



Interface and Hardware Commands

- [client vlan](#), on page 3
- [debug ilpower](#), on page 4
- [debug interface](#), on page 5
- [debug lldp packets](#), on page 6
- [debug nmsp](#), on page 7
- [debug platform poe](#), on page 8
- [duplex](#), on page 9
- [errdisable detect cause](#), on page 11
- [errdisable recovery cause](#), on page 13
- [errdisable recovery interval](#), on page 15
- [interface](#), on page 16
- [interface range](#), on page 18
- [ip mtu](#), on page 19
- [ipv6 mtu](#), on page 20
- [lldp \(interface configuration\)](#), on page 21
- [logging event power-inline-status](#), on page 22
- [mdix auto](#), on page 23
- [mode \(power-stack configuration\)](#), on page 24
- [monitoring](#), on page 26
- [network-policy](#), on page 28
- [network-policy profile \(global configuration\)](#), on page 29
- [nmsp attachment suppress](#), on page 30
- [power efficient-ethernet auto](#), on page 31
- [power-priority](#), on page 32
- [power inline](#), on page 34
- [power inline police](#), on page 37
- [power supply](#), on page 39
- [show CAPWAP summary](#), on page 41
- [show controllers cpu-interface](#), on page 42
- [show controllers ethernet-controller](#), on page 44
- [show controllers utilization](#), on page 53
- [show eee](#), on page 55
- [show env](#), on page 58

- [show errdisable detect](#), on page 61
- [show errdisable recovery](#), on page 62
- [show interfaces](#), on page 63
- [show interfaces counters](#), on page 67
- [show interfaces switchport](#), on page 69
- [show interfaces transceiver](#), on page 71
- [show memory platform](#), on page 74
- [show module](#), on page 77
- [show mgmt-infra trace messages ilpower](#), on page 78
- [show mgmt-infra trace messages ilpower-ha](#), on page 80
- [show mgmt-infra trace messages platform-mgr-poe](#), on page 81
- [show network-policy profile](#), on page 82
- [show platform CAPWAP summary](#), on page 83
- [show platform forward](#), on page 84
- [show platform hardware fed switch forward](#), on page 86
- [show platform resources](#), on page 88
- [show platform software ilpower](#), on page 89
- [show platform software process list](#), on page 91
- [show platform software process slot switch](#), on page 94
- [show platform software status control-processor](#), on page 96
- [show processes cpu platform monitor](#), on page 99
- [show processes memory platform](#), on page 101
- [show power inline](#), on page 104
- [show stack-power](#) , on page 109
- [show stack-power](#) , on page 111
- [show system mtu](#), on page 112
- [show tech-support](#) , on page 113
- [show wireless interface summary](#), on page 115
- [speed](#), on page 116
- [stack-power](#) , on page 118
- [switchport block](#), on page 120
- [system mtu](#), on page 121
- [test mcu read-register](#), on page 122
- [transceiver type all](#), on page 124
- [voice-signaling vlan \(network-policy configuration\)](#), on page 125
- [voice vlan \(network-policy configuration\)](#), on page 127
- [wireless ap-manager interface](#), on page 129
- [wireless exclusionlist](#), on page 130
- [wireless linktest](#), on page 131
- [wireless management interface](#), on page 132
- [wireless peer-blocking forward-upstream](#), on page 133

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

interface-id-name-or-group-name Interface ID, name, or VLAN group name. The interface ID can also be in digits too.

Command Default

The default interface is configured.

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS XE 3.3SE	Cisco IOS XE 3.3SE 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.

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

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

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

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

Related Topics

[wlan](#)

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

Syntax Description

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

Command Default

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

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 stack master. To enable debugging on a stack member, you can start a session from the stack master by using the **session** *switch-number* EXEC command. Then enter the **debug** command at the command-line prompt of the stack member. You also can use the **remote command** *stack-member-number* *LINE* EXEC command on the stack master switch to enable debugging on a member switch without first starting a session.

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} | null interface-number |
port-channel port-channel-number | states | vlan vlan-id}
no debug interface {interface-id | counters {exceptions | protocol memory} | null interface-number |
port-channel port-channel-number | states | vlan vlan-id}
```

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.
null <i>interface-number</i>	Displays debug messages for null interfaces. The interface number is always 0 .
port-channel <i>port-channel-number</i>	Displays debug messages for the specified EtherChannel port-channel interface. The <i>port-channel-number</i> range is 1 to 48.
vlan <i>vlan-id</i>	Displays debug messages for the specified VLAN. The vlan range is 1 to 4094.
counters	Displays counters debugging information.
exceptions	Displays debug messages when a recoverable exceptional condition occurs during the computation of the interface packet and data rate statistics.
protocol memory	Displays debug messages for memory operations of protocol counters.
states	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 3.3SE	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 stack master. To enable debugging on a stack member, you can start a session from the stack master by using the **session** *switch-number* EXEC command. Then enter the **debug** command at the command-line prompt of the stack member. You also can use the **remote command** *stack-member-number* *LINE* EXEC command on the stack master switch to enable debugging on a member switch without first starting a session.

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 3.3SE	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.

Syntax Description	all	Displays all NMSP debug messages.
	connection	Displays debug messages for NMSP connection events.
	error	Displays debugging information for NMSP error messages.
	event	Displays debug messages for NMSP events.
	rx	Displays debugging information for NMSP receive messages.
	tx	Displays debugging information for NMSP transmit messages.
	packet	Displays debug messages for NMSP packet events.

Command Default Debugging is disabled.

Command Modes Privileged EXEC

Command History	Release	Modification
	Cisco IOS XE 3.3SE	This command was introduced.

Usage Guidelines



Note Attachment information is not supported in Cisco IOS XE Denali 16.1.1 and later releases.

The **undebug 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 stack master. To enable debugging on a stack member, you can start a session from the stack master by using the **session switch-number** EXEC command. Then enter the **debug** command at the command-line prompt of the stack member. You also can use the **remote command stack-member-number LINE** EXEC command on the stack master switch to enable debugging on a member switch without first starting a session.

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

error	(Optional) Displays PoE-related error debug messages.
info	(Optional) Displays PoE-related information debug messages.
switch <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 3.3SE	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

auto Enables automatic duplex configuration. The port automatically detects whether it should run in full- or half-duplex mode, depending on the attached device mode.

full Enables full-duplex mode.

half 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 3.3SE	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 reenable 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:

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

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 | link-flap | loopback | pagp-flap | pppoe-ia-rate-limit | psp shutdown vlan | 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 | link-flap | loopback | pagp-flap | pppoe-ia-rate-limit | psp shutdown vlan | security-violation shutdown vlan | sfp-config-mismatch}
```

Syntax	Description
all	Enables error detection for all error-disabled causes.
arp-inspection	Enables error detection for dynamic Address Resolution Protocol (ARP) inspection.
bpduguard shutdown vlan	Enables per-VLAN error-disable for BPDU guard.
dhcp-rate-limit	Enables error detection for DHCP snooping.
dtp-flap	Enables error detection for the Dynamic Trunking Protocol (DTP) flapping.
gbic-invalid	Enables error detection for an invalid Gigabit Interface Converter (GBIC) module. Note This error refers to an invalid small form-factor pluggable (SFP) module.
inline-power	Enables error detection for the Power over Ethernet (PoE) error-disabled cause. Note This keyword is supported only on switches with PoE ports.
link-flap	Enables error detection for link-state flapping.
loopback	Enables error detection for detected loopbacks.
pagp-flap	Enables error detection for the Port Aggregation Protocol (PAgP) flap error-disabled cause.
pppoe-ia-rate-limit	Enables error detection for the PPPoE Intermediate Agent rate-limit error-disabled cause.
psp shutdown vlan	Enables error detection for protocol storm protection (PSP).
security-violation shutdown vlan	Enables voice aware 802.1x security.
sfp-config-mismatch	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	Modification
	Cisco IOS XE 3.3SE	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.

For protocol storm protection, excess packets are dropped for a maximum of two virtual ports. Virtual port error disabling using the **psp** keyword is not supported for EtherChannel and Flexlink interfaces.

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

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

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

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

```
Device(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:

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

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

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 | link-flap | loopback | mac-limit | pagp-flap | port-mode-failure |
pppoe-ia-rate-limit | psecure-violation | psp | security-violation | sfp-config-mismatch | storm-control |
udld}
```

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

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

port-mode-failure	Enables the timer to recover from the port mode change failure error-disabled state.
pppoe-ia-rate-limit	Enables the timer to recover from the PPPoE IA rate limit error-disabled state.
psecure-violation	Enables the timer to recover from a port security violation disable state.
psp	Enables the timer to recover from the protocol storm protection (PSP) error-disabled state.
security-violation	Enables the timer to recover from an IEEE 802.1x-violation disabled state.
sfp-config-mismatch	Enables error detection on an SFP configuration mismatch.
storm-control	Enables the timer to recover from a storm control error.
udld	Enables the timer to recover from the UniDirectional Link Detection (UDLD) error-disabled state.

Command Default Recovery is disabled for all causes.

Command Modes Global configuration

Command History

Release	Modification
Cisco IOS XE 3.3SE	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 BPDU guard error-disabled cause:

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

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	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE 3.3SE</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE 3.3SE	This command was introduced.
Release	Modification				
Cisco IOS XE 3.3SE	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:

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

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
Auto-Template <i>Auto-template interface-number</i>	Enables you to configure auto-template interface. Values range from 1 to 999.
Capwap <i>Capwap interface number</i>	Enables you to configure CAPWAP tunnel interface. Values range from 0 to 2147483647.
GigabitEthernet <i>Gigabit Ethernet interface number</i>	Enables you to configure Gigabit Ethernet IEEE 802.3z interface. Values range from 0 to 9.
Group VI <i>Group VI interface number</i>	Enables you to configure the internal interface. Values range from 0 to 9.
Internal Interface <i>Internal Interface</i>	Enables you to configure internal interface.
Loopback <i>Loopback Interface number</i>	Enables you to configure loopback interface. Values range from 0 to 2147483647.
Null <i>Null interface number</i>	Enables you to configure null interface. Value is 0.
Port-channel <i>interface number</i>	Enables you to configure Ethernet channel interfaces. Values range from 1 to 128.
TenGigabitEthernet <i>interface number</i>	Enables you to configure a 10-Gigabit Ethernet interface. Values range from 0 to 9.
Tunnel <i>interface number</i>	Enables you to configure the tunnel interface. Values range from 0 to 2147483647.
Vlan <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	Release	Modification
	Cisco IOS XE 3.3SE	This command was introduced.

Usage Guidelines

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

This example shows how you can configure interface:

```
Device# 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	Description
GigabitEthernet <i>interface-number</i>	Configures the Gigabit Ethernet IEEE 802.3z interface. Values range from 1 to 9.
Loopback <i>interface-number</i>	Configures the loopback interface. Values range from 0 to 2147483647.
Port-Channel <i>interface-number</i>	Configures 10-Gigabit Ethernet channel of interfaces. Values range from 1 to 128.
TenGigabit Ethernet <i>interface-number</i>	Configures 10-Gigabit Ethernet interfaces. Values range from 0 to 9.
Tunnel <i>interface-number</i>	Configures the tunnel interface. Values range from 0 to 2147483647.
VLAN <i>interface-number</i>	Configures the switch VLAN interfaces. Values range from 1 to 4095.
Macro <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 3.3SE	This command was introduced.

This example shows how you can configure interface range:

```
Device(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	<i>bytes</i> 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	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE 3.3SE</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE 3.3SE	This command was introduced.
Release	Modification				
Cisco IOS XE 3.3SE	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.

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

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

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

```
Device(config)# interface vlan 200
Device(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.

```
Device# 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>

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	<i>bytes</i> 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 3.3SE	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.

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

```
Device(config)# interface gigabitEthernet4/0/1
Device(config-if)# ipv6 mtu 2000
```

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

```
Device(config)# interface gigabitEthernet4/0/1
Device(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.

```
Device# 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>

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.

Syntax Description		
med-tlv-select		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"> • inventory-management— LLDP MED Inventory Management TLV. • location— LLDP MED Location TLV. • network-policy— LLDP MED Network Policy TLV.
receive		Enables the interface to receive LLDP transmissions.
tlv-select		Selects the LLDP TLVs to send.
power-management		Sends the LLDP Power Management TLV.
transmit		Enables LLDP transmission on the interface.

Command Default LLDP is disabled.

Command Modes Interface configuration

Command History	Release	Modification
	Cisco IOS XE 3.3SE	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.

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

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

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

```
Device(config)# interface gigabitethernet1/0/1
Device(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 3.3SE	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:

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

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 3.3SE	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.

Auto-MDIX is supported on all 10/100 and 10/100/1000 Mb/s interfaces and on 10/100/1000BASE-TX small form-factor pluggable (SFP) module interfaces. It is not supported on 1000BASE-SX or -LX SFP module interfaces.

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.

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

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

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		
power-shared		Sets the power stack to operate in power-shared mode. This is the default.
redundant		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.
strict		(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 3.3SE	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.

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.

```
Device(config)# stack-power stack power1  
Device(config-stackpower)# mode power-shared strict  
Device(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.

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

monitoring

To enable digital optical monitoring (DOM) and to specify the polling interval, enter the **monitoring** command in the transceiver type configuration mode. To disable monitoring, use the **no** form of the command.

```
monitoring
[{interval seconds}]
no monitoring
```

Syntax Description	interval seconds (Optional) Specifies the interval at which polling of monitoring parameter occurs. The valid range is 300 to 3600 seconds, and the default interval is 600 seconds.				
Command Default	DOM is disabled				
Command Modes	Transceiver type configuration mode (config-xcvr-type)				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Denali 16.3.6</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Denali 16.3.6	This command was introduced.
Release	Modification				
Cisco IOS XE Denali 16.3.6	This command was introduced.				

- Usage Guidelines**
- You can enable optical monitoring only for optical transceivers that support DOM. Use these resources to verify:
- See the following publication on cisco.com:
https://www.cisco.com/c/en/us/td/docs/interfaces_modules/transceiver_modules/compatibility/matrix/DOM_matrix.html
 - Display the list of DOM-supported transceivers on the switch, by entering the **show interfaces transceiver supported-list** command in privileged EXEC mode.

This example shows how to enable monitoring of optical transceivers, set the polling interval to 1500 seconds and display real-time values:

```
Device# configure terminal
Device(config)# transceiver type all
Device(config-xcvr-type)# monitoring interval 1500
Device(config-xcvr-type)# end
Device# show interfaces transceiver detail
```

mA: milliamperes, dBm: decibels (milliwatts), NA or 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 calibrated.

Port	Temperature (Celsius)	High Alarm Threshold (Celsius)	High Warn Threshold (Celsius)	Low Warn Threshold (Celsius)	Low Alarm Threshold (Celsius)
Gi5/1/2	43.0	110.0	93.0	-30.0	-40.0
Te5/1/3	32.0	90.0	85.0	-5.0	-10.0

Port	Voltage (Volts)	High Alarm Threshold (Volts)	High Warn Threshold (Volts)	Low Warn Threshold (Volts)	Low Alarm Threshold (Volts)

Gi5/1/2	3.28	3.90	3.70	2.90	2.70
Te5/1/3	3.28	3.63	3.47	3.14	2.97
Port	Current (milliamperes)	High Alarm Threshold (mA)	High Warn Threshold (mA)	Low Warn Threshold (mA)	Low Alarm Threshold (mA)
Gi5/1/2	22.1	80.0	70.0	4.0	2.0
Te5/1/3	19.8	105.0	95.0	4.0	2.0
Port	Optical Transmit Power (dBm)	High Alarm Threshold (dBm)	High Warn Threshold (dBm)	Low Warn Threshold (dBm)	Low Alarm Threshold (dBm)
Gi5/1/2	-5.4	0.9	-1.0	-11.5	-13.4
Te5/1/3	2.4	7.9	4.9	-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)
Gi5/1/2	-8.1	0.7	-1.0	-20.0	-24.0
Te5/1/3	-4.2	-0.0	-3.0	-23.0	-27.2

This example shows how to disable monitoring for all transceiver types:

```
Device(config)#transceiver type all
Device(config-xcvr-type)# no monitoring
Device(config-xcvr-type)#end
Device# show interfaces transceiver detail
```

Transceiver monitoring is disabled for all interfaces.
<output truncated>

Related Commands

Command	Description
transceiver type all	Enters the transceiver type configuration mode.
show interfaces transceiver	Display the physical properties of a small form-factor pluggable (SFP) module interface.

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

profile-number 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 3.3SE	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.

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

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

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

profile-number 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 3.3SE Cisco IOS XE 3.3SE	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).

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

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

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 (config-if)

Command History	Release	Modification
	Cisco IOS XE 3.3SE Cisco IOS XE 3.3SE	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).



Note Attachment information is not supported in Cisco IOS XE Denali 16.1.1 and later releases.

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

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

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

Command History	Release	Modification
	Cisco IOS XE 3.3SE	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 device 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.

This example shows how to enable EEE for an interface:

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

This example shows how to disable EEE for an interface:

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

high <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 high value must be lower than the value set for the low-priority ports and higher than the value set for the switch.
low <i>value</i>	Sets the power priority for the ports configured as low-priority ports. The range is 1 to 27. The low value must be higher than the value set for the high-priority ports and the value set for the switch.
switch <i>value</i>	Sets the power priority for the switch. The range is 1 to 27. The switch 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 3.3SE Cisco IOS XE 3.3SE	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.

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

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] | never | port priority {high | low} | static [max
max-wattage]}
no power inline {auto | never | port priority {high | low} | static [max max-wattage]}
```

Syntax Description		
auto		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.
max <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.
never		Disables device detection, and disables power to the port.
port		Configures the power priority of the port. The default priority is low.
priority { high low }		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.
static		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 3.3SE	This command was introduced.

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:

```
Device(config)# interface gigabitethernet1/0/1
Device(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.

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:

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

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

```
Device(config)# interface gigabitethernet1/0/2
Device(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:

```
Device(config)# interface gigabitethernet1/0/2
Device(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:

```
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# power inline port priority high
```

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	action errdisable	(Optional) Configures the device 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.
	action log	(Optional) Configures the device 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 3.3SE	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 device 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 device takes action when a powered device consumes more power than the allocated maximum amount.

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

When power policing is enabled, the device 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
2. The device 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 device 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 device 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_{max}* limitation and might experience an *I_{cut}* 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 device 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 device is locked to CDP, it does not provide power to devices that send LLDP requests. If CDP is disabled after the device has locked on it, the device 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 device 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 device either turns power off to the port, or the device generates a syslog message and updates the LEDs (the port LEDs are blinking amber) while still providing power to the device.

- To configure the device 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 device 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 device.

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 device to generate a syslog message on the PoE port on a device:

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

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.
slot		Selects the switch power supply to set.
A		Selects the power supply in slot A.
B		Selects the power supply in slot B. Note Power supply slot B is the closest slot to the outer edge of the switch.
off		Sets the switch power supply to off.
on		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 3.3SE	This command was introduced.

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:

```
Device> 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
Device
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:

```
Device> 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:

```
Device> 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
```

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	
Command History	Release	Modification
	Cisco IOS XE 3.3SE	This command was introduced.

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

```
Device# 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	switch <i>stack-member-number</i> (Optional) Specifies the stack member number.				
Command Default	None				
Command Modes	Privileged EXEC				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE 3.3SE</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE 3.3SE	This command was introduced.
Release	Modification				
Cisco IOS XE 3.3SE	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:

```
Device# 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

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 {l2 | l3} | l3-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.
down-when-looped	(Optional) Displays states related to down-when-looped detection.
phy	(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.
detail	(Optional) Displays details about the PHY internal registers.
port-asic	(Optional) Displays information about the port ASIC internal registers.
statistics	Displays port ASIC statistics, including the Rx/Sup Queue and miscellaneous statistics.
exceptions	Displays port ASIC exception statistics.
interface <i>interface-id</i>	Specifies the interface for which to display port ASIC statistics.
l2	Displays statistics for the Layer 2 interface.
l3	Displays statistics for the Layer 3 interface.
l3-ifid <i>if-id</i>	Specifies the Layer 3 IF interface ID for which to display port ASIC statistics.
port-ifid <i>if-id</i>	Specifies the PortIF interface ID for which to display port ASIC statistics.
vlan-ifid <i>if-id</i>	Specifies the VLANIF interface ID for which to display port ASIC statistics.
switch <i>stack-member-number</i>	(Optional) Specifies the stack member number for which to display send and receive statistics.
asic <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 3.3SE	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:

```
Device# 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
```

```
show controllers ethernet-controller
```

```
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.
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.

Field	Description
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.
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.

Field	Description
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.
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.

Field	Description
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.
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 ¹ 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.

Field	Description
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.
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.

¹ 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 ² 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.

Field	Description
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.
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.

² FCS = frame check sequence

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

```
Device# 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
```

show controllers utilization

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

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

Syntax Description	<i>interface-id</i> (Optional) ID of the physical interface.	
Command Default	None	
Command Modes	User EXEC Privileged EXEC	
Command History	Release	Modification
	Cisco IOS XE 3.3SE	This command was introduced.

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

```
Device> 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:

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

Table 4: Show controllers utilization Field Descriptions

Field	Description
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.

Field	Description
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		
capabilities		Displays EEE capabilities for the specified interface.
status		Displays EEE status information for the specified interface.
interface <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 3.3SE	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.

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

```
Device# 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:

```
Device# 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.

```
Device# show eee status interface gigabitethernet1/0/4
Gil/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 is operational and the ports are in low power save mode:

```
Device# show eee status interface gigabitethernet1/0/3
Gil/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:

```
Device# show eee status interface gigabitethernet1/0/3
Gil/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"> • N/A—The port is not capable of EEE. • Disabled—The port EEE is disabled. • 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. • Operational—The port EEE is enabled and operating. <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>

Field	Description
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">• N/A—The port is not capable of EEE.• Interrupted—The link partner is in the process of moving to low power mode.• Low Power—The link partner is in low power mode.• None—EEE is disabled or not capable at the link partner side.• Received—The link partner is in low power mode and there is traffic activity. <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	
all	Displays the fan and temperature environmental status and the status of the internal power supplies.
fan	Displays the switch fan status.
power	Displays the internal power status of the active switch.
all	(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 stack masteractive switch.
switch	(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.
stack	Displays all environmental status for each switch in the stack or for the specified switch. This keyword is available only on stacking-capable switches.
temperature	Displays the switch temperature status.
status	(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 3.3SE	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 stack masteractive 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:

```
Device>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 OK
FAN PS-2 is NOT PRESENT
Switch 1: SYSTEM TEMPERATURE is OK
SW  PID                      Serial#      Status          Sys Pwr  PoE Pwr  Watts
--  -
1A  PWR-C2-250WAC              LIT16372A1M  OK              Good      Good      250
1B  Not Present
```

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

```
Device>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 all** command on the stack masteractive switch:

```
Device# show env power all
SW  PID                      Serial#      Status          Sys Pwr  PoE Pwr  Watts
--  -
1A  PWR-C2-250WAC              LIT16372A1M  OK              Good      Good      250
1B  Not Present
```

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

```
Device> 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.

```
Device> 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 3.3SE	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.

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 3.3SE	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.

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

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}] | 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.
vlan <i>vlan-id</i>	(Optional) VLAN identification. The range is 1 to 4094.
accounting	(Optional) Displays accounting information on the interface, including active protocols and input and output packets and octets. Note The display shows only packets processed in software; hardware-switched packets do not appear.
capabilities	(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.
module <i>number</i>	(Optional) Displays capabilities of all interfaces on the switch or specified stack member. This option is not available if you entered a specific interface ID.
debounce	(Optional) Displays port debounce timer information for an interface.
description	(Optional) Displays the administrative status and description set for an interface.
etherchannel	(Optional) Displays interface EtherChannel information.
flowcontrol	(Optional) Displays interface flow control information.
mtu	(Optional) Displays the MTU for each interface or for the specified interface.
pruning	(Optional) Displays trunk VTP pruning information for the interface.
stats	(Optional) Displays the input and output packets by switching the path for the interface.

status	(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.
err-disabled	(Optional) Displays interfaces in an error-disabled state.
trunk	(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 3.3SE	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.

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

```
Device# 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:

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:

```

Device# show interfaces gigabitethernet1/0/2 description
Interface          Status      Protocol Description
Gil/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:

```

Device# 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:

```

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

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

```

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

```

Device# 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:

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

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:

```
Device# 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:

```
Device# 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.

```
Device# 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
```

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.
errors	(Optional) Displays error counters.
etherchannel	(Optional) Displays EtherChannel counters, including octets, broadcast packets, multicast packets, and unicast packets received and sent.
module <i>stack-member-number</i>	(Optional) Displays counters for the specified stack member. Note In this command, the module keyword refers to the stack member number. The module number that is part of the interface ID is always zero.
protocol status	(Optional) Displays the status of protocols enabled on interfaces.
trunk	(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 3.3SE Cisco IOS XE 3.3SE	This command was introduced.

Usage Guidelines

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

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

```
Device# 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.

```
Device# 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:

```
Device# 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.

```
Device# 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>

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** [{*module number*}]

Syntax Description	<p><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.</p> <p>module number (Optional) Displays switchport configuration of all interfaces on the switch or specified stack member.</p> <p>This option is not available if you entered a specific interface ID.</p>				
Command Default	None				
Command Modes	Privileged EXEC				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE 3.3SE</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE 3.3SE	This command was introduced.
Release	Modification				
Cisco IOS XE 3.3SE	This command was introduced.				
Usage Guidelines	<p>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.</p> <p>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.</p>				



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

```
Device# 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
```

show interfaces switchport

```

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.
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.

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**}]

Syntax Description	
<i>interface-id</i>	(Optional) ID of the physical interface, including type, stack member (stacking-capable switches only) module, and port number.
detail	(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.
module number	(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.
properties	(Optional) Displays speed, duplex, and inline power settings on an interface.
supported-list	(Optional) Lists all supported transceivers.

Command Modes	
	User EXEC
	Privileged EXEC

Command History	Release	Modification
	Cisco IOS XE 3.3SE	This command was introduced.

Examples

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

```
Device# show interfaces transceiver
```

```
If device is externally calibrated, only calibrated values are printed.
++ : high alarm, + : high warning, - : low warning, -- : low alarm.
NA or N/A: not applicable, Tx: transmit, Rx: receive.
mA: milliamperes, dBm: decibels (milliwatts).
```

Port	Temperature (Celsius)	Voltage (Volts)	Current (mA)	Optical Tx Power (dBm)	Optical Rx Power (dBm)
Gi5/1/2	42.9	3.28	22.1	-5.4	-8.1
Te5/1/3	32.0	3.28	19.8	2.4	-4.2

```
Device# show interfaces gigabitethernet1/1/1 transceiver properties
Name : Gi1/1/1
Administrative Speed: auto
Operational Speed: auto
Administrative Duplex: auto
```

show interfaces transceiver

```
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:

```
Device# 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

```
Device# show interfaces transceiver supported-list
Transceiver Type          Cisco p/n min version
                          supporting DOM
```

DWDM GBIC	ALL
DWDM SFP	ALL
RX only WDM GBIC	ALL
DWDM XENPAK	ALL
DWDM X2	ALL
DWDM XFP	ALL
CWDM GBIC	NONE
CWDM X2	ALL
CWDM XFP	ALL
XENPAK ZR	ALL
X2 ZR	ALL
XFP ZR	ALL
Rx_only_WDM_XENPAK	ALL
XENPAK_ER	10-1888-04
X2_ER	ALL
XFP_ER	ALL
XENPAK_LR	10-1838-04
X2_LR	ALL
XFP_LR	ALL

```

XENPAK_LW          ALL
X2_LW              ALL
XFP_LW             NONE
XENPAK_SR          NONE
X2_SR              ALL
XFP_SR             ALL
XENPAK_LX4         NONE
X2_LX4             NONE
XFP_LX4            NONE
XENPAK_CX4         NONE
X2_CX4             NONE
XFP_CX4            NONE
SX_GBIC            NONE
LX_GBIC            NONE
ZX_GBIC            NONE
CWDM_SFP           ALL
Rx_only_WDM_SFP   NONE
SX_SFP             ALL
LX_SFP             ALL
ZX_SFP             ALL
EX_SFP             ALL
SX_SFP             NONE
LX_SFP             NONE
ZX_SFP             NONE
GigE_BX_U_SFP     NONE
GigE_BX_D_SFP     ALL
X2_LRM             ALL
SR_SFPP            ALL
LR_SFPP            ALL
LRM_SFPP           ALL
ER_SFPP            ALL
ZR_SFPP            ALL
DWDM_SFPP         ALL
GigE_BX_40U_SFP   ALL
GigE_BX_40D_SFP   ALL
GigE_BX_40DA_SFP  ALL
GigE_BX_80U_SFP   ALL
GigE_BX_80D_SFP   ALL
GIG_BXU_SFPP      ALL
GIG_BXD_SFPP      ALL
GIG_BX40U_SFPP    ALL
GIG_BX40D_SFPP    ALL
GigE_Dual_Rate_LX_SFP ALL
CWDM_SFPP         ALL
CPAK_SR10         ALL
CPAK_LR4          ALL
QSFP_LR           ALL
QSFP_SR           ALL

```

Related Commands

Command	Description
transceiver type all	Enters the transceiver type configuration mode.
monitoring	Enables digital optical monitoring.

show memory platform

To display memory statistics of a platform, use the **show memory platform** command in privileged EXEC mode.

show memory platform [{**compressed-swap** | **information** | **page-merging**}]

Syntax Description	
compressed-swap	(Optional) Displays platform memory compressed-swap information.
information	(Optional) Displays general information about the platform.
page-merging	(Optional) Displays platform memory page-merging information.

Command Modes Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Denali 16.1.1	This command was introduced.

Usage Guidelines Prior to Cisco IOS XE Denali 16.3.1, the Free Memory displayed in the command output was obtained from the underlying Linux kernel. This value was not accurate because some memory chunks that was available for use was not considered as free memory.

In Cisco IOS XE Denali 16.3.1, the free memory is accurately computed and displayed in the Free Memory field of the command output.

Examples

The following is sample output from the **show memory platform** command:

```
Switch# show memory platform

Virtual memory   : 12874653696
Pages resident  : 627041
Major page faults: 2220
Minor page faults: 2348631

Architecture    : mips64
Memory (kB)
  Physical      : 3976852
  Total         : 3976852
  Used          : 2761276
  Free          : 1215576
  Active        : 2128196
  Inactive      : 1581856
  Inact-dirty   : 0
  Inact-clean   : 0
  Dirty         : 0
  AnonPages     : 1294984
  Bounce        : 0
  Cached        : 1978168
  Commit Limit  : 1988424
  Committed As  : 3343324
  High Total    : 0
  High Free     : 0
```

```

Low Total      : 3976852
Low Free       : 1215576
Mapped         : 516316
NFS Unstable   : 0
Page Tables    : 17124
Slab           : 0
VMmalloc Chunk : 1069542588
VMmalloc Total : 1069547512
VMmalloc Used  : 2588
Writeback      : 0
HugePages Total : 0
HugePages Free : 0
HugePages Rsvd : 0
HugePage Size  : 2048

Swap (kB)
Total          : 0
Used           : 0
Free           : 0
Cached         : 0

Buffers (kB)   : 437136

Load Average
1-Min          : 1.04
5-Min          : 1.16
15-Min         : 0.94

```

The following is sample output from the **show memory platform information** command:

Device# **show memory platform information**

```

Virtual memory : 12870438912
Pages resident : 626833
Major page faults: 2222
Minor page faults: 2362455

Architecture   : mips64
Memory (kB)
Physical       : 3976852
Total          : 3976852
Used           : 2761224
Free           : 1215628
Active         : 2128060
Inactive       : 1584444
Inact-dirty    : 0
Inact-clean    : 0
Dirty          : 284
AnonPages      : 1294656
Bounce         : 0
Cached         : 1979644
Commit Limit   : 1988424
Committed As   : 3342184
High Total     : 0
High Free      : 0
Low Total      : 3976852
Low Free       : 1215628
Mapped         : 516212
NFS Unstable   : 0
Page Tables    : 17096
Slab           : 0
VMmalloc Chunk : 1069542588
VMmalloc Total : 1069547512

```

show memory platform

```
VMmalloc Used : 2588
Writeback      : 0
HugePages Total: 0
HugePages Free : 0
HugePages Rsvd : 0
HugePage Size  : 2048
```

```
Swap (kB)
Total      : 0
Used       : 0
Free       : 0
Cached     : 0
```

```
Buffers (kB) : 438228
```

```
Load Average
1-Min      : 1.54
5-Min      : 1.27
15-Min     : 0.99
```

show module

To display module information such as switch number, model number, serial number, hardware revision number, software version, MAC address and so on, use this command in user EXEC or privileged EXEC mode.

```
show module [{switch-num}]
```

Syntax Description	<i>switch-num</i> (Optional) Number of the switch.				
Command Default	None				
Command Modes	User EXEC (>) Privileged EXEC (#)				
Command History	<table><thead><tr><th>Release</th><th>Modification</th></tr></thead><tbody><tr><td>Cisco IOS XE Denali 16.1.1</td><td>This command was introduced.</td></tr></tbody></table>	Release	Modification	Cisco IOS XE Denali 16.1.1	This command was introduced.
Release	Modification				
Cisco IOS XE Denali 16.1.1	This command was introduced.				
Usage Guidelines	Entering the show module command without the <i>switch-num</i> argument is the same as entering the show module all command.				
Examples	This example shows how to display information for all the modules on a Cisco Catalyst 3850 Series switch:				

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	switch <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 3.3SE	This command was introduced.

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

```
Device# 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] Gil/0/1 port config Initialized
[10/23/12 14:05:20.379 UTC 16 3] Interface Gil/0/1 initialization done.
[10/23/12 14:05:20.380 UTC 17 3] Gil/0/24 port config Initialized
[10/23/12 14:05:20.380 UTC 18 3] Interface Gil/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
```

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	switch <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	<table border="1"> <thead> <tr> <th style="text-align: left;">Release</th> <th style="text-align: left;">Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE 3.3SE</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE 3.3SE	This command was introduced.
Release	Modification				
Cisco IOS XE 3.3SE	This command was introduced.				

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

```
Device# 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.
```

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*]

Syntax Description	switch <i>stack-member-number</i> (Optional) Specifies the stack member number for which to display messages within a trace buffer.				
Command Default	None				
Command Modes	Privileged EXEC				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE 3.3SE</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE 3.3SE	This command was introduced.
Release	Modification				
Cisco IOS XE 3.3SE	This command was introduced.				

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

```
Device# 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)
```

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

profile-number (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 3.3SE	This command was introduced.

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

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

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 3.3SE	This command was introduced.

This example displays the tunnel identifier and details:

```
Device# 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 platform forward

Use the **show platform forward** privileged EXEC command for an interface to display how the hardware would forward a frame that matches the specified parameters.

```
show platform forward interface-id [ vlan vlan-id ] src-macdst-mac [ l3protocol-id ] [ ipv6
| sap | snap ] [ cos cos [ ip src-ip dst-ip [ frag field ] [ dscp dscp ] { l4protocol-id |
icmp icmp-type icmp-code | igmp igmp-version igmp-type | sctp src-port dst-port | tcp src-post
dst-port flags | udp src-port dst-port ] } [ | { begin | exclude | include } expression ]
```

Syntax Description

<i>interface-id</i>	The input physical interface, the port on which the packet comes in to the switch (including type and port number).
vlan <i>vlan-id</i>	(Optional) Input VLAN ID. The range is 1 to 4094. If not specified, and the input interface is not a routed port, the default is 1.
<i>src-mac</i>	48-bit source MAC address.
<i>dst-mac</i>	48-bit destination MAC address.
ipv6	(Optional) IPv6 frame. This keyword is available only if the switch is running the IP services image.
sap	(Optional) Service access point (SAP) encapsulation type.
snap	(Optional) Subnetwork Access Protocol (SNAP) encapsulation type.
cos <i>cos</i>	(Optional) Class of service (CoS) value of the frame. The range is 0 to 7.
ip <i>src-ip</i> <i>dst-ip</i>	(Optional, but required for IP packets) Source and destination IP addresses in dotted decimal notation.
frag <i>field</i>	(Optional) The IP fragment field for a fragmented IP packet. The range is 0 to 65535.
dscp <i>dscp</i>	(Optional) Differentiated Services Code Point (DSCP) field in the IP header. The range is 0 to 63.
<i>l4protocol-id</i>	The numeric value of the Layer 4 protocol field in the IP header. The range is 0 to 255. For example, 47 is generic routing encapsulation (GRE), and 89 is Open Shortest Path First (OSPF). If the protocol is TCP, User Datagram Protocol (UDP), Internet Control Message Protocol (ICMP), or Internet Group Management Protocol (IGMP), you should use the appropriate keyword instead of a numeric value.
icmp <i>icmp-type</i> <i>icmp-code</i>	ICMP parameters. The <i>icmp-type</i> and <i>icmp-code</i> ranges are 0 to 255.
igmp <i>igmp-version</i> <i>igmp-type</i>	IGMP parameters. The <i>igmp-version</i> range is 1 to 15; the <i>igmp-type</i> range is 0 to 15.
sctp <i>src-port</i> <i>dst-port</i>	Stream Control Transmission Protocol (SCTP) parameters. The ranges for the SCTP source and destination ports are 0 to 65535.

tcp <i>src-port dst-port flags</i>	TCP parameters: TCP source port, destination port, and the numeric value of the TCP flags byte in the header. The src-port and dst-port ranges are 0 to 65535. The flag range is 0 to 1024.
udp <i>src-port dst-port</i>	UDP parameters. The src-port and dst-port ranges are 0 to 65535.
begin	(Optional) Display begins with the line that matches the <i>expression</i> .
exclude	(Optional) Display excludes lines that match the <i>expression</i> .
include	(Optional) Display includes lines that match the specified <i>expression</i> .
<i>expression</i>	Expression in the output to use as a reference point.

Command Modes Privileged EXEC

Command History	Release	Modification
	Cisco IOS XE Denali 16.1.1	This command was reintroduced.

Usage Guidelines You should use this command only when you are working directly with a technical support representative while troubleshooting a problem. Do not use this command unless a technical support representative asks you to do so.

Expressions are case sensitive. For example, if you enter | **exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

show platform hardware fed switch forward

To display device-specific hardware information, use the **show platform hardware fed switch** *switch_number* command.

This topic elaborates only the forwarding-specific options, that is, the options available with the **show platform hardware fed switch** {*switch_num* | **active** | **standby**} **forward summary** command.

The output of the **show platform hardware fed switch** *switch_number* **forward summary** displays all the details about the forwarding decision taken for the packet.

show platform hardware fed switch {*switch_num* | **active** | **standby**} **forward summary**

Syntax Description

switch { <i>switch_num</i> active standby }	The switch for which you want to display information. You have the following options :
	<ul style="list-style-type: none"> • <i>switch_num</i>—ID of the switch. • active—Displays information relating to the active switch. • standby—Displays information relating to the standby switch, if available.

forward summary	Displays packet forwarding information.
------------------------	---

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

Usage Guidelines

Do not use this command unless a technical support representative asks you to. Use this command only when you are working directly with a technical support representative while troubleshooting a problem.

Fields displayed in the command output are explained below.

- **Station Index** : The Station Index is the result of the layer 2 lookup and points to a station descriptor which provides the following:
 - **Destination Index** : Determines the egress port(s) to which the packets should be sent to. Global Port Number(GPN) can be used as the destination index. A destination index with 15 down to 12 bits set indicates the GPN to be used. For example, destination index - 0xF04E corresponds to GPN - 78 (0x4e).
 - **Rewrite Index** : Determines what needs to be done with the packets. For layer 2 switching, this is typically a bridging action
 - **Flexible Lookup Pipeline Stages(FPS)** : Indicates the forwarding decision that was taken for the packet - routing or bridging
 - **Replication Bit Map** : Determines if the packets should be sent to CPU or stack
 - Local Data Copy = 1

- Remote Data copy = 0
- Local CPU Copy = 0
- Remote CPU Copy = 0

Example

This is an example of output from the **show platform hardware fed switch** {*switch_num* | **active** | **standby** } **forward summary** command.

```
Device#show platform hardware fed switch 1 forward summary
```

```
Time: Fri Sep 16 08:25:00 PDT 2016
```

```
Incomming Packet Details:
```

```
###[ Ethernet ]###
```

```
dst      = 00:51:0f:f2:0e:11
src      = 00:1d:01:85:ba:22
type     = ARP
```

```
###[ ARP ]###
```

```
hwtype   = 0x1
ptype    = IPv4
hwlen    = 6
plen     = 4
op       = is-at
hwsrc    = 00:1d:01:85:ba:22
psrc     = 10.10.1.33
hwdst    = 00:51:0f:f2:0e:11
pdst     = 10.10.1.1
```

```
Ingress:
```

```
Switch           : 1
Port              : GigabitEthernet1/0/1
Global Port Number : 1
Local Port Number : 1
Asic Port Number  : 21
ASIC Number       : 0
STP state         :
                  blkLrn31to0: 0xffdffffd
                  blkFwd31to0: 0xffdffffd
Vlan              : 1
Station Descriptor : 170
DestIndex         : 0xF009
DestModIndex      : 2
RewriteIndex      : 2
Forwarding Decision: FPS 2A L2 Destination
```

```
Replication Bitmap:
```

```
Local CPU copy   : 0
Local Data copy  : 1
Remote CPU copy  : 0
Remote Data copy : 0
```

```
Egress:
```

```
Switch           : 1
Outgoing Port     : GigabitEthernet1/0/9
Global Port Number : 9
ASIC Number       : 0
Vlan              : 1
```

show platform resources

To display platform resource information, use the **show platform resources** command in privileged EXEC mode.

show platform resources

This command has no arguments or keywords.

Command Modes Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Denali 16.1.1	This command was introduced.

Usage Guidelines The output of this command displays the used memory, which is total memory minus the accurate free memory.

Example

The following is sample output from the **show platform resources** command:

```
Switch# show platform resources
```

```
**State Acronym: H - Healthy, W - Warning, C - Critical
```

Resource State	Usage	Max	Warning	Critical
Control Processor H	7.20%	100%	90%	95%
DRAM H	2701MB (69%)	3883MB	90%	95%

show platform software ilpower

To display the inline power details of all the PoE ports on the device, use the **show platform software ilpower** command in privileged EXEC mode.

```
show platform software ilpower {details | port {GigabitEthernet interface-number } | system slot-number }
```

Syntax Description	details	Displays inline power details for all the interfaces.
	port	Displays inline power port configuration.
	GigabitEthernet interface-number	The GigabitEthernet interface number. Values range from 0 to 9.
	system slot-number	Displays inline power system configuration.
Command Modes	Privileged EXEC (#)	
Command History	Release	Modification
	Cisco IOS XE Denali 16.3.2	This command was modified. The keyword details argument was added.
	Cisco IOS XE Denali 16.1.1	The command was introduced.

Examples

The following is sample output from the **show platform software ilpower details** command:

```
Device# show platform software ilpower details
ILP Port Configuration for interface Gi1/0/1
  Initialization Done:    Yes
  ILP Supported:         Yes
  ILP Enabled:           Yes
  POST:                  Yes
  Detect On:              No
  Powered Device Detected:      No
  Powered Device Class Done:    No
  Cisco Powered Device:        No
  Power is On:                No
  Power Denied:                No
  Powered Device Type:         Null
  Powerd Device Class:         Null
  Power State:                 NULL
  Current State:               NGWC_ILP_DETECTING_S
  Previous State:              NGWC_ILP_SHUT_OFF_S
  Requested Power in milli watts: 0
  Short Circuit Detected:      0
  Short Circuit Count:         0
  Cisco Powerd Device Detect Count: 0
  Spare Pair mode:            0
  IEEE Detect:                 Stopped
  IEEE Short:                  Stopped
  Link Down:                   Stopped
  Voltage sense:               Stopped
  Spare Pair Architecture:     1
```

show platform software ilpower

```
Signal Pair Power allocation in milli watts: 0
Spare Pair Power On: 0
Powered Device power state: 0
Timer:
  Power Good: Stopped
  Power Denied: Stopped
  Cisco Powered Device Detect: Stopped
```

show platform software process list

To display the list of running processes on a platform, use the **show platform software process list** command in privileged EXEC mode.

```
show platform software process list switch {switch-number | active | standby} {0 | F0 | R0}
[{name process-name | process-id process-ID | sort memory | summary}]
```

Syntax Description	
switch <i>switch-number</i>	Displays information about the switch. Valid values for <i>switch-number</i> argument are from 0 to 9.
active	Displays information about the active instance of the switch.
standby	Displays information about the standby instance of the switch.
0	Displays information about the shared port adapters (SPA) Interface Processor slot 0.
F0	Displays information about the Embedded Service Processor (ESP) slot 0.
R0	Displays information about the Route Processor (RP) slot 0.
name process-name	(Optional) Displays information about the specified process. Enter the process name.
process-id process-ID	(Optional) Displays information about the specified process ID. Enter the process ID.
sort	(Optional) Displays information sorted according to processes.
memory	(Optional) Displays information sorted according to memory.
summary	(Optional) Displays a summary of the process memory of the host device.

Command Modes Privileged EXE (#)

Command History	Release	Modification
	Cisco IOS XE Denali 16.1.1	The command was introduced.

Usage Guidelines Prior to Cisco IOS XE Denali 16.3.1, the Free Memory displayed in the command output was obtained from the underlying Linux kernel. This value was not accurate because some memory chunks that was available for use was not considered as free memory.

In Cisco IOS XE Denali 16.3.1, the free memory is accurately computed and displayed in the Free Memory field of the command output.

Examples

The following is sample output from the **show platform software process list switch active R0** command:

```
Switch# show platform software process list switch active R0 summary

Total number of processes: 278
```

show platform software process list

```

Running          : 2
Sleeping         : 276
Disk sleeping    : 0
Zombies          : 0
Stopped          : 0
Paging           : 0

Up time          : 8318
Idle time        : 0
User time        : 216809
Kernel time      : 78931

Virtual memory   : 12933324800
Pages resident   : 634061
Major page faults: 2228
Minor page faults: 3491744

Architecture     : mips64
Memory (kB)
  Physical        : 3976852
  Total           : 3976852
  Used            : 2766952
  Free            : 1209900
  Active          : 2141344
  Inactive        : 1589672
  Inact-dirty     : 0
  Inact-clean     : 0
  Dirty          : 4
  AnonPages       : 1306800
  Bounce          : 0
  Cached          : 1984688
  Commit Limit    : 1988424
  Committed As    : 3358528
  High Total      : 0
  High Free       : 0
  Low Total       : 3976852
  Low Free        : 1209900
  Mapped          : 520528
  NFS Unstable    : 0
  Page Tables     : 17328
  Slab            : 0
  VmMalloc Chunk  : 1069542588
  VmMalloc Total  : 1069547512
  VmMalloc Used   : 2588
  Writeback       : 0
  HugePages Total: 0
  HugePages Free  : 0
  HugePages Rsvd  : 0
  HugePage Size   : 2048

Swap (kB)
  Total           : 0
  Used            : 0
  Free            : 0
  Cached          : 0

Buffers (kB)     : 439528

Load Average
  1-Min           : 1.13
  5-Min           : 1.18
  15-Min          : 0.92

```

The table below describes the significant fields shown in the displays.

Table 7: show platform software process list Field Descriptions

Field	Description
Name	Displays the command name associated with the process. Different threads in the same process may have different command values.
Pid	Displays the process ID that is used by the operating system to identify and keep track of the processes.
PPid	Displays process ID of the parent process.
Group Id	Displays the group ID
Status	Displays the process status in human readable form.
Priority	Displays the negated scheduling priority.
Size	Prior to Cisco IOS XE Gibraltar 16.10.1: Displays Virtual Memory size. From Cisco IOS XE Gibraltar 16.10.1 onwards: Displays the Resident Set Size (RSS) that shows how much memory is allocated to that process in the RAM.

show platform software process slot switch

To display platform software process switch information, use the **show platform software process slot switch** command in privileged EXEC mode.

```
show platform software process slot switch {switch-number | active | standby} {0 | F0 | R0}
monitor [{cycles no-of-times [{interval delay [{lines number}]}}]
```

Syntax Description

<i>switch-number</i>	Switch number.
active	Specifies the active instance.
standby	Specifies the standby instance.
0	Specifies the shared port adapter (SPA) interface processor slot 0.
F0	Specifies the Embedded Service Processor (ESP) slot 0.
R0	Specifies the Route Processor (RP) slot 0.
monitor	Monitors the running processes.
<i>cycles no-of-times</i>	(Optional) Sets the number of times to run monitor command. Valid values are from 1 to 4294967295. The default is 5.
<i>interval delay</i>	(Optional) Sets a delay after each . Valid values are from 0 to 300. The default is 3.
<i>lines number</i>	(Optional) Sets the number of lines of output displayed. Valid values are from 0 to 512. The default is 0.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Denali 16.1.1	This command was introduced.

Usage Guidelines

The output of the **show platform software process slot switch** and **show processes cpu platform monitor location** commands display the output of the Linux **top** command. The output of these commands display Free memory and Used memory as displayed by the Linux **top** command. The values displayed for the Free memory and Used memory by these commands do not match the values displayed by the output of other platform-memory related CLIs.

Examples

The following is sample output from the **show platform software process slot switch active R0 monitor** command:

```
Switch# show platform software process slot switch active R0 monitor
```

```
top - 00:01:52 up 1 day, 11:20, 0 users, load average: 0.50, 0.68, 0.83
Tasks: 311 total, 2 running, 309 sleeping, 0 stopped, 0 zombie
Cpu(s): 7.4%us, 3.3%sy, 0.0%ni, 89.2%id, 0.0%wa, 0.0%hi, 0.1%si, 0.0%st
Mem: 3976844k total, 3955036k used, 21808k free, 419312k buffers
Swap: 0k total, 0k used, 0k free, 1946764k cached
```

```

  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
  5693 root        20   0  3448 1368  912 R   7  0.0   0:00.07 top
 17546 root        20   0 2044m 244m  79m S   7  6.3 186:49.08 fed main event
 18662 root        20   0 1806m 678m 263m S   5 17.5 215:32.38 linux_iods-imag
 30276 root        20   0  171m  42m  33m S   5  1.1 125:06.77 repm
 17835 root        20   0  935m  74m  63m S   4  1.9  82:28.31 sif_mgr
 18534 root        20   0  182m 150m  10m S   2  3.9   8:12.08 smand
     1 root        20   0  8440 4740 2184 S   0  0.1   0:09.52 systemd
     2 root        20   0     0     0     0 S   0  0.0   0:00.00 kthreadd
     3 root        20   0     0     0     0 S   0  0.0   0:02.86 ksoftirqd/0
     5 root         0 -20     0     0     0 S   0  0.0   0:00.00 kworker/0:0H
     7 root        RT   0     0     0     0 S   0  0.0   0:01.44 migration/0
     8 root        20   0     0     0     0 S   0  0.0   0:00.00 rcu_bh
     9 root        20   0     0     0     0 S   0  0.0   0:23.08 rcu_sched
    10 root        20   0     0     0     0 S   0  0.0   0:58.04 rcuc/0
    11 root        20   0     0     0     0 S   0  0.0 21:35.60 rcuc/1
    12 root        RT   0     0     0     0 S   0  0.0   0:01.33 migration/1

```

Related Commands

Command	Description
show processes cpu platform monitor location	Displays information about the CPU utilization of the IOS-XE processes.

show platform software status control-processor

To display platform software control-processor status, use the **show platform software status control-processor** command in privileged EXEC mode.

show platform software status control-processor [{brief}]

Syntax Description	brief (Optional) Displays a summary of the platform control-processor status.
---------------------------	--

Command Modes	Privileged EXEC (#)
----------------------	---------------------

Command History	Release	Modification
	Cisco IOS XE Denali 16.1.1	This command was introduced.

Usage Guidelines	Prior to Cisco IOS XE Denali 16.3.1, the Free Memory displayed in the command output was obtained from the underlying Linux kernel. This value was not accurate because some memory chunks that was available for use was not considered as free memory.
-------------------------	--

In Cisco IOS XE Denali 16.3.1, the free memory is accurately computed and displayed in the Free Memory field of the command output.

Examples

The following is sample output from the **show platform memory software status control-processor** command:

```
Switch# show platform software status control-processor

2-RP0: online, statistics updated 7 seconds ago
Load Average: healthy
  1-Min: 1.00, status: healthy, under 5.00
  5-Min: 1.21, status: healthy, under 5.00
 15-Min: 0.90, status: healthy, under 5.00
Memory (kb): healthy
  Total: 3976852
  Used: 2766284 (70%), status: healthy
  Free: 1210568 (30%)
  Committed: 3358008 (84%), under 95%
Per-core Statistics
CPU0: CPU Utilization (percentage of time spent)
  User: 4.40, System: 1.70, Nice: 0.00, Idle: 93.80
  IRQ: 0.00, SIRQ: 0.10, IOWait: 0.00
CPU1: CPU Utilization (percentage of time spent)
  User: 3.80, System: 1.20, Nice: 0.00, Idle: 94.90
  IRQ: 0.00, SIRQ: 0.10, IOWait: 0.00
CPU2: CPU Utilization (percentage of time spent)
  User: 7.00, System: 1.10, Nice: 0.00, Idle: 91.89
  IRQ: 0.00, SIRQ: 0.00, IOWait: 0.00
CPU3: CPU Utilization (percentage of time spent)
  User: 4.49, System: 0.69, Nice: 0.00, Idle: 94.80
  IRQ: 0.00, SIRQ: 0.00, IOWait: 0.00

3-RP0: unknown, statistics updated 2 seconds ago
Load Average: healthy
  1-Min: 0.24, status: healthy, under 5.00
  5-Min: 0.27, status: healthy, under 5.00
```

```
15-Min: 0.32, status: healthy, under 5.00
Memory (kb): healthy
  Total: 3976852
  Used: 2706768 (68%), status: healthy
  Free: 1270084 (32%)
  Committed: 3299332 (83%), under 95%
Per-core Statistics
CPU0: CPU Utilization (percentage of time spent)
  User: 4.50, System: 1.20, Nice: 0.00, Idle: 94.20
  IRQ: 0.00, SIRQ: 0.10, IOWait: 0.00
CPU1: CPU Utilization (percentage of time spent)
  User: 5.20, System: 0.50, Nice: 0.00, Idle: 94.29
  IRQ: 0.00, SIRQ: 0.00, IOWait: 0.00
CPU2: CPU Utilization (percentage of time spent)
  User: 3.60, System: 0.70, Nice: 0.00, Idle: 95.69
  IRQ: 0.00, SIRQ: 0.00, IOWait: 0.00
CPU3: CPU Utilization (percentage of time spent)
  User: 3.00, System: 0.60, Nice: 0.00, Idle: 96.39
  IRQ: 0.00, SIRQ: 0.00, IOWait: 0.00

4-RP0: unknown, statistics updated 2 seconds ago
Load Average: healthy
  1-Min: 0.21, status: healthy, under 5.00
  5-Min: 0.24, status: healthy, under 5.00
  15-Min: 0.24, status: healthy, under 5.00
Memory (kb): healthy
  Total: 3976852
  Used: 1452404 (37%), status: healthy
  Free: 2524448 (63%)
  Committed: 1675120 (42%), under 95%
Per-core Statistics
CPU0: CPU Utilization (percentage of time spent)
  User: 2.30, System: 0.40, Nice: 0.00, Idle: 97.30
  IRQ: 0.00, SIRQ: 0.00, IOWait: 0.00
CPU1: CPU Utilization (percentage of time spent)
  User: 4.19, System: 0.69, Nice: 0.00, Idle: 95.10
  IRQ: 0.00, SIRQ: 0.00, IOWait: 0.00
CPU2: CPU Utilization (percentage of time spent)
  User: 4.79, System: 0.79, Nice: 0.00, Idle: 94.40
  IRQ: 0.00, SIRQ: 0.00, IOWait: 0.00
CPU3: CPU Utilization (percentage of time spent)
  User: 2.10, System: 0.40, Nice: 0.00, Idle: 97.50
  IRQ: 0.00, SIRQ: 0.00, IOWait: 0.00

9-RP0: unknown, statistics updated 4 seconds ago
Load Average: healthy
  1-Min: 0.20, status: healthy, under 5.00
  5-Min: 0.35, status: healthy, under 5.00
  15-Min: 0.35, status: healthy, under 5.00
Memory (kb): healthy
  Total: 3976852
  Used: 1451328 (36%), status: healthy
  Free: 2525524 (64%)
  Committed: 1675932 (42%), under 95%
Per-core Statistics
CPU0: CPU Utilization (percentage of time spent)
  User: 1.90, System: 0.50, Nice: 0.00, Idle: 97.60
  IRQ: 0.00, SIRQ: 0.00, IOWait: 0.00
CPU1: CPU Utilization (percentage of time spent)
  User: 4.39, System: 0.19, Nice: 0.00, Idle: 95.40
  IRQ: 0.00, SIRQ: 0.00, IOWait: 0.00
CPU2: CPU Utilization (percentage of time spent)
  User: 5.70, System: 1.00, Nice: 0.00, Idle: 93.30
  IRQ: 0.00, SIRQ: 0.00, IOWait: 0.00
```

show platform software status control-processor

```
CPU3: CPU Utilization (percentage of time spent)
  User: 1.30, System: 0.60, Nice: 0.00, Idle: 98.00
  IRQ: 0.00, SIRQ: 0.10, IOWait: 0.00
```

The following is sample output from the **show platform memory software status control-processor brief** command:

```
Switch# show platform software status control-processor brief
```

Load Average

Slot	Status	1-Min	5-Min	15-Min
2-RP0	Healthy	1.10	1.21	0.91
3-RP0	Healthy	0.23	0.27	0.31
4-RP0	Healthy	0.11	0.21	0.22
9-RP0	Healthy	0.10	0.30	0.34

Memory (kB)

Slot	Status	Total	Used (Pct)	Free (Pct)	Committed (Pct)
2-RP0	Healthy	3976852	2766956 (70%)	1209896 (30%)	3358352 (84%)
3-RP0	Healthy	3976852	2706824 (68%)	1270028 (32%)	3299276 (83%)
4-RP0	Healthy	3976852	1451888 (37%)	2524964 (63%)	1675076 (42%)
9-RP0	Healthy	3976852	1451580 (37%)	2525272 (63%)	1675952 (42%)

CPU Utilization

Slot	CPU	User	System	Nice	Idle	IRQ	SIRQ	IOWait
2-RP0	0	4.10	2.00	0.00	93.80	0.00	0.10	0.00
	1	4.60	1.00	0.00	94.30	0.00	0.10	0.00
	2	6.50	1.10	0.00	92.40	0.00	0.00	0.00
	3	5.59	1.19	0.00	93.20	0.00	0.00	0.00
3-RP0	0	2.80	1.20	0.00	95.90	0.00	0.10	0.00
	1	4.49	1.29	0.00	94.20	0.00	0.00	0.00
	2	5.30	1.60	0.00	93.10	0.00	0.00	0.00
4-RP0	3	5.80	1.20	0.00	93.00	0.00	0.00	0.00
	0	1.30	0.80	0.00	97.89	0.00	0.00	0.00
	1	1.30	0.20	0.00	98.50	0.00	0.00	0.00
9-RP0	2	5.60	0.80	0.00	93.59	0.00	0.00	0.00
	3	5.09	0.19	0.00	94.70	0.00	0.00	0.00
	0	3.99	0.69	0.00	95.30	0.00	0.00	0.00
	1	2.60	0.70	0.00	96.70	0.00	0.00	0.00
9-RP0	2	4.49	0.89	0.00	94.60	0.00	0.00	0.00
	3	2.60	0.20	0.00	97.20	0.00	0.00	0.00

show processes cpu platform monitor

To displays information about the CPU utilization of the IOS-XE processes, use the **show processes cpu platform monitor** command in privileged EXEC mode.

show processes cpu platform monitor location switch {*switch-number* | **active** | **standby**} {**0** | **F0** | **R0**}

Syntax Description	location	Displays information about the Field Replaceable Unit (FRU) location.
	switch	Specifies the switch.
	<i>switch-number</i>	Switch number.
	active	Specifies the active instance.
	standby	Specifies the standby instance.
	0	Specifies the shared port adapter (SPA) interface processor slot 0.
	F0	Specifies the Embedded Service Processor (ESP) slot 0.
	R0	Specifies the Route Processor (RP) slot 0.

Command Modes Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Denali 16.1.1	This command was introduced.

Usage Guidelines The output of the **show platform software process slot switch** and **show processes cpu platform monitor location** commands display the output of the Linux **top** command. The output of these commands display Free memory and Used memory as displayed by the Linux **top** command. The values displayed for the Free memory and Used memory by these commands do not match the values displayed by the output of other platform-memory related CLIs.

Examples

The following is sample output from the **show processes cpu monitor location switch active R0** command:

```
Switch# show processes cpu platform monitor location switch active R0

top - 00:04:21 up 1 day, 11:22, 0 users, load average: 0.42, 0.60, 0.78
Tasks: 312 total, 4 running, 308 sleeping, 0 stopped, 0 zombie
Cpu(s): 7.4%us, 3.3%sy, 0.0%ni, 89.2%id, 0.0%wa, 0.0%hi, 0.1%si, 0.0%st
Mem: 3976844k total, 3956928k used, 19916k free, 419312k buffers
Swap: 0k total, 0k used, 0k free, 1947036k cached

  PID USER      PR  NI  VIRT  RES  SHR  S  %CPU  %MEM    TIME+  COMMAND
  6294 root      20   0  3448  1368  912  R   9.0   0.0   0:00.07 top
 17546 root      20   0 2044m 244m   79m  S   6.3  187:02.07 fed main event
 30276 root      20   0  171m  42m   33m  S   7.1   1.1 125:15.54 repm
    16 root      20   0     0     0     0  S   5.0   0.0  22:07.92 rcuc/2
    21 root      20   0     0     0     0  R   5.0   0.0  22:13.24 rcuc/3
```

show processes cpu platform monitor

```

18662 root      20    0 1806m 678m 263m R    5 17.5 215:47.59 linux_iosd-imag
   11 root      20    0     0    0    0 S    4  0.0 21:37.41 rcuc/1
10333 root      20    0 6420 3916 1492 S    4  0.1  4:47.03 btrace_rotate.s
   10 root      20    0     0    0    0 S    2  0.0  0:58.13 rcuc/0
 6304 root      20    0   776   12    0 R    2  0.0  0:00.01 ls
17835 root      20    0 935m  74m  63m S    2  1.9 82:34.07 sif_mgr
   1 root      20    0 8440 4740 2184 S    0  0.1  0:09.52 systemd
   2 root      20    0     0    0    0 S    0  0.0  0:00.00 kthreadd
   3 root      20    0     0    0    0 S    0  0.0  0:02.86 ksoftirqd/0
   5 root        0 -20     0    0    0 S    0  0.0  0:00.00 kworker/0:0H
   7 root      RT    0     0    0    0 S    0  0.0  0:01.44 migration/0

```

Related Commands

Command	Description
show platform software process slot switch	Displays platform software process switch information.

show processes memory platform

To display memory usage per Cisco IOS XE process, use the **show processes memory platform** command in privileged EXEC mode.

```
show processes memory platform [{detailed {name process-name | process-id process-ID} [{location | maps [{location}] | smaps [{location}]}] | location | sorted [{location}]}] switch {switch-number | active | standby} {0 | F0 | R0}
```

Syntax Description		
detailed <i>process-name</i>		(Optional) Displays detailed memory information for a specified Cisco IOS XE process.
name <i>process-name</i>		(Optional) Matches the Cisco IOS XE process name.
process-id <i>process-ID</i>		(Optional) Matches the Cisco IOS XE process ID.
location		(Optional) Displays information about the FRU location.
maps		(Optional) Displays memory maps of a process.
smaps		(Optional) Displays smaps of a process.
sorted		(Optional) Displays the sorted output based on the total memory used by Cisco IOS XE processes.
switch <i>switch-number</i>		Displays information about the device.
active		Displays information about the active instance of the switch.
standby		Displays information about the standby instance of the switch.
0		Displays information about the SPA-Inter-Processor slot 0.
F0		Displays information about the Embedded Service Processor (ESP) slot 0.
R0		Displays information about the Route Processor (RP) slot 0.

Command Modes Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Denali 16.1.1	The command was introduced.

show processes memory platform

Usage Guidelines

Prior to Cisco IOS XE Denali 16.3.1, the Free Memory displayed in the command output was obtained from the underlying Linux kernel. This value was not accurate because some memory chunks that was available for use was not considered as free memory.

In Cisco IOS XE Denali 16.3.1, the free memory is accurately computed and displayed in the Free Memory field of the command output.

Examples

The following is sample output from the **show processes memory platform** command:

```
Switch# show processes memory platform

System memory: 3976852K total, 2761580K used, 1215272K free,
Lowest: 1215272K
  Pid  Text      Data  Stack  Dynamic  RSS    Total  Name
-----
    1  1246     4400   132    1308    4400   8328   systemd
   96   233     2796   132     132    2796  12436  systemd-journal
  105   284     1796   132     176    1796   5208   systemd-udev
  707    52     2660   132     172    2660  11688  in.telnetd
  744   968     3264   132    1700    3264   5800   brelay.sh
  835    52     2660   132     172    2660  11688  in.telnetd
  863   968     3264   132    1700    3264   5800   brelay.sh
  928   968     3996   132    2312    3996   6412   reflector.sh
  933   968     3976   132    2312    3976   6412   droputil.sh
  934   968     2140   132     528    2140   4628   oom.sh
  936   173     936    132    132     936    3068   xinetd
  945   968     1472   132    132    1472   4168   libvirtd.sh
  947   592    43164   132   3096   43164  154716  repm
  954    45      932    132    132     932    3132   rpcbind
  986   482     3476   132    132    3476  169288  libvirtd
  988    66      940    132    132     940    2724   rpc.statd
  993   968     928    132    132     928    4232   boothelper_evt.
 1017   21      640    132    132     640    2500   inotifywait
 1089   102    1200    132    132    1200   3328   rpc.mountd
 1328    9     2940    132    148    2940  13844   rotee
 1353   39     532    132    132     532    2336   sleep

!
!
!
```

The following is sample output from the **show processes memory platform information** command:

```
Switch# show processes memory platform location switch active R0

System memory: 3976852K total, 2762844K used, 1214008K free,
Lowest: 1214008K
  Pid  Text      Data  Stack  Dynamic  RSS    Total  Name
-----
    1  1246     4400   132    1308    4400   8328   systemd
   96   233     2796   132     132    2796  12436  systemd-journal
  105   284     1796   132     176    1796   5208   systemd-udev
  707    52     2660   132     172    2660  11688  in.telnetd
  744   968     3264   132    1700    3264   5800   brelay.sh
  835    52     2660   132     172    2660  11688  in.telnetd
  863   968     3264   132    1700    3264   5800   brelay.sh
  928   968     3996   132    2312    3996   6412   reflector.sh
  933   968     3976   132    2312    3976   6412   droputil.sh

!
!
!
```

The following is sample output from the **show processes memory platform sorted** command:

```
Switch# show processes memory platform sorted

System memory: 3976852K total, 2762884K used, 1213968K free,
Lowest: 1213968K
  Pid   Text      Data  Stack  Dynamic    RSS    Total      Name
-----
  9655  3787     264964  136    18004    264964  2675968    wcm
 17261   324     248588  132    103908   248588  2093076    fed main event
  7885 149848    684864  136      80     684864  1853548    linux_iosd-imag
 17891   398     75772  136    1888     75772   958240    sif_mgr
 17067  1087    77912  136    1796    77912   702184    platform_mgr
  4268   391    102084  136    5596   102084  482656    cli_agent
  4856   357    93388  132    3680    93388   340052    dbm
 29842  8722    64428  132    8056    64428   297068    fman_fp_image
  5960  9509    76088  136    3200    76088   287156    fman_rp
!
!
!
```

The following is sample output from the **show processes memory platform sorted location switch active R0** command:

```
Switch# show processes memory platform sorted location switch active R0

System memory: 3976852K total, 2763584K used, 1213268K free,
Lowest: 1213268K
  Pid   Text      Data  Stack  Dynamic    RSS    Total      Name
-----
  9655  3787     264968  136    18004    264968  2675968    wcm
 17261   324     249020  132    103908   249020  2093076    fed main event
  7885 149848    684912  136      80     684912  1853548    linux_iosd-imag
 17891   398     75884  136    1888     75884   958240    sif_mgr
 17067  1087    77820  136    1796    77820   702184    platform_mgr
  4268   391    102084  136    5596   102084  482656    cli_agent
  4856   357    93388  132    3680    93388   340052    dbm
 29842  8722    64428  132    8056    64428   297068    fman_fp_image
  5960  9509    76088  136    3200    76088   287156    fman_rp
!
!
!
```

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

Command Modes	
	User EXEC
	Privileged EXEC

Command History	Release	Modification
	Cisco IOS XE 3.3SE	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.

```
Device> 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
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:

```

Device> 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.

```

Device> 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 8: show power inline Field Descriptions

Field	Description
Available	The total amount of configured power ³ 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.
Oper	Operating mode: <ul style="list-style-type: none"> • on—The powered device is detected, and power is applied. • off—No PoE is applied. • faulty—Device detection or a powered device is in a faulty state. • power-deny—A powered device is detected, but no PoE is available, or the maximum wattage exceeds the detected powered-device maximum.

Field	Description
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>CutoffPower</i> field in the show power inline police 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.

³ 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:

```
Device> 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

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
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.

```
Device> 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 9: show power inline police Field Descriptions

Field	Description
Available	The total amount of configured power ⁴ 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.

Field	Description
Oper State	<p>Operating mode:</p> <ul style="list-style-type: none"> • errdisable—Policing is enabled. • faulty—Device detection on a powered device is in a faulty state. • off—No PoE is applied. • on—The powered device is detected, and power is applied. • power-deny—A powered device is detected, but no PoE is available, or the real-time power consumption exceeds the maximum power allocation. <p>Note 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"> • errdisable—Policing is enabled, and the switch shuts down the port when the real-time power consumption exceeds the maximum power allocation. • log—Policing is enabled, and the switch generates a syslog message when the real-time power consumption exceeds the maximum power allocation. • none—Policing is disabled.
Oper Police	<p>Policing status:</p> <ul style="list-style-type: none"> • errdisable—The real-time power consumption exceeds the maximum power allocation, and the switch shuts down the PoE port. • log—The real-time power consumption exceeds the maximum power allocation, and the switch generates a syslog message. • n/a—Device detection is disabled, power is not applied to the PoE port, or no policing action is configured. • ok—Real-time power consumption is less than the maximum power allocation.
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.

⁴ 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.

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 [{budgeting | detail | load-shedding | neighbors}] [order power-stack-name] |
[{stack-name [stack-id] | switch [switch-id]]}
```

Syntax Description	
budgeting	(Optional) Displays the stack power budget table.
detail	(Optional) Displays the stack power stack details.
load-shedding	(Optional) Displays the stack power load shedding table.
neighbors	(Optional) Displays the stack power neighbor table.
order <i>power-stack-name</i>	(Optional) Displays the load shedding priority for a power stack. Note This keyword is available only after the load-shedding keyword.
stack-name	(Optional) Displays budget table, details, or neighbors for all power stacks or the specified power stack. Note This keyword is not available after the load-shedding keyword.
<i>stack-id</i>	(Optional) Power stack ID for the power stack. The stack ID must be 31 characters or less.
switch	(Optional) Displays budget table, details, load-shedding, or neighbors for all switches or the specified switch.
<i>switch-id</i>	(Optional) Switch ID for the switch. The switch number is from 1 to 9.

Command Modes Privileged EXEC

Command History	Release	Modification
	Cisco IOS XE Denali 16.3.2	Support for all the options was enabled for this command.
	Cisco IOS XE Denali 16.1.1	This command was reintroduced.

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:

show stack-power

```

Device# 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 350    150   200    0       1   1

```

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

```

Device# show stack-power budgeting
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 350    150   200    0       1   1

      Power Stack      PS-A  PS-B  Power  Alloc  Avail  Consumd Pwr
SW  Name              (W)   (W)   Budgt (W) Power (W) Pwr (W) Sys/PoE (W)
--  -----
1   Powerstack-1      350   0     200    200    0     60 /0
-----
Totals:                200    0     60 /0

```

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

power-stack-name (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 3.3SE	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:

```
Device# 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
```

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 3.3SE	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:

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

show tech-support

To automatically run **show** commands that display system information, use the **show tech-support** command in the privilege EXEC mode.

show tech-support

[**cef** | **cft** | **eigrp** | **evc** | **fnf**] | [**ipc** | **ipmulticast** | **ipsec** | **mfib** | **nat** | **nbar** | **onep** | **ospf** | **page** | **password** | **rsvp** | **subscriber** | **vrrp** | **wccp** | **wireless**]

Syntax	Description
cef	(Optional) Displays CEF related information.
cft	(Optional) Displays CFT related information.
eigrp	(Optional) Displays EIGRP related information.
evc	(Optional) Displays EVC related information.
fnf	(Optional) Displays flexible netflow related information.
ipc	(Optional) Displays IPC related information.
ipmulticast	(Optional) Displays IP multicast related information.
ipsec	(Optional) Displays IPSEC related information.
mfib	(Optional) Displays MFIB related information.
nat	(Optional) Displays NAT related information.
onep	(Optional) Displays ONEP related information.
ospf	(Optional) Displays OSPF related information.
page	(Optional) Displays the command output on a single page at a time. Use the Return key to display the next line of output or use the space bar to display the next page of information. If not used, the output scrolls (that is, it does not stop for page breaks). Press the Ctrl-C keys to stop the command output.
password	(Optional) Leaves passwords and other security information in the output. If not used, passwords and other security-sensitive information in the output are replaced with the label "<removed>".
subscriber	(Optional) Displays subscriber related information.
vrrp	(Optional) Displays VRRP related information.
wccp	(Optional) Displays WCCP related information.
wireless	(Optional) Displays wireless related information.

Command Modes Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Denali 16.3.2	This command was enhanced to display of the outputs of the following commands in the output modifier : <ul style="list-style-type: none"> • show power inline • show platform software ilpower details • show power inline police • show stack-power budgeting
	Cisco IOS XE Denali 16.1.1	This command was implemented on the Cisco Catalyst 3650 Switch

Usage Guidelines

The output from the **show tech-support** command is very long. To better manage this output, you can redirect the output to a file (for example, **show tech-support > filename**) in the local writable storage file system or the remote file system. Redirecting the output to a file also makes sending the output to your Cisco Technical Assistance Center (TAC) representative easier.

You can use one of the following redirection methods:

- **> filename** - Redirects the output to a file.
- **>> filename** - Redirects the output to a file in append mode.

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 3.3SE	This command was introduced.

Usage Guidelines

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

Device# **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		
	10	Specifies that the port runs at 10 Mb/s.
	100	Specifies that the port runs at 100 Mb/s.
	1000	Specifies that the port runs at 1000 Mb/s. This option is valid and visible only on 10/100/1000 Mb/s ports.
	auto	Automatically detects the speed the port should run at based on the port at the other end of the link. If you use the 10 , 100 , or 1000 keywords with the auto keyword, the port only autonegotiates at the specified speeds.
	nonegotiate	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 3.3SE	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 reenables 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:

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

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

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

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

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

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	stack <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.
	switch <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 3.3SE	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:

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

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	<p>multicast Specifies that unknown multicast traffic should be blocked.</p> <p>Note Only pure Layer 2 multicast traffic is blocked. Multicast packets that contain IPv4 or IPv6 information in the header are not blocked.</p>				
	<p>unicast Specifies that unknown unicast traffic should be blocked.</p>				
Command Default	Unknown multicast and unicast traffic is not blocked.				
Command Modes	Interface configuration				
Command History	<table border="1"> <thead> <tr> <th data-bbox="342 924 1101 980">Release</th> <th data-bbox="1101 924 1497 980">Modification</th> </tr> </thead> <tbody> <tr> <td data-bbox="342 980 1101 1037">Cisco IOS XE 3.3SE</td> <td data-bbox="1101 980 1497 1037">This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE 3.3SE	This command was introduced.
Release	Modification				
Cisco IOS XE 3.3SE	This command was introduced.				
Usage Guidelines	<p>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.</p> <p>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.</p> <p>Blocking unknown multicast or unicast traffic is not automatically enabled on protected ports; you must explicitly configure it.</p> <p>For more information about blocking packets, see the software configuration guide for this release.</p> <p>This example shows how to block unknown unicast traffic on an interface:</p> <pre>Device(config-if)# switchport block unicast</pre> <p>You can verify your setting by entering the show interfaces interface-id switchport privileged EXEC command.</p>				

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 3.3SE	This command was introduced.

Usage Guidelines	<p>You can verify your setting by entering the show system mtu privileged EXEC command.</p> <p>The switch does not support the MTU on a per-interface basis.</p> <p>If you enter a value that is outside the allowed range for the specific type of interface, the value is not accepted.</p>
-------------------------	--

Examples

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

```
Device(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.
```

test mcu read-register

To enable debugging of the Power over Ethernet (PoE) controller, use the **test mcu read-register** command in privileged EXEC mode.

test mcu read-register {**det-cls-offset** | **manufacture-id** | **port-mode**}

Syntax Description	
det-cls-offset	Displays the read detection classification register summary.
manufacture-id	Displays the PoE controller manufacture ID.
port-mode	Displays the port mode details.

Command Modes Privileged EXEC

Command History	Release	Modification
	Cisco IOS XE 3.3SE	This command was introduced.

Examples

The following is sample output from the **test mcu read-register det-cls-offset** command:

```
Device# test mcu read-register det-cls-offset 1
DETECTION ENABLE BIT SUMMARY

Controller   port1      port2      port3      port4      register
-----
1            1          0          1          0          5
2            1          0          1          0          5
3            1          0          1          0          5
4            1          0          1          0          5
5            1          0          1          0          5
6            1          0          1          0          5
7            1          0          1          0          5
8            1          0          1          0          5
9            1          0          1          0          5
10           1          0          1          0          5
11           0          0          1          0          4
12           1          0          0          0          1

CLASSIFICATION ENABLE BIT SUMMARY

Controller   port1      port2      port3      port4      register
-----

```

1	1	0	1	0	5
2	1	0	1	0	5
3	1	0	1	0	5
4	1	0	1	0	5
5	1	0	1	0	5
6	1	0	1	0	5
7	1	0	1	0	5
8	1	0	1	0	5
9	1	0	1	0	5
10	1	0	1	0	5
11	0	0	1	0	4
12	1	0	0	0	1

The following is sample output from the **test mcu read-register manufacture-id** command:

```
MANUFACTURE ID : DEVICE_BCM_PALPATINE reg_val = 0x1B
```

The following is sample output from the **test mcu read-register port-mode** command:

```
PORT MODE SUMMERY
```

Controller	port1	port2	port3	port4	register (hexadecimal)
1	01	00	01	00	22
2	01	00	01	00	22
3	01	00	01	00	22
4	01	00	01	00	22
5	01	00	01	00	22
6	01	00	01	00	22
7	01	00	01	00	22
8	01	00	01	00	22
9	01	00	01	00	22
10	01	00	01	00	22
11	00	00	01	00	20
12	01	00	00	00	2

transceiver type all

To enter the transceiver type configuration mode and enable transceiver monitoring, enter the **transceiver type all** command in global configuration mode. This command does not have the **no** form.

transceiver type all

Syntax Description This command has no arguments or keywords.

Command Default Transceiver type configuration is disabled.

Command Modes Global configuration

Command History	Release	Modification
	Cisco IOS XE Denali 16.3.6	This command was introduced.

Usage Guidelines After you have entered the transceiver type configuration mode, you can enter the **monitoring** command to enable digital optical monitoring.

Related Commands	Command	Description
	monitoring	Enables digital optical monitoring.

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	
vlan-id	(Optional) The VLAN for voice traffic. The range is 1 to 4094.
cos <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.
dscp <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.
dot1p	(Optional) Configures the phone to use IEEE 802.1p priority tagging and to use VLAN 0 (the native VLAN).
none	(Optional) Does not instruct the Cisco IP phone about the voice VLAN. The phone uses the configuration from the phone key pad.
untagged	(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 3.3SE	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.

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

```
Device(config)# network-policy profile 1  
Device(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:

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

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

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

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	
vlan-id	(Optional) The VLAN for voice traffic. The range is 1 to 4094.
cos <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.
dscp <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.
dot1p	(Optional) Configures the phone to use IEEE 802.1p priority tagging and to use VLAN 0 (the native VLAN).
none	(Optional) Does not instruct the Cisco IP phone about the voice VLAN. The phone uses the configuration from the phone key pad.
untagged	(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 3.3SE	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.

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

```
Device(config)# network-policy profile 1  
Device(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:

```
Device(config)# network-policy profile 1  
Device(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:

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

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	TenGigabitEthernet <i>interface-name</i>	Configures 10-Gigabit Ethernet interface. Values range from 0 to 9.
	Vlan <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 3.3SE	This command was introduced.

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

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

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

```
Device# #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.
	description <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 3.3SE	This command was introduced.

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

```
Device# 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:

```
Device# 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	frame-size <i>size</i>	Specifies the link test frame size for each packet. The values range from 1 to 1400.
	number-of-frames <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 3.3SE	This command was introduced.

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

```
Device# 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.
	TenGigabitEthernet <i>interface-name</i>	The 10-Gigabit Ethernet interface number. The values range from 0 to 9.
	Vlan <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 3.3SE	This command was introduced.

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

```
Device# 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	GigabitEthernet <i>interface</i>	The Gigabit Ethernet interface number. Values range from 0 to 9.
	TenGigabitEthernet <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 3.3SE	This command was introduced.

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

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

wireless peer-blocking forward-upstream