



# Configuring Interface Characteristics

- [Information About Configuring Interface Characteristics, on page 1](#)
- [How to Configure Interface Characteristics, on page 10](#)
- [Monitoring Interface Characteristics, on page 22](#)
- [Configuration Examples for Interface Characteristics, on page 24](#)
- [Additional References for the Interface Characteristics Feature, on page 26](#)
- [Feature History and Information for Configuring Interface Characteristics, on page 27](#)

## Information About Configuring Interface Characteristics

### Interface Types

This section describes the different types of interfaces supported by the switch. The rest of the chapter describes configuration procedures for physical interface characteristics.



---

**Note** The stack ports on the rear of the stacking-capable switches are not Ethernet ports and cannot be configured.

---

### Port-Based VLANs

A VLAN is a switched network that is logically segmented by function, team, or application, without regard to the physical location of the users. Packets received on a port are forwarded only to ports that belong to the same VLAN as the receiving port. Network devices in different VLANs cannot communicate with one another without a Layer 3 device to route traffic between the VLANs.

VLAN partitions provide hard firewalls for traffic in the VLAN, and each VLAN has its own MAC address table. A VLAN comes into existence when a local port is configured to be associated with the VLAN, when the VLAN Trunking Protocol (VTP) learns of its existence from a neighbor on a trunk, or when a user creates a VLAN. VLANs can be formed with ports across the stack.

To configure VLANs, use the **vlan *vlan-id*** global configuration command to enter VLAN configuration mode. The VLAN configurations for normal-range VLANs (VLAN IDs 1 to 1005) are saved in the VLAN database. If VTP is version 1 or 2, to configure extended-range VLANs (VLAN IDs 1006 to 4094), you must first set VTP mode to transparent. Extended-range VLANs created in transparent mode are not added to the VLAN

database but are saved in the switch running configuration. With VTP version 3, you can create extended-range VLANs in client or server mode. These VLANs are saved in the VLAN database.

In a switch stack, the VLAN database is downloaded to all switches in a stack, and all switches in the stack build the same VLAN database. The running configuration and the saved configuration are the same for all switches in a stack.

Add ports to a VLAN by using the **switchport** interface configuration commands:

- Identify the interface.
- For a trunk port, set trunk characteristics, and, if desired, define the VLANs to which it can belong.
- For an access port, set and define the VLAN to which it belongs.

## Switch Ports

Switch ports are Layer 2-only interfaces associated with a physical port. Switch ports belong to one or more VLANs. A switch port can be an access port or a trunk port. You can configure a port as an access port or trunk port or let the Dynamic Trunking Protocol (DTP) operate on a per-port basis to set the switchport mode by negotiating with the port on the other end of the link. switch ports are used for managing the physical interface and associated Layer 2 protocols and do not handle routing or bridging.

Configure switch ports by using the **switchport** interface configuration commands.

### Access Ports

An access port belongs to and carries the traffic of only one VLAN (unless it is configured as a voice VLAN port). Traffic is received and sent in native formats with no VLAN tagging. Traffic arriving on an access port is assumed to belong to the VLAN assigned to the port. If an access port receives a tagged packet (Inter-Switch Link [ISL] or IEEE 802.1Q tagged), the packet is dropped, and the source address is not learned.

The types of access ports supported are:

- Static access ports are manually assigned to a VLAN (or through a RADIUS server for use with IEEE 802.1x).
- VLAN membership of dynamic access ports is learned through incoming packets. By default, a dynamic access port is not a member of any VLAN, and forwarding to and from the port is enabled only when the VLAN membership of the port is discovered. Dynamic access ports on the switch are assigned to a VLAN by a VLAN Membership Policy Server (VMPS). The VMPS can be a Catalyst 6500 series switch; the switch cannot be a VMPS server.

You can also configure an access port with an attached Cisco IP Phone to use one VLAN for voice traffic and another VLAN for data traffic from a device attached to the phone.

### Trunk Ports

A trunk port carries the traffic of multiple VLANs and by default is a member of all VLANs in the VLAN database.

The switch supports only IEEE 802.1Q trunk ports. An IEEE 802.1Q trunk port supports simultaneous tagged and untagged traffic. An IEEE 802.1Q trunk port is assigned a default port VLAN ID (PVID), and all untagged traffic travels on the port default PVID. All untagged traffic and tagged traffic with a NULL VLAN ID are assumed to belong to the port default PVID. A packet with a VLAN ID equal to the outgoing port default PVID is sent untagged. All other traffic is sent with a VLAN tag.

Although by default, a trunk port is a member of every VLAN known to the VTP, you can limit VLAN membership by configuring an allowed list of VLANs for each trunk port. The list of allowed VLANs does not affect any other port but the associated trunk port. By default, all possible VLANs (VLAN ID 1 to 4094) are in the allowed list. A trunk port can become a member of a VLAN only if VTP knows of the VLAN and if the VLAN is in the enabled state. If VTP learns of a new, enabled VLAN and the VLAN is in the allowed list for a trunk port, the trunk port automatically becomes a member of that VLAN and traffic is forwarded to and from the trunk port for that VLAN. If VTP learns of a new, enabled VLAN that is not in the allowed list for a trunk port, the port does not become a member of the VLAN, and no traffic for the VLAN is forwarded to or from the port.

## Switch Virtual Interfaces

A switch virtual interface (SVI) represents a VLAN of switch ports as one interface to the routing or bridging function in the system. You can associate only one SVI with a VLAN. You configure an SVI for a VLAN only to route between VLANs or to provide IP host connectivity to the switch. By default, an SVI is created for the default VLAN (VLAN 1) to permit remote switch administration. Additional SVIs must be explicitly configured.



---

**Note** You cannot delete interface VLAN 1.

---

SVIs provide IP host connectivity only to the system. SVIs are created the first time that you enter the **vlan** interface configuration command for a VLAN interface. The VLAN corresponds to the VLAN tag associated with data frames on an ISL or IEEE 802.1Q encapsulated trunk or the VLAN ID configured for an access port. Configure a VLAN interface for each VLAN for which you want to route traffic, and assign it an IP address.

Although the switch stack or switch supports a total of 1005 VLANs and SVIs, the interrelationship between the number of SVIs and routed ports and the number of other features being configured might impact CPU performance because of hardware limitations.

When you create an SVI, it does not become active until it is associated with a physical port.

### SVI Autostate Exclude

The line state of an SVI with multiple ports on a VLAN is in the *up* state when it meets these conditions:

- The VLAN exists and is active in the VLAN database on the switch
- The VLAN interface exists and is not administratively down.
- At least one Layer 2 (access or trunk) port exists, has a link in the *up* state on this VLAN, and is in the spanning-tree forwarding state on the VLAN.



---

**Note** The protocol link state for VLAN interfaces come up when the first switchport belonging to the corresponding VLAN link comes up and is in STP forwarding state.

---

The default action, when a VLAN has multiple ports, is that the SVI goes down when all ports in the VLAN go down. You can use the SVI autostate exclude feature to configure a port so that it is not included in the SVI line-state up-or-down calculation. For example, if the only active port on the VLAN is a monitoring port,

you might configure `autostate exclude` on that port so that the VLAN goes down when all other ports go down. When enabled on a port, **autostate exclude** applies to all VLANs that are enabled on that port.

The VLAN interface is brought up when one Layer 2 port in the VLAN has had time to converge (transition from STP listening-learning state to forwarding state). This prevents features such as routing protocols from using the VLAN interface as if it were fully operational and minimizes other problems.

## EtherChannel Port Groups

EtherChannel port groups treat multiple switch ports as one switch port. These port groups act as a single logical port for high-bandwidth connections between switches or between switches and servers. An EtherChannel balances the traffic load across the links in the channel. If a link within the EtherChannel fails, traffic previously carried over the failed link changes to the remaining links. You can group multiple trunk ports into one logical trunk port or multiple access ports into one logical access port. Most protocols operate over either single ports or aggregated switch ports and do not recognize the physical ports within the port group. Exceptions are the DTP, the Cisco Discovery Protocol (CDP), and the Port Aggregation Protocol (PAgP), which operate only on physical ports.

When you configure an EtherChannel, you create a port-channel logical interface and assign an interface to the EtherChannel. For Layer 2 interfaces, use the **channel-group** interface configuration command to dynamically create the port-channel logical interface. This command binds the physical and logical ports together.

## Power over Ethernet Ports

A PoE-capable switch port automatically supplies power to one of these connected devices if the switch senses that there is no power on the circuit:

- a Cisco pre-standard powered device (such as a Cisco IP Phone or a Cisco Aironet Access Point)
- an IEEE 802.3af-compliant powered device

A powered device can receive redundant power when it is connected to a PoE switch port and to an AC power source. The device does not receive redundant power when it is only connected to the PoE port.

## Using the Switch USB Ports

The switch has three USB ports on the front panel — a USB mini-Type B console port and two USB Type A ports.

### USB Mini-Type B Console Port

The switch has the following console ports:

- USB mini-Type B console connection
- RJ-45 console port

Console output appears on devices connected to both ports, but console input is active on only one port at a time. By default, the USB connector takes precedence over the RJ-45 connector.



**Note** Windows PCs require a driver for the USB port. See the hardware installation guide for driver installation instructions.

Use the supplied USB Type A-to-USB mini-Type B cable to connect a PC or other device to the switch. The connected device must include a terminal emulation application. When the switch detects a valid USB connection to a powered-on device that supports host functionality (such as a PC), input from the RJ-45 console is immediately disabled, and input from the USB console is enabled. Removing the USB connection immediately reenables input from the RJ-45 console connection. An LED on the switch shows which console connection is in use.

## Console Port Change Logs

At software startup, a log shows whether the USB or the RJ-45 console is active. Each switch in a stack issues this log. Every switch always first displays the RJ-45 media type.

In the sample output, Switch 1 has a connected USB console cable. Because the bootloader did not change to the USB console, the first log from Switch 1 shows the RJ-45 console. A short time later, the console changes and the USB console log appears. Switch 2 and Switch 3 have connected RJ-45 console cables.

```
switch-stack-1
*Mar 1 00:01:00.171: %USB_CONSOLE-6-MEDIA_RJ45: Console media-type is RJ45.
*Mar 1 00:01:00.431: %USB_CONSOLE-6-MEDIA_USB: Console media-type is USB.
```

```
switch-stack-2
*Mar 1 00:01:09.835: %USB_CONSOLE-6-MEDIA_RJ45: Console media-type is RJ45.
```

```
switch-stack-3
*Mar 1 00:01:10.523: %USB_CONSOLE-6-MEDIA_RJ45: Console media-type is RJ45.
```

When the USB cable is removed or the PC de-activates the USB connection, the hardware automatically changes to the RJ-45 console interface:

```
switch-stack-1
Mar 1 00:20:48.635: %USB_CONSOLE-6-MEDIA_RJ45: Console media-type is RJ45.
```

You can configure the console type to always be RJ-45, and you can configure an inactivity timeout for the USB connector.

## USB Type A Ports

The USB Type A ports provide access to external USB flash devices, also known as thumb drives or USB keys. The switch supports Cisco 64 MB, 256 MB, 512 MB, 1 GB, 4 GB, and 8 GB flash drives. You can use standard Cisco IOS command-line interface (CLI) commands to read, write, erase, and copy to or from the flash device. You can also configure the switch to boot from the USB flash drive.

For information about configuring the switch to boot from a USB flash drive, refer to the *Catalyst 2960-X Switch System Management Configuration Guide*.

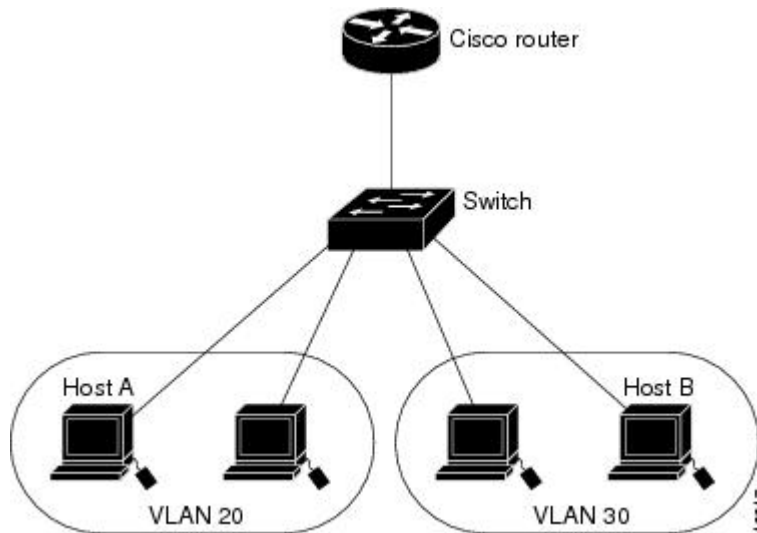
For information about reading, writing, erasing, and copying files to or from the flash device, refer to the *Catalyst 2960-X Switch Managing Cisco IOS Image Files Configuration Guide*.

## Interface Connections

Devices within a single VLAN can communicate directly through any switch. Ports in different VLANs cannot exchange data without going through a routing device.

In the following configuration example, when Host A in VLAN 20 sends data to Host B in VLAN 30, the data must go from Host A to the device, to the router, back to the device, and then to Host B.

**Figure 1: Connecting VLANs with the Switch**



With a standard Layer 2 switch, ports in different VLANs have to exchange information through a router.



**Note** The Catalyst 3560-CX and 2960-CX switches do not support stacking. Ignore all references to stacking throughout this book.

## Interface Configuration Mode

The switch supports these interface types:

- Physical ports—switch ports and routed ports
- VLANs—switch virtual interfaces
- Port channels—EtherChannel interfaces

You can also configure a range of interfaces.

To configure a physical interface (port), specify the interface type, module number, and switch port number, and enter interface configuration mode.

- Type—Gigabit Ethernet (`gigabitethernet` or `gi`) for 10/100/1000 Mb/s Ethernet ports, or small form-factor pluggable (SFP) module Gigabit Ethernet interfaces (`gigabitethernet` or `gi`).
- Stack member number—The number that identifies the switch within the stack. The range is 1 to 8 for a stack of Catalyst 2960-X switches, and 1 to 4 for a mixed stack of Catalyst 2960-X and Catalyst 2960-S

switches. The switch number is assigned the first time the switch initializes. The default switch number, before it is integrated into a switch stack, is 1. When a switch has been assigned a stack member number, it keeps that number until another is assigned to it.

You can use the switch port LEDs in Stack mode to identify the stack member number of a switch.

- Module number—The module or slot number on the switch (always 0).
- Port number—The interface number on the switch. The 10/100/1000 port numbers always begin at 1, starting with the far left port when facing the front of the switch, for example, `gigabitethernet1/0/1` or `gigabitethernet1/0/8`. For a switch with 10/100/1000 ports and SFP module ports, SFP module ports are numbered consecutively following the 10/100/1000 ports.

You can identify physical interfaces by physically checking the interface location on the switch. You can also use the **show** privileged EXEC commands to display information about a specific interface or all the interfaces on the switch. The remainder of this chapter primarily provides physical interface configuration procedures.

These are examples of how to identify interfaces on a stacking-capable switch:

- To configure 10/100/1000 port 4 on a standalone switch, enter this command:

```
Switch(config)# interface gigabitethernet1/0/4
```

- To configure 10/100/1000 port 4 on stack member 3, enter this command:

```
Switch(config)# interface gigabitethernet3/0/4
```

## Default Ethernet Interface Configuration

This table shows the Ethernet interface default configuration, including some features that apply only to Layer 2 interfaces.

**Table 1: Default Layer 2 Ethernet Interface Configuration**

Feature	Default Setting
Operating mode	Layer 2 or switching mode ( <b>switchport</b> command).
Allowed VLAN range	VLANs 1– 4094.
Default VLAN (for access ports)	VLAN 1.
Native VLAN (for IEEE 802.1Q trunks)	VLAN 1.
802.1p priority-tagged traffic	Drop all packets tagged with VLAN 0.
VLAN trunking	Switchport mode dynamic auto (supports DTP).
Port enable state	All ports are enabled.
Port description	None defined.
Speed	Autonegotiate. (Not supported on the 10-Gigabit interfaces.)

Feature	Default Setting
Duplex mode	Autonegotiate. (Not supported on the 10-Gigabit interfaces.)
Flow control	Flow control is set to <b>receive: off</b> . It is always off for sent packets.
EtherChannel (PAgP)	Disabled on all Ethernet ports.
Port blocking (unknown multicast and unknown unicast traffic)	Disabled (not blocked).
Broadcast, multicast, and unicast storm control	Disabled.
Protected port	Disabled.
Port security	Disabled.
Port Fast	Disabled.
Auto-MDIX	Enabled.  <b>Note</b> The switch might not support a pre-standard powered device—such as Cisco IP phones and access points that do not fully support IEEE 802.3af—if that powered device is connected to the switch through a crossover cable. This is regardless of whether auto-MIDX is enabled on the switch port.
Power over Ethernet (PoE)	Enabled (auto).
Keepalive messages	Disabled on SFP module ports; enabled on all other ports.

## Interface Speed and Duplex Mode

Ethernet interfaces on the switch operate at 10, 100, or 1000 Mb/s and in either full- or half-duplex mode. In full-duplex mode, two stations can send and receive traffic at the same time. Normally, 10-Mb/s ports operate in half-duplex mode, which means that stations can either receive or send traffic.

Switch models include Gigabit Ethernet (10/100/1000-Mb/s) ports and small form-factor pluggable (SFP) module slots supporting SFP modules.

## Speed and Duplex Configuration Guidelines

When configuring an interface speed and duplex mode, note these guidelines:

- Do not disable Auto-Negotiation on PoE switches.
- Gigabit Ethernet (10/100/1000-Mb/s) ports support all speed options and all duplex options (auto, half, and full). However, Gigabit Ethernet ports operating at 1000 Mb/s do not support half-duplex mode.



- For SFP module ports, the speed and duplex CLI options change depending on the SFP module type:
  - The 1000BASE-*x* (where *x* is -BX, -CWDM, -LX, -SX, and -ZX) SFP module ports support the **nonegotiate** keyword in the **speed** interface configuration command. Duplex options are not supported.
  - The 1000BASE-T SFP module ports support the same speed and duplex options as the 10/100/1000-Mb/s ports.
- If both ends of the line support autonegotiation, we highly recommend the default setting of **auto** negotiation.
- If one interface supports autonegotiation and the other end does not, configure duplex and speed on both interfaces; do not use the **auto** setting on the supported side.
- When STP is enabled and a port is reconfigured, the switch can take up to 30 seconds to check for loops. The port LED is amber while STP reconfigures.
- As best practice, we suggest configuring the speed and duplex options on a link to auto or to fixed on both the ends. If one side of the link is configured to auto and the other side is configured to fixed, the link will not be up and this is expected.



---

**Caution** Changing the interface speed and duplex mode configuration might shut down and re-enable the interface during the reconfiguration.

---

## IEEE 802.3x Flow Control

Flow control enables connected Ethernet ports to control traffic rates during congestion by allowing congested nodes to pause link operation at the other end. If one port experiences congestion and cannot receive any more traffic, it notifies the other port by sending a pause frame to stop sending until the condition clears. Upon receipt of a pause frame, the sending device stops sending any data packets, which prevents any loss of data packets during the congestion period.



---

**Note** The switch ports can receive, but not send, pause frames.

---

You use the **flowcontrol** interface configuration command to set the interface's ability to **receive** pause frames to **on**, **off**, or **desired**. The default state is **off**.

When set to **desired**, an interface can operate with an attached device that is required to send flow-control packets or with an attached device that is not required to but can send flow-control packets.

These rules apply to flow control settings on the device:

- **receive on** (or **desired**): The port cannot send pause frames but can operate with an attached device that is required to or can send pause frames; the port can receive pause frames.
- **receive off**: Flow control does not operate in either direction. In case of congestion, no indication is given to the link partner, and no pause frames are sent or received by either device.



**Note** For details on the command settings and the resulting flow control resolution on local and remote ports, see the **flowcontrol** interface configuration command in the command reference for this release.

# How to Configure Interface Characteristics

## Configuring Interfaces

These general instructions apply to all interface configuration processes.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> <pre>Switch&gt; enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> <pre>Switch# configure terminal</pre>	Enters global configuration mode.
<b>Step 3</b>	<b>interface</b> <b>Example:</b> <pre>Switch(config)# interface gigabitethernet1/0/1 Switch(config-if)#</pre>	Identifies the interface type, the switch number (only on stacking-capable switches), and the number of the connector. <p><b>Note</b> You do not need to add a space between the interface type and the interface number. For example, in the preceding line, you can specify either <b>gigabitethernet 1/0/1</b>, <b>gigabitethernet1/0/1</b>, <b>gi 1/0/1</b>, or <b>gi1/0/1</b>.</p>
<b>Step 4</b>	Follow each <b>interface</b> command with the interface configuration commands that the interface requires.	Defines the protocols and applications that will run on the interface. The commands are collected and applied to the interface when you enter another interface command or enter <b>end</b> to return to privileged EXEC mode.
<b>Step 5</b>	<b>interface range</b> or <b>interface range macro</b>	(Optional) Configures a range of interfaces. <p><b>Note</b> Interfaces configured in a range must be the same type and must be configured with the same feature options.</p>

	Command or Action	Purpose
Step 6	<code>show interfaces</code>	Displays a list of all interfaces on or configured for the switch. A report is provided for each interface that the device supports or for the specified interface.

## Adding a Description for an Interface

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `interface interface-id`
4. `description string`
5. `end`
6. `show interfaces interface-id description`
7. `copy running-config startup-config`

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<p><code>enable</code></p> <p><b>Example:</b></p> <pre>Switch&gt; enable</pre>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<p><code>configure terminal</code></p> <p><b>Example:</b></p> <pre>Switch# configure terminal</pre>	<p>Enters global configuration mode.</p>
Step 3	<p><code>interface interface-id</code></p> <p><b>Example:</b></p> <pre>Switch(config)# interface gigabitethernet1/0/2</pre>	<p>Specifies the interface for which you are adding a description, and enter interface configuration mode.</p>
Step 4	<p><code>description string</code></p> <p><b>Example:</b></p> <pre>Switch(config-if)# description Connects to Marketing</pre>	<p>Adds a description (up to 240 characters) for an interface.</p>
Step 5	<p><code>end</code></p> <p><b>Example:</b></p>	<p>Returns to privileged EXEC mode.</p>

	Command or Action	Purpose
	<code>Switch(config-if)# end</code>	
<b>Step 6</b>	<code>show interfaces interface-id description</code>	Verifies your entry.
<b>Step 7</b>	<b>copy running-config startup-config</b> <b>Example:</b> <code>Switch# copy running-config startup-config</code>	(Optional) Saves your entries in the configuration file.

## Configuring a Range of Interfaces

To configure multiple interfaces with the same configuration parameters, use the **interface range** global configuration command. When you enter the interface-range configuration mode, all command parameters that you enter are attributed to all interfaces within that range until you exit this mode.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface range** {*port-range* | **macro** *macro\_name*}
4. **end**
5. **show interfaces** [*interface-id*]
6. **copy running-config startup-config**

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> <code>Switch&gt; enable</code>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> <code>Switch# configure terminal</code>	Enters global configuration mode.
<b>Step 3</b>	<b>interface range</b> { <i>port-range</i>   <b>macro</b> <i>macro_name</i> } <b>Example:</b> <code>Switch(config)# interface range macro</code>	Specifies the range of interfaces (VLANs or physical ports) to be configured, and enter interface-range configuration mode. <ul style="list-style-type: none"> <li>• You can use the <b>interface range</b> command to configure up to five port ranges or a previously defined macro.</li> </ul>

	Command or Action	Purpose
		<ul style="list-style-type: none"> <li>The <b>macro</b> variable is explained in the <a href="#">Configuring and Using Interface Range Macros, on page 13</a>.</li> <li>In a comma-separated <i>port-range</i>, you must enter the interface type for each entry and enter spaces before and after the comma.</li> <li>In a hyphen-separated <i>port-range</i>, you do not need to re-enter the interface type, but you must enter a space before the hyphen.</li> </ul> <p><b>Note</b> Use the normal configuration commands to apply the configuration parameters to all interfaces in the range. Each command is executed as it is entered.</p>
<b>Step 4</b>	<b>end</b> <b>Example:</b> <pre>Switch(config)# end</pre>	Returns to privileged EXEC mode.
<b>Step 5</b>	<b>show interfaces</b> [ <i>interface-id</i> ] <b>Example:</b> <pre>Switch# show interfaces</pre>	Verifies the configuration of the interfaces in the range.
<b>Step 6</b>	<b>copy running-config startup-config</b> <b>Example:</b> <pre>Switch# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

## Configuring and Using Interface Range Macros

You can create an interface range macro to automatically select a range of interfaces for configuration. Before you can use the **macro** keyword in the **interface range macro** global configuration command string, you must use the **define interface-range** global configuration command to define the macro.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **define interface-range** *macro\_name interface-range*
4. **interface range macro** *macro\_name*
5. **end**
6. **show running-config | include define**

## 7. copy running-config startup-config

## DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> <pre>Switch&gt; enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> <pre>Switch# configure terminal</pre>	Enters global configuration mode.
<b>Step 3</b>	<b>define interface-range <i>macro_name</i> <i>interface-range</i></b> <b>Example:</b> <pre>Switch(config)# define interface-range enet_list gigabitethernet1/0/1 - 2</pre>	Defines the interface-range macro, and save it in NVRAM. <ul style="list-style-type: none"> <li>• The <i>macro_name</i> is a 32-character maximum character string.</li> <li>• A macro can contain up to five comma-separated interface ranges.</li> <li>• Each <i>interface-range</i> must consist of the same port type.</li> </ul> <p><b>Note</b> Before you can use the <b>macro</b> keyword in the <b>interface range macro</b> global configuration command string, you must use the <b>define interface-range</b> global configuration command to define the macro.</p>
<b>Step 4</b>	<b>interface range macro <i>macro_name</i></b> <b>Example:</b> <pre>Switch(config)# interface range macro enet_list</pre>	Selects the interface range to be configured using the values saved in the interface-range macro called <i>macro_name</i> .  You can now use the normal configuration commands to apply the configuration to all interfaces in the defined macro.
<b>Step 5</b>	<b>end</b> <b>Example:</b> <pre>Switch(config)# end</pre>	Returns to privileged EXEC mode.
<b>Step 6</b>	<b>show running-config   include define</b> <b>Example:</b> <pre>Switch# show running-config   include define</pre>	Shows the defined interface range macro configuration.

	Command or Action	Purpose
Step 7	<b>copy running-config startup-config</b> <b>Example:</b> <pre>Switch# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

## Configuring Ethernet Interfaces

### Setting the Interface Speed and Duplex Parameters

#### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *interface-id*
4. **speed** {10 | 100 | 1000 | 2500 | 5000 | 10000 | auto [10 | 100 | 1000 | 2500 | 5000 | 10000] | nonegotiate}
5. **duplex** {auto | full | half}
6. **end**
7. **show interfaces** *interface-id*
8. **copy running-config startup-config**
9. **copy running-config startup-config**

#### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b> <b>Example:</b> <pre>Switch&gt; enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b> <b>Example:</b> <pre>Switch# configure terminal</pre>	Enters global configuration mode.
Step 3	<b>interface</b> <i>interface-id</i> <b>Example:</b> <pre>Switch(config)# interface gigabitethernet1/0/3</pre>	Specifies the physical interface to be configured, and enter interface configuration mode.
Step 4	<b>speed</b> {10   100   1000   2500   5000   10000   auto [10   100   1000   2500   5000   10000]   nonegotiate}	Enter the appropriate speed parameter for the interface:

	Command or Action	Purpose
	<p><b>Example:</b></p> <pre>Switch(config-if)# speed 10</pre>	<ul style="list-style-type: none"> <li>Enter <b>10, 100, 1000 2500, 5000, or 10000</b> to set a specific speed for the interface.</li> <li>Enter <b>auto</b> to enable the interface to autonegotiate speed with the connected device. If you specify a speed and also set the <b>auto</b> keyword, the port autonegotiates only at the specified speeds.</li> <li>The <b>nonegotiate</b> keyword is available only for SFP module ports. SFP module ports operate only at 1000 Mb/s but can be configured to not negotiate if connected to a device that does not support autonegotiation.</li> </ul>
<b>Step 5</b>	<p><b>duplex {auto   full   half}</b></p> <p><b>Example:</b></p> <pre>Switch(config-if)# duplex half</pre>	<p>This command is not available on a 10-Gigabit Ethernet interface.</p> <p>Enter the duplex parameter for the interface.</p> <p>Enable half-duplex mode (for interfaces operating only at 10 or 100 Mb/s). You cannot configure half-duplex mode for interfaces operating at 1000 Mb/s.</p> <p>You can configure the duplex setting when the speed is set to <b>auto</b>.</p>
<b>Step 6</b>	<p><b>end</b></p> <p><b>Example:</b></p> <pre>Switch(config-if)# end</pre>	<p>Returns to privileged EXEC mode.</p>
<b>Step 7</b>	<p><b>show interfaces <i>interface-id</i></b></p> <p><b>Example:</b></p> <pre>Switch# show interfaces gigabitethernet1/0/3</pre>	<p>Displays the interface speed and duplex mode configuration.</p>
<b>Step 8</b>	<p><b>copy running-config startup-config</b></p> <p><b>Example:</b></p> <pre>Switch# copy running-config startup-config</pre>	<p>(Optional) Saves your entries in the configuration file.</p>
<b>Step 9</b>	<p><b>copy running-config startup-config</b></p> <p><b>Example:</b></p> <pre>Switch# copy running-config startup-config</pre>	<p>(Optional) Saves your entries in the configuration file.</p>



## Configuring IEEE 802.3x Flow Control

### SUMMARY STEPS

1. **configure terminal**
2. **interface** *interface-id*
3. **flowcontrol** {receive} {on | off | desired}
4. **end**
5. **show interfaces** *interface-id*
6. **copy running-config startup-config**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>configure terminal</b> <b>Example:</b> Switch# <b>configure terminal</b>	Enters global configuration mode
Step 2	<b>interface</b> <i>interface-id</i> <b>Example:</b> Switch(config)# <b>interface gigabitethernet1/0/1</b>	Specifies the physical interface to be configured, and enter interface configuration mode.
Step 3	<b>flowcontrol</b> {receive} {on   off   desired} <b>Example:</b> Switch(config-if)# <b>flowcontrol receive on</b>	Configures the flow control mode for the port.
Step 4	<b>end</b> <b>Example:</b> Switch(config-if)# <b>end</b>	Returns to privileged EXEC mode.
Step 5	<b>show interfaces</b> <i>interface-id</i> <b>Example:</b> Switch# <b>show interfaces gigabitethernet1/0/1</b>	Verifies the interface flow control settings.
Step 6	<b>copy running-config startup-config</b> <b>Example:</b> Switch# <b>copy running-config startup-config</b>	(Optional) Saves your entries in the configuration file.

## Configuring SVI Autostate Exclude

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface *interface-id***
4. **switchport autostate exclude**
5. **end**
6. **show running config interface *interface-id***
7. **copy running-config startup-config**

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> <pre>Switch&gt; enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> <pre>Switch# configure terminal</pre>	Enters global configuration mode.
<b>Step 3</b>	<b>interface <i>interface-id</i></b> <b>Example:</b> <pre>Switch(config)# interface gigabitethernet1/0/2</pre>	Specifies a Layer 2 interface (physical port or port channel), and enter interface configuration mode.
<b>Step 4</b>	<b>switchport autostate exclude</b> <b>Example:</b> <pre>Switch(config-if)# switchport autostate exclude</pre>	Excludes the access or trunk port when defining the status of an SVI line state (up or down)
<b>Step 5</b>	<b>end</b> <b>Example:</b> <pre>Switch(config-if)# end</pre>	Returns to privileged EXEC mode.
<b>Step 6</b>	<b>show running config interface <i>interface-id</i></b>	(Optional) Shows the running configuration. Verifies the configuration.

	Command or Action	Purpose
Step 7	<b>copy running-config startup-config</b> <b>Example:</b> <pre>Switch# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

## Shutting Down and Restarting the Interface

Shutting down an interface disables all functions on the specified interface and marks the interface as unavailable on all monitoring command displays. This information is communicated to other network servers through all dynamic routing protocols. The interface is not mentioned in any routing updates.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface {vlan *vlan-id*} | {gigabitethernet *interface-id*} | {port-channel *port-channel-number*}**
4. **shutdown**
5. **no shutdown**
6. **end**
7. **show running-config**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b> <b>Example:</b> <pre>Switch&gt; enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b> <b>Example:</b> <pre>Switch# configure terminal</pre>	Enters global configuration mode.
Step 3	<b>interface {vlan <i>vlan-id</i>}   {gigabitethernet <i>interface-id</i>}   {port-channel <i>port-channel-number</i>}</b> <b>Example:</b> <pre>Switch(config)# interface gigabitethernet1/0/2</pre>	Selects the interface to be configured.
Step 4	<b>shutdown</b> <b>Example:</b>	Shuts down an interface.

	Command or Action	Purpose
	<code>Switch(config-if) # shutdown</code>	
<b>Step 5</b>	<b>no shutdown</b> <b>Example:</b> <code>Switch(config-if) # no shutdown</code>	Restarts an interface.
<b>Step 6</b>	<b>end</b> <b>Example:</b> <code>Switch(config-if) # end</code>	Returns to privileged EXEC mode.
<b>Step 7</b>	<b>show running-config</b> <b>Example:</b> <code>Switch# show running-config</code>	Verifies your entries.

## Configuring the Console Media Type

Follow these steps to set the console media type to RJ-45. If you configure the console as RJ-45, USB console operation is disabled, and input comes only through the RJ-45 connector.

This configuration applies to all switches in a stack.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **line console 0**
4. **media-type rj45**
5. **end**
6. **copy running-config startup-config**

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> <code>Switch&gt; enable</code>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>

	Command or Action	Purpose
Step 2	<b>configure terminal</b> <b>Example:</b> <pre>Switch# configure terminal</pre>	Enters global configuration mode.
Step 3	<b>line console 0</b> <b>Example:</b> <pre>Switch(config)# line console 0</pre>	Configures the console and enters line configuration mode.
Step 4	<b>media-type rj45</b> <b>Example:</b> <pre>Switch(config-line)# media-type rj45</pre>	Configures the console media type to be only RJ-45 port. If you do not enter this command and both types are connected, the USB port is used by default.
Step 5	<b>end</b> <b>Example:</b> <pre>Switch(config)# end</pre>	Returns to privileged EXEC mode.
Step 6	<b>copy running-config startup-config</b> <b>Example:</b> <pre>Switch# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

## Configuring the USB Inactivity Timeout

The configurable inactivity timeout reactivates the RJ-45 console port if the USB console port is activated but no input activity occurs on it for a specified time period. When the USB console port is deactivated due to a timeout, you can restore its operation by disconnecting and reconnecting the USB cable.



**Note** The configured inactivity timeout applies to all switches in a stack. However, a timeout on one switch does not cause a timeout on other switches in the stack.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **line console 0**
4. **usb-inactivity-timeout** *timeout-minutes*

## 5. copy running-config startup-config

### DETAILED STEPS

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> Switch> <b>enable</b>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> Switch# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 3</b>	<b>line console 0</b> <b>Example:</b> Switch(config)# <b>line console 0</b>	Configures the console and enters line configuration mode.
<b>Step 4</b>	<b>usb-inactivity-timeout</b> <i>timeout-minutes</i> <b>Example:</b> Switch(config-line)# <b>usb-inactivity-timeout 30</b>	Specify an inactivity timeout for the console port. The range is 1 to 240 minutes. The default is to have no timeout configured.
<b>Step 5</b>	<b>copy running-config startup-config</b> <b>Example:</b> Switch# <b>copy running-config startup-config</b>	(Optional) Saves your entries in the configuration file.

# Monitoring Interface Characteristics

## Monitoring Interface Status

Commands entered at the privileged EXEC prompt display information about the interface, including the versions of the software and the hardware, the configuration, and statistics about the interfaces.

Table 2: Show Commands for Interfaces

Command	Purpose
<b>show interfaces</b> <i>interface-id</i> <b>status</b> [err-disabled]	Displays interface status or a list of interfaces in the error-disabled state.
<b>show interfaces</b> [ <i>interface-id</i> ] <b>switchport</b>	Displays administrative and operational status of switching (nonrouting) ports. You can use this command to find out if a port is in routing or in switching mode.
<b>show interfaces</b> [ <i>interface-id</i> ] <b>description</b>	Displays the description configured on an interface or all interfaces and the interface status.
<b>show ip interface</b> [ <i>interface-id</i> ]	Displays the usability status of all interfaces configured for IP routing or the specified interface.
<b>show interface</b> [ <i>interface-id</i> ] <b>stats</b>	Displays the input and output packets by the switching path for the interface.
<b>show interfaces</b> <i>interface-id</i>	(Optional) Displays speed and duplex on the interface.
<b>show interfaces transceiver dom-supported-list</b>	(Optional) Displays Digital Optical Monitoring (DOM) status on the connect SFP modules.
<b>show interfaces transceiver properties</b>	(Optional) Displays temperature, voltage, or amount of current on the interface.
<b>show interfaces</b> [ <i>interface-id</i> ] [{ <b>transceiver properties</b>   <b>detail</b> }] <i>module number</i>	Displays physical and operational status about an SFP module.
<b>show running-config interface</b> [ <i>interface-id</i> ]	Displays the running configuration in RAM for the interface.
<b>show version</b>	Displays the hardware configuration, software version, the names and sources of configuration files, and the boot images.
<b>show controllers ethernet-controller</b> <i>interface-id</i> <b>phy</b>	Displays the operational state of the auto-MDIX feature on the interface.

## Clearing and Resetting Interfaces and Counters

Table 3: Clear Commands for Interfaces

Command	Purpose
<b>clear counters</b> [ <i>interface-id</i> ]	Clears interface counters.
<b>clear interface</b> <i>interface-id</i>	Resets the hardware logic on an interface.
<b>clear line</b> [ <i>number</i>   <b>console 0</b>   <i>vty number</i> ]	Resets the hardware logic on an asynchronous serial line.



**Note** The **clear counters** privileged EXEC command does not clear counters retrieved by using Simple Network Management Protocol (SNMP), but only those seen with the **show interface** privileged EXEC command.

## Configuration Examples for Interface Characteristics

### Configuring a Range of Interfaces: Examples

This example shows how to use the **interface range** global configuration command to set the speed to 100 Mb/s on ports 1 to 4 on switch 1:

```
Switch# configure terminal
Switch(config)# interface range gigabitethernet1/0/1 - 4
Switch(config-if-range)# speed 100
```

This example shows how to use a comma to add different interface type strings to the range to enable Gigabit Ethernet ports 1 to 3 and 10-Gigabit Ethernet ports 1 and 2 to receive flow-control pause frames:

```
Switch# configure terminal
Switch(config)# interface range gigabitethernet1/0/1 - 3 , tengigabitethernet1/0/1 - 2
Switch(config-if-range)# flowcontrol receive on
```

If you enter multiple configuration commands while you are in interface-range mode, each command is executed as it is entered. The commands are not batched and executed after you exit interface-range mode. If you exit interface-range configuration mode while the commands are being executed, some commands might not be executed on all interfaces in the range. Wait until the command prompt reappears before exiting interface-range configuration mode.

### Configuring and Using Interface Range Macros: Examples

This example shows how to define an interface-range named *enet\_list* to include ports 1 and 2 on switch 1 and to verify the macro configuration:

```
Switch# configure terminal
Switch(config)# define interface-range enet_list gigabitethernet1/0/1 - 2
Switch(config)# end
Switch# show running-config | include define
define interface-range enet_list GigabitEthernet1/0/1 - 2
```

This example shows how to create a multiple-interface macro named *macro1*:

```
Switch# configure terminal
Switch(config)# define interface-range macro1 gigabitethernet1/0/1 - 2, gigabitethernet1/0/5
- 7, tengigabitethernet1/0/1 -2
Switch(config)# end
```

This example shows how to enter interface-range configuration mode for the interface-range macro *enet\_list*:



```
Switch# configure terminal
Switch(config)# interface range macro enet_list
Switch(config-if-range)#
```

This example shows how to delete the interface-range macro *enet\_list* and to verify that it was deleted.

```
Switch# configure terminal
Switch(config)# no define interface-range enet_list
Switch(config)# end
Switch# show run | include define
Switch#
```

## Setting Interface Speed and Duplex Mode: Example

This example shows how to set the interface speed to 100 Mb/s and the duplex mode to half on a 10/100/1000 Mb/s port:

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/0/3
Switch(config-if)# speed 10
Switch(config-if)# duplex half
```

This example shows how to set the interface speed to 100 Mb/s on a 10/100/1000 Mb/s port:

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# speed 100
```

## Configuring the Console Media Type: Example

This example disables the USB console media type and enables the RJ-45 console media type.

```
Switch# configure terminal
Switch(config)# line console 0
Switch(config-line)# media-type rj45
```

This configuration terminates any active USB console media type in the stack. A log shows that this termination has occurred. This example shows that the console on switch 1 reverted to RJ-45.

```
*Mar 1 00:25:36.860: %USB_CONSOLE-6-CONFIG_DISABLE: Console media-type USB disabled by
system configuration, media-type reverted to RJ45.
```

At this point no switches in the stack allow a USB console to have input. A log entry shows when a console cable is attached. If a USB console cable is connected to switch 2, it is prevented from providing input.

```
*Mar 1 00:34:27.498: %USB_CONSOLE-6-CONFIG_DISALLOW: Console media-type USB is disallowed
by system configuration, media-type remains RJ45. (switch-stk-2)
```

This example reverses the previous configuration and immediately activates any USB console that is connected.

```
Switch# configure terminal
```

```
Switch(config)# line console 0
Switch(config-line)# no media-type rj45
```

## Configuring the USB Inactivity Timeout: Example

This example configures the inactivity timeout to 30 minutes:

```
Switch# configure terminal
Switch(config)# line console 0
Switch(config-line)# usb-inactivity-timeout 30
```

To disable the configuration, use these commands:

```
Switch# configure terminal
Switch(config)# line console 0
Switch(config-line)# no usb-inactivity-timeout
```

If there is no (input) activity on a USB console port for the configured number of minutes, the inactivity timeout setting applies to the RJ-45 port, and a log shows this occurrence:

```
*Mar  1 00:47:25.625: %USB_CONSOLE-6-INACTIVITY_DISABLE: Console media-type USB disabled
due to inactivity, media-type reverted to RJ45.
```

At this point, the only way to reactivate the USB console port is to disconnect and reconnect the cable.

When the USB cable on the switch has been disconnected and reconnected, a log similar to this appears:

```
*Mar  1 00:48:28.640: %USB_CONSOLE-6-MEDIA_USB: Console media-type is USB.
```

## Additional References for the Interface Characteristics Feature

### Error Message Decoder

Description	Link
To help you research and resolve system error messages in this release, use the Error Message Decoder tool.	<a href="https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi">https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi</a>

### Standards and RFCs

Standard/RFC	Title
None	--

**MIBs**

MIB	MIBs Link
All the supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

**Technical Assistance**

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<a href="http://www.cisco.com/support">http://www.cisco.com/support</a>

## Feature History and Information for Configuring Interface Characteristics

Release	Modification
Cisco IOS Release 15.0(2)EX	This feature was introduced.

