> <i>dscp-value</i>	(Optional) Specifies the differentiated services code point (DSCP) value for the configured VLAN. The range is 0 to 63; the default is 46.
<b>dot1p</b>	(Optional) Configures the phone to use IEEE 802.1p priority tagging and to use VLAN 0 (the native VLAN).
<b>none</b>	(Optional) Does not instruct the Cisco IP phone about the voice VLAN. The phone uses the configuration from the phone key pad.
<b>untagged</b>	(Optional) Configures the phone to send untagged voice traffic. This is the default for the phone.

### Command Default

No network-policy profiles for the voice application type are defined.

The default CoS value is 5.

The default DSCP value is 46.

The default tagging mode is untagged.

### Command Modes

Network-policy profile configuration

### Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

### Usage Guidelines

Use the **network-policy profile** global configuration command to create a profile and to enter network-policy profile configuration mode.

The voice application type is for dedicated IP telephones and similar devices that support interactive voice services. These devices are typically deployed on a separate VLAN for ease of deployment and enhanced security through isolation from data applications.

When you are in network-policy profile configuration mode, you can create the profile for voice by specifying the values for VLAN, class of service (CoS), differentiated services code point (DSCP), and tagging mode.

These profile attributes are contained in the Link Layer Discovery Protocol for Media Endpoint Devices (LLDP-MED) network-policy time-length-value (TLV).

To return to privileged EXEC mode from the network-policy profile configuration mode, enter the **exit** command.

### Examples

This example shows how to configure the voice application type for VLAN 100 with a priority 4 CoS:

```
Switch(config)# network-policy profile 1
Switch(config-network-policy)# voice vlan 100 cos 4
```

This example shows how to configure the voice application type for VLAN 100 with a DSCP value of 34:

```
Switch(config)# network-policy profile 1
Switch(config-network-policy)# voice vlan 100 dscp 34
```

This example shows how to configure the voice application type for the native VLAN with priority tagging:

```
Switch(config-network-policy)# voice vlan dot1p cos 4
```

### Related Commands

Command	Description
<a href="#">network-policy</a>	Applies a network-policy profile to an interface.
<a href="#">network-policy profile (global configuration)</a>	Creates a network-policy profile and enters network-policy configuration mode.
<a href="#">voice-signaling vlan (network-policy configuration)</a>	Creates a network-policy profile for the voice-signaling application type.

## wireless ap-manager interface

To configure the wireless AP-manager interface, use the **wireless ap-manager interface** command.

**wireless ap-managerinterface** {**TenGigabitEthernet** *interface-number*| **Vlan** *interface-number*}

### Syntax Description

<b>TenGigabitEthernet</b> <i>interface-name</i>	Configures 10-Gigabit Ethernet interface. Values range from 0 to 9.
<b>Vlan</b> <i>interface-name</i>	Configures VLANs. Values range from 1 to 4095.

### Command Default

None

### Command Modes

Global configuration

### Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

### Examples

This example shows how to configure the wireless AP-manager:

```
Switch# wireless ap-manager interface vlan
<1-4095> Vlan interface number
```

This example shows how to configure the wireless AP-manager:

```
Switch# #wireless ap-manager interface vlan 10
```

# wireless exclusionlist

To manage exclusion list entries, use the **wireless exclusionlist** global configuration command. To remove the exclusion list entries, use the **no** form of the command.

```
wireless exclusionlist mac-addr description description
no wireless exclusionlist mac-addr
```

## Syntax Description

<i>mac-addr</i>	The MAC address of the local excluded entry.
<b>description</b> <i>description</i>	Specifies the description for an exclusion-list entry.

## Command Default

None

## Command Modes

Global configuration

## Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

## Examples

This example shows how to create a local exclusion list entry for the MAC address xxx.xxx.xxx:

```
Switch# wireless exclusionlist xxx.xxx.xxx
```

This example shows how to create a description for the local exclusion list entry for the MAC address xxx.xxx.xxx:

```
Switch# wireless exclusionlist xxx.xxx.xxx description sample
```

# wireless linktest

To configure linktest frame size and number of frames to send, use the **wireless linktest** command.

**wireless linktest** {**frame-size** *size*|**number-of-frames** *value*}

## Syntax Description

<b>frame-size</b> <i>size</i>	Specifies the link test frame size for each packet. The values range from 1 to 1400.
<b>number-of-frames</b> <i>value</i>	Specifies the number of frames to be sent for the link test. The values range from 1 to 100.

## Command Default

None

## Command Modes

Global configuration

## Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

## Examples

This example shows how to configure the link test frame size of each frame as 10:

```
Switch# wireless linktest frame-size 10
```

# wireless management interface

To configure wireless management parameters on an interface, use the **wireless management interface** global configuration command. To remove a wireless management parameters on an interface, use the **no** form of the command.

**wireless management interface** *interface-name* {**TenGigabitEthernet** *interface-name*| **Vlan** *interface-name*}  
**no wireless management interface**

## Syntax Description

<i>interface-name</i>	The interface number.
<b>TenGigabitEthernet</b> <i>interface-name</i>	The 10-Gigabit Ethernet interface number. The values range from 0 to 9.
<b>Vlan</b> <i>interface-name</i>	The VLAN interface number. The values range from 1 to 4095.

## Command Default

None

## Command Modes

Global configuration

## Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

## Examples

This example shows how to configure VLAN 10 on the wireless interface:

```
Switch# wireless management interface Vlan 10
```

## wireless peer-blocking forward-upstream

To configure peer-to-peer blocking for forward upstream, use the **wireless peer-blocking forward-upstream** command. To remove a peer-to-peer blocking, use the **no** form of the command.

**wireless peer-blocking forward-upstream** *interface* {**GigabitEthernet** *interface-number* **TenGigabitEthernet** *interface-number*}

**no wireless peer-blocking forward-upstream** {**GigabitEthernet** *interface-number* **TenGigabitEthernet** *interface-number*}

### Syntax Description

<b>GigabitEthernet</b> <i>interface</i>	The Gigabit Ethernet interface number. Values range from 0 to 9.
<b>TenGigabitEthernet</b> <i>interface</i>	The 10-Gigabit Ethernet interface number. Values range from 0 to 9.

### Command Default

None

### Command Modes

Global configuration

### Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

### Examples

This example shows how to configure peer-to-peer blocking for interface 10-gigabit ethernet interface:

```
Switch(config)# wireless peer-blocking forward-upstream TenGigabitEthernet 1/1/4
```