



Configuring Interface Characteristics

- [Information About Interface Characteristics, on page 1](#)
- [How to Configure Interface Characteristics, on page 16](#)
- [Configuration Examples for Interface Characteristics, on page 31](#)

Information About Interface Characteristics

The following sections provide information about interface characteristics.

Interface Types

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

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.

VLANs provide access control for traffic, 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.

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

Add ports to a VLAN by using the **switchport** command in interface configuration mode.

- 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).

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 IEEE 802.1Q trunk port type is supported. 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.

Tunnel Ports

Tunnel ports are used in IEEE 802.1Q tunneling to segregate the traffic of customers in a service-provider network from other customers who are using the same VLAN number. You configure an asymmetric link from a tunnel port on a service-provider edge switch to an IEEE 802.1Q trunk port on the customer switch. Packets entering the tunnel port on the edge switch, already IEEE 802.1Q-tagged with the customer VLANs, are encapsulated with another layer of an IEEE 802.1Q tag (called the metro tag), containing a VLAN ID unique in the service-provider network, for each customer. The double-tagged packets go through the

service-provider network keeping the original customer VLANs separate from those of other customers. At the outbound interface, also a tunnel port, the metro tag is removed, and the original VLAN numbers from the customer network are retrieved.

Tunnel ports cannot be trunk ports or access ports and must belong to a VLAN unique to each customer.

Routed Ports

A routed port is a physical port that acts like a port on a router; it does not have to be connected to a router. A routed port is not associated with a particular VLAN, as is an access port. A routed port behaves like a regular router interface, except that it does not support VLAN subinterfaces. Routed ports can be configured with a Layer 3 routing protocol. A routed port is a Layer 3 interface only and does not support Layer 2 protocols, such as DTP and STP.

Configure routed ports by putting the interface into Layer 3 mode with the **no switchport** interface configuration command. Then assign an IP address to the port, enable routing, and assign routing protocol characteristics by using the **ip routing** and **router protocol** global configuration commands.



Note Entering a **no switchport** interface configuration command shuts down the interface and then re-enables it, which might generate messages on the device to which the interface is connected. When you put an interface that is in Layer 2 mode into Layer 3 mode, the previous configuration information related to the affected interface might be lost.



Note A port configured as a switchport does not support MAC address configuration. It does not support the **mac-address x.x.x** command.

The number of routed ports that you can configure is not limited by software. However, the interrelationship between this number and the number of other features being configured might impact CPU performance because of hardware limitations.

Switch Virtual Interfaces

A switch virtual interface (SVI) represents a VLAN of switch ports as one interface to the routing 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 device. By default, an SVI is created for the default VLAN (VLAN 1) to permit remote device 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.

You can also use the interface range command to configure existing VLAN SVIs within the range. The commands entered under the interface range command are applied to all existing VLAN SVIs within the

range. You can enter the command **interface range create vlan x - y** to create all VLANs in the specified range that do not already exist. When the VLAN interface is created, **interface range vlan id** can be used to configure the VLAN interface.

Although the device 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.

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 devices or between devices 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, group multiple access ports into one logical access port, group multiple tunnel ports into one logical tunnel port, or group multiple routed ports into one logical routed 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 3 interfaces, you manually create the logical interface by using the **interface port-channel** global configuration command. Then you manually assign an interface to the EtherChannel by using the **channel-group** interface configuration command. 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.

SKU Details

Table 1: Cisco IE3500 Series Switch SKU details

PID	Uplink Port			Downlink Port			PoE	FPGA
	Type	Ports	Interface Name	Type	Ports	Interface Name		
IE-3500-8T3S	SFP	3	Gigabit	Copper	8	Gigabit	No	No
IE-3500-8P3S			Ethernet			Ethernet	Yes	No
IE-3505-8T3S			1/1-3			1/4-11	No	Yes
IE-3505-8P3S							Yes	Yes
IE-3500-8U3X		3	TenGigbit				Yes	No
IE-3500-8T3X			Ethernet				(4PPoE)	
			1/1-3				No	No

PID	Uplink Port			Downlink Port			PoE	FPGA
	Type	Ports	Interface Name	Type	Ports	Interface Name		
IEM-3500-16P	Not Applicable			Copper	16	Gigabit Ethernet 2/1-16	Yes	Yes, if connected to IE3505 SKU.
IEM-3500-16T					16	Gigabit Ethernet 2/1-16	No	
IEM-3500-8P					8	Gigabit Ethernet 2/1-8	Yes	
IEM-3500-8T					8	Gigabit Ethernet 2/1-8	No	
IEM-3500-4MU					4	TwoGigabit Ethernet 2/1-4	Yes (4PPoE)	
IEM-3500-8S				SFP	8	Gigabit Ethernet 2/1-8	No	
IEM-3500-14T2S				Copper/SFP	14 Copper 2 SFP	Gigabit Ethernet 2/1-16		
IEM-3500-6T2S					6 Copper 2 SFP	Gigabit Ethernet 2/1-8		

Table 2: Cisco IE3500 Series Switch SKU details

PID	Uplink Port			Downlink Port			PoE	FPGA	
	Type	Ports	Interface Name	Type	Ports	Interface Name			
IE-3500-8T3S	SFP/	3	Gigabit Ethernet 1/1-3	Copper RJ45	8	Gigabit Ethernet 1/4-11	No	No	
IE-3500-8P3S	SFP+						Yes	No	
IE-3505-8T3S							No	Yes	
IE-3505-8P3S							Yes	Yes	
IE-3500-8U3X			TenGigbit Ethernet 1/1-3				Yes (4PPoE)	No	
IE-3500-8T3X							No	No	

PID	Uplink Port			Downlink Port			PoE	FPGA	
	Type	Ports	Interface Name	Type	Ports	Interface Name			
IE-3500H-8T	Copper RJ45	3	Gigabit Ethernet 1/1-3	Copper RJ45	5	Gigabit Ethernet 1/4-8	No	No	
IE-3500H-16T					13	Gigabit Ethernet 1/4-16			
IE-3505H-16T					13	Gigabit Ethernet 1/4-16			Yes
IE-3500H-24T					21	Gigabit Ethernet 1/4-24			No
IE-3500H-12FT4T		4	Gigabit Ethernet 1/1-4		12	FastEthernet 1/5-16	Yes		
IE-3500H-20FT4T					20	FastEthernet 1/5-24			
IE-3500H-14P2T		2	Gigabit Ethernet 1/1-2		14	Gigabit Ethernet 1/3-16			
IE-3500H-12P2MU2X	SFP/ SFP+	2	TenGigabit Ethernet 1/15-16		14	Gigabit Ethernet 1/1-12	Yes (4PPoE)		
						TwoGigabit Ethernet 1/13-14			

PID	Uplink Port			Downlink Port			PoE	FPGA
	Type	Ports	Interface Name	Type	Ports	Interface Name		
IEM-3500-16P	Not Applicable			Copper RJ45	16	Gigabit Ethernet 2/1-16	Yes	Yes, if connected to IE3505 SKU.
IEM-3500-16T					16	Gigabit Ethernet 2/1-16	No	
IEM-3500-8P					8	Gigabit Ethernet 2/1-8	Yes	
IEM-3500-8T					8	Gigabit Ethernet 2/1-8	No	
IEM-3500-4MU ¹					4	TwoGigabit Ethernet 2/1-4	Yes (4PPoE)	
IEM-3500-8S				SFP	8	Gigabit Ethernet 2/1-8	No	
IEM-3500-14T2S				Copper RJ45/ SFP	Copper RJ45: 14 SFP: 2	Gigabit Ethernet 2/1-16		
IEM-3500-6T2S					Copper RJ45: 6 SFP: 2	Gigabit Ethernet 2/1-8		

¹ HSR, PRP, and DLR are not supported on the IEM-3500-4MU= expansion module.

The uplink ports on the switches are fixed and correspond to SFP ports, meaning they require an SFP module, either copper or fiber, for operation.

PID decode details

Use the information below to decode the PID details.

Table 3: PID type

PID Type	Description
IE3500	Basic SKU
IE3505	Advance SKU
IE3500H	Basic SKU Heavy Duty
IE3505H	Advance SKU Heavy Duty
IEM	Expansion Module ²

² HSR is not supported with expansion modules.

Table 4: Port type

Port Type	Description
T	Copper
P	PoE Copper
U	4PPoE Copper
S	SFP (Copper/Fiber)
X	SFP 10G (Copper/Fiber)
MU	Mgig 4PPoE Copper
FT	FastEthernet

PID Syntax: <PID Type>-<number of Ports> <Port Type> <number of Ports> <Port Type>

For example, see the below PID IE3505-8T3S breakdown:

- IE3505: Indicates the PID type as an advance SKU.
- 8T3S indicates the following:
 - 8: The number of downlink ports.
 - T: The downlink port type as Copper.
 - 3: The number of uplink ports.
 - S: The uplink port type as SFP (Copper/Fiber).

Power over Ethernet

The Power over Ethernet (PoE) technology allows PoE (802.3af standard), PoE+ (802.3at), and Universal Power over Ethernet Plus (UPoE+, 802.3bt) ports to supply power for the operation of a device.

For more information, see the *Configuring PoE* section of this guide.

Switch Ports

This topic provides information about using the switch ports on Cisco IE3500 Series Switch.

Console Port

The device has the following console ports:

- Cisco IE3500H Heavy Duty Series Switch
 - M12 A-coded 5-pin connector console port.
- Cisco IE3500 Rugged Series Switch
 - RJ-45 console port
 - USB mini-Type C serial console
 - USB Type A 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 C cable to connect a PC or other device to the device. The connected device must include a terminal emulation application. When the device 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 device 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. Every device always first displays the RJ-45 media type.

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

```
switch
*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.
```

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

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 Port

The USB Type A port provides access to external USB flash devices, also known as thumb drives or USB keys. The port supports Cisco USB flash drives with capacities from 128 MB to 16 GB (USB devices with port densities of 128 MB, 256 MB, 1 GB, 4 GB, 8 GB, and 16 GB are supported). You can use standard Cisco IOS command-line interface (CLI) commands to read, write, erase, and copy to or from the flash device.

Disabling USB Ports

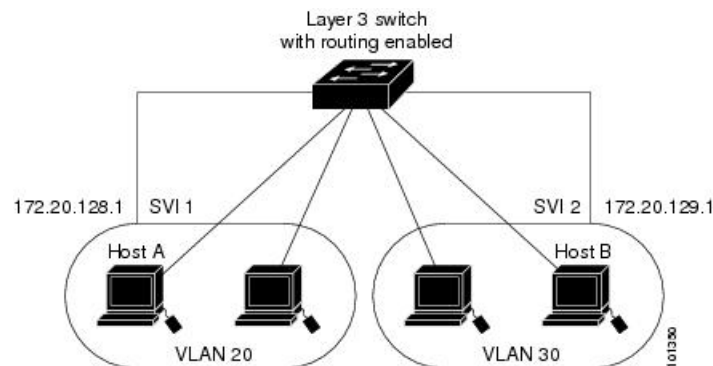
All the USB ports in a standalone device can be disabled using the **platform usb disable** command. Configuring this command disables all external media, including both USB flash and SD flash devices. To reenabling the USB ports, use the **no platform usb disable** command.

When a USB port is disabled, no system messages are generated if a USB is inserted.

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. With a standard Layer 2 device, ports in different VLANs have to exchange information through a router. By using the device with routing enabled, when you configure both VLAN 20 and VLAN 30 with an SVI to which an IP address is assigned, packets can be sent from Host A to Host B directly through the device with no need for an external router.

Figure 1: Connecting VLANs with a Switch



VLAN routing can be achieved in two ways:

- **With a Network Advantage license:** Advanced routing protocols such as OSPF, EIGRP, and BGP are supported
- **With a Network Essentials license:** Basic routing protocols like RIP and static routing can be used.

The routing function can be enabled on all SVIs. The device routes only IP traffic. When IP routing protocol parameters and address configuration are added to an SVI, any IP traffic received from these ports is routed.

Interface Configuration Mode

The device supports these interface types:

- Physical ports: Device ports and routed ports
- VLANs: Switch virtual interfaces
- Port channels: EtherChannel interfaces

You can also configure a range of interfaces.



Note Before inserting a new SFP, you must clear any existing (speed and duplex) configuration on the port. If you fail to clear the port, any user configuration done before the insertion of the SFP may show undefined behavior.

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

- Type: Gigabit Ethernet (GigabitEthernet or gi) for 10/100/1000 Mbps Ethernet ports and small form-factor pluggable (SFP) module Gigabit Ethernet interfaces.
- On a device with SFP uplink ports, the SFP Uplink ports starts from GigabitEthernet1/1 through GigabitEthernet1/3 and Fixed Downlink ports starts from GigabitEthernet1/4 through GigabitEthernet1/11

You can identify physical interfaces by physically checking the interface location on the device. 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 configure interfaces on standalone device:

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

```
Device# configure terminal
Device(config)# interface GigabitEthernet1/4
```

- To configure the first SFP module (uplink) port on a standalone device, enter this command:

```
Device# configure terminal
Device(config)# interface GigabitEthernet 1/1
```

Default Ethernet Interface Configuration

To configure Layer 2 parameters, if the interface is in Layer 3 mode, you must enter the **switchport** interface configuration command without any parameters to put the interface into Layer 2 mode. This shuts down the interface and then re-enables it, which might generate messages on the device to which the interface is connected. When you put an interface that is in Layer 3 mode into Layer 2 mode, the previous configuration information related to the affected interface might be lost, and the interface is returned to its default configuration.

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

Table 5: Default Layer 2 Ethernet Interface Configuration

Feature	Default Setting
Operating mode	Layer 2 or switching mode (switchport command).
Allowed VLAN range	VLANs 1 to 4094.
Default VLAN (for access ports)	VLAN 1 (Layer 2 interfaces only).
Native VLAN (for IEEE 802.1Q trunks)	VLAN 1 (Layer 2 interfaces only).
VLAN trunking	Switchport mode dynamic auto (supports DTP) (Layer 2 interfaces only).
Port enable state	All ports are enabled.
Port description	None defined.
Speed	Autonegotiate.
Duplex mode	Autonegotiate.
Flow control	Flow control is not supported for sent packets.
EtherChannel (PAgP)	Disabled on all Ethernet ports.
Port blocking (unknown multicast and unknown unicast traffic)	Disabled (not blocked) (Layer 2 interfaces only).
Broadcast, multicast, and unicast storm control	Disabled.
Protected port	Disabled (Layer 2 interfaces only).
Port security	Disabled (Layer 2 interfaces only).
Port Fast	Disabled.
Auto-MDIX	Enabled.
Power over Ethernet (PoE)	Enabled (auto).

Interface Speed and Duplex Mode

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

The switch support speeds at 100 Mb and 1 Gb and operate at full-duplex mode on SFP modules that support speeds up to 1 Gbps. For the list of supported switch models, refer *Cisco IE3500 Series Switch Hardware Installation Guide*.

Speed and Duplex Configuration Guidelines

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

- Gigabit Ethernet (10/100/1000 Mbps) ports support all speed options and all duplex options (auto, half, and full). However, Gigabit Ethernet ports operating at 1000 Mbps and above do not support half-duplex mode.

Multi-Gigabit Ethernet ports (2.5 Gbps) support all speed options, but only support auto and full duplex mode. These ports do not support half-duplex mode at any speed.

SFP ports operating at 1 Gbps, SFP+ ports operating at 10 Gbps support only the **no speed nonegotiate** or **speed nonegotiate** commands. Duplex options are not supported.



Note SFP and SFP+ ports support speed (auto, 10, 100, 1000) and duplex (auto/full/half) options only if the 1000Base-T SFP is used. SFP ports support speed (auto/100) and duplex (auto/full/half) options only if the GLC-GE-100FX modules are used.

- 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 device 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; this is expected behavior.



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 **on**.

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.

Layer 3 Interfaces

The device supports these types of Layer 3 interfaces:

- **SVIs**: Configure SVIs for any VLANs for which you want to route traffic. SVIs are created when you enter a VLAN ID following the **interface vlan** global configuration command. To delete an SVI, use the **no interface vlan** global configuration command.



Note

- VLAN 1 interface is the default interface and cannot be deleted.
- When you create an SVI, it does not become active until it is associated with a physical port.
- SVI MAC addresses do not change after a device reload. This is expected behavior.

When configuring SVIs, you can use the **switchport autostate exclude** command on a port to exclude that port from being included in determining SVI line-state. To disable autostate on the SVI, use the **no autostate** command on the SVI.

- **Routed ports**: Routed ports are physical ports configured to be in Layer 3 mode by using the **no switchport** interface configuration command.
- **Layer 3 EtherChannel ports**: EtherChannel interfaces made up of routed ports.

A Layer 3 device can have an IP address assigned to each routed port and SVI.

There is no defined limit to the number of SVIs and routed ports that can be configured in a device. However, the interrelationship between the number of SVIs and routed ports and the number of other features being configured might have an impact on CPU usage because of hardware limitations. If the device is using its maximum hardware resources, attempts to create a routed port or SVI have these results:

- If you try to create a new routed port, the device generates a message that there are not enough resources to convert the interface to a routed port, and the interface remains as a switchport.

- If you try to create an extended-range VLAN, an error message is generated, and the extended-range VLAN is rejected.
- If the device is notified by VLAN Trunking Protocol (VTP) of a new VLAN, it sends a message that there are not enough hardware resources available and shuts down the VLAN. The output of the **show vlan** user EXEC command shows the VLAN in a suspended state.
- If the device attempts to boot up with a configuration that has more VLANs and routed ports than hardware can support, the VLANs are created, but the routed ports are shut down, and the device sends a message that this was due to insufficient hardware resources.



Note All Layer 3 interfaces require an IP address to route traffic. This procedure shows how to configure an interface as a Layer 3 interface and how to assign an IP address to an interface:

If the physical port is in Layer 2 mode (the default), you must enter the **no switchport** interface configuration command to put the interface into Layer 3 mode. Entering a **no switchport** command disables and then re-enables the interface, which might generate messages on the device to which the interface is connected. Furthermore, when you put an interface that is in Layer 2 mode into Layer 3 mode, the previous configuration information related to the affected interface might be lost, and the interface is returned to its default configuration.

How to Configure Interface Characteristics

The following sections provide information about the various tasks that comprise the procedure to configure interface characteristics.

Configuring an Interface

These general instructions apply to all interface configuration processes.

Procedure

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	interface Example:	Identifies the interface type, and the number of the connector.

	Command or Action	Purpose
	Device(config)# interface gigabitethernet1/1 Device(config-if)#	
Step 4	Follow each interface 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 end to return to privileged EXEC mode.
Step 5	show interfaces	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

Follow these steps to add a description for an interface.

Procedure

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	interface interface-id Example: Device(config)# interface gigabitethernet1/1	Specifies the interface for which you are adding a description, and enter interface configuration mode.
Step 4	description string Example: Device(config-if)# description Connects to Marketing	Adds a description for an interface.
Step 5	end Example:	Returns to privileged EXEC mode.

	Command or Action	Purpose
	Device (config-if) # end	
Step 6	show interfaces <i>interface-id</i> description	Verifies your entry.
Step 7	copy running-config startup-config Example: Device# copy running-config startup-config	(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.

Procedure

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	interface range {GigabitEthernet Loopback Port-channel Tunnel create macro} } Example: Device (config)# interface range GigabitEthernet 1/1-11, GigabitEthernet 2/1-8	Specifies the range of interfaces (VLANs or physical ports) to be configured, and enter interface-range configuration mode. For example, an 8 port expansion module can use: <i>GigabitEthernet 2/1-8</i> . - You can use the interface range command to configure up to five port ranges or a previously defined macro. - The macro variable is explained in Configuring and Using Interface Range Macros. - 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.

	Command or Action	Purpose
		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.
Step 4	end Example: Device(config)# end	Returns to privileged EXEC mode.

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.

Procedure

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	define interface-range <i>macro_name</i> <i>interface-range</i> Example: Device(config)# define interface-range enet_list gigabitethernet1/1-11	Defines the interface-range macro, and saves it in NVRAM. - The <i>macro_name</i> is a 32-character maximum character string. - A macro can contain up to five comma-separated interface ranges. - Each <i>interface-range</i> must consist of the same port type. Note 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.

	Command or Action	Purpose
Step 4	interface range macro <i>macro_name</i> Example: <pre>Device(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.
Step 5	end Example: <pre>Device(config)# end</pre>	Returns to privileged EXEC mode.
Step 6	show running-config include define Example: <pre>Device# show running-config include define</pre>	Shows the defined interface range macro configuration.
Step 7	copy running-config startup-config Example: <pre>Device# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

Setting the Interface Speed and Duplex Parameters

Follow these steps to configure the interface speed and duplex parameters.

Procedure

	Command or Action	Purpose
Step 1	enable Example: <pre>Device> enable</pre>	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	configure terminal Example: <pre>Device# configure terminal</pre>	Enters global configuration mode.
Step 3	interface <i>interface-id</i> Example:	Specifies the physical interface to be configured, and enters interface configuration mode.

	Command or Action	Purpose
	Device(config)# interface gigabitethernet1/3	
Step 4	duplex {auto full half} Example: Device(config-if)# duplex half	Enters the duplex parameter for the interface. Enables half-duplex mode (for interfaces operating only at 10 or 100 Mb/s). Half duplex is not supported on multi-Gigabit Ethernet ports configured for speed of 1000 Mb/s. You can configure the duplex setting when the speed is set to auto .
Step 5	end Example: Device(config-if)# end	Returns to privileged EXEC mode.
Step 6	show interfaces interface-id Example: Device# show interfaces gigabitethernet1/1	Displays the interface speed and duplex mode configuration.
Step 7	copy running-config startup-config Example: Device# copy running-config startup-config	(Optional) Saves your entries in the configuration file.

Configuring the IEEE 802.3x Flow Control

Follow these steps to configure the IEEE 802.3x flow control.

Procedure

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode

	Command or Action	Purpose
Step 3	interface <i>interface-id</i> Example: <pre>Device(config)# interface gigabitethernet1/4</pre>	Specifies the physical interface to be configured, and enters interface configuration mode.
Step 4	flowcontrol {receive} {on off desired} Example: <pre>Device(config-if)# flowcontrol receive on</pre>	Configures the flow control mode for the port.
Step 5	end Example: <pre>Device(config-if)# end</pre>	Returns to privileged EXEC mode.
Step 6	show flowcontrol interface <i>interface-id</i> Example: <pre>Device# show flowcontrol interface GigabitEthernet1/4</pre>	Verifies the specified interface flow control settings.
Step 7	show flowcontrol module <i>slot</i> Example: <pre>Device# show flowcontrol module 1</pre>	Verifies the interface flow control settings on the module.
Step 8	copy running-config startup-config Example: <pre>Device# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

Configure Layer 3 Interface

Follow these steps to configure a layer 3 interface.

Procedure

	Command or Action	Purpose
Step 1	enable Example: <pre>Device> enable</pre>	Enables privileged EXEC mode. Enter your password, if prompted.

	Command or Action	Purpose
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	interface {gigabitethernet interface-id} {vlan vlan-id} {port-channel port-channel-number} Example: Device(config)# interface gigabitethernet1/1	Specifies the interface to be configured as a Layer 3 interface, and enters interface configuration mode.
Step 4	no switchport Example: Device(config-if)# no switchport	(For physical ports only) Enters Layer 3 mode.
Step 5	ip address ip_address subnet_mask Example: Device(config-if)# ip address 192.0.2.10 255.255.255.0	Configures the IP address and IP subnet.
Step 6	no shutdown Example: Device(config-if)# no shutdown	Enables the interface.
Step 7	end Example: Device(config-if)# end	Returns to privileged EXEC mode.
Step 8	show interfaces [interface-id]	Verifies the configuration.
Step 9	copy running-config startup-config Example: Device# copy running-config startup-config	(Optional) Saves your entries in the configuration file.

Configuring a Logical Layer 3 GRE Tunnel Interface

Before you begin

Generic Routing Encapsulation (GRE) is a tunneling protocol used to encapsulate network layer protocols inside virtual point-to-point links. A GRE tunnel only provides encapsulation and not encryption.

**Note**

- GRE tunnels are supported on the hardware. When GRE is configured without tunnel options, packets are hardware-switched. When GRE is configured with tunnel options (such as key, checksum, and so on), packets are switched in the software.
- A maximum of 10 GRE tunnels are supported.
- Other features such as Access Control Lists (ACL) and Quality of Service (QoS) are not supported for the GRE tunnels.
- The **tunnel path-mtu-discovery** command is not supported for GRE tunnels. To avoid fragmentation, you can set the maximum transmission unit (MTU) of both ends of the GRE tunnel to the lowest value by using the **ip mtu 832** command.

To configure a GRE tunnel, perform this task:

Procedure

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	interface tunnel <i>number</i> Example: Device(config)# interface tunnel 2	Enables tunneling on the interface.
Step 4	ip address <i>ip_address subnet_mask</i> Example: Device(config)# ip address 192.0.2.10 255.255.255.0	Configures the IP address and IP subnet.
Step 5	tunnel source {<i>ip_address</i> <i>type_number</i>} Example: Device(config)# tunnel source 10.0.0.1	Configures the tunnel source.
Step 6	tunnel destination {<i>host_name</i> <i>ip_address</i>} Example: Device(config)# tunnel destination 10.0.0.2	Configures the tunnel destination.

	Command or Action	Purpose
Step 7	tunnel mode gre ip Example: Device(config)# tunnel mode gre ip	Configures the tunnel mode.
Step 8	end Example: Device(config)# end	Exits configuration mode.

Configuring SVI Autostate Exclude

SVI Autostate controls the status of a Switch Virtual Interface (SVI), determining whether it is up or down based on the operational state of its associated switch ports. In Layer 3 switches, the **switchport autostate exclude** command automatically brings up a VLAN when configured. By default, SVI autostate is enabled. It can also be disabled to manually bring up the VLAN.

Follow these steps to exclude SVI autostate.

Procedure

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	interface interface-id Example: Device(config)# interface gigabitethernet1/1	Specifies a Layer 2 interface (physical port or port channel), and enters interface configuration mode.
Step 4	switchport autostate exclude Example: Device(config-if)# switchport autostate exclude	Excludes the access or trunk port when defining the status of an SVI line state (up or down)
Step 5	end Example:	Returns to privileged EXEC mode.

	Command or Action	Purpose
	Device (config-if) # end	
Step 6	show running config interface <i>interface-id</i> Example: Device# show running config interface gigabitethernet1/1	(Optional) Shows the running configuration. Verifies the configuration.
Step 7	copy running-config startup-config Example: Device# copy running-config startup-config	(Optional) Saves your entries in the configuration file.

Shutting Down and Restarting an 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.

Procedure

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	interface {vlan <i>vlan-id</i>} { gigabitethernet <i>interface-id</i>} {port-channel <i>port-channel-number</i>} Example: Device (config) # interface gigabitethernet1/1	Selects the interface to be configured.
Step 4	shutdown Example: Device (config-if) # shutdown	Shuts down an interface.

	Command or Action	Purpose
Step 5	no shutdown Example: Device(config-if)# no shutdown	Restarts an interface.
Step 6	end Example: Device(config-if)# end	Returns to privileged EXEC mode.
Step 7	show running-config Example: Device# show running-config	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.

Procedure

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	line console 0 Example: Device(config)# line console 0	Configures the console and enters line configuration mode.
Step 4	media-type rj45 Example: Device(config-line)# media-type rj45	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	end Example:	Returns to privileged EXEC mode.

	Command or Action	Purpose
	Device(config)# end	
Step 6	copy running-config startup-config Example: Device# copy running-config startup-config	(Optional) Saves your entries in the configuration file.

Configuring USB Inactivity Timeout

When the USB console port is deactivated due to a timeout, you can restore its operation by disconnecting and reconnecting the USB cable.

Procedure

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	line console 0 Example: Device(config)# line console 0	Configures the console and enters line configuration mode.
Step 4	usb-inactivity-timeout timeout-minutes Example: Device(config-line)# usb-inactivity-timeout 30	Specifies an inactivity timeout for the console port. The range is 1 to 240 minutes. The default is to have no timeout configured.
Step 5	copy running-config startup-config Example: Device# copy running-config startup-config	(Optional) Saves your entries in the configuration file.

Disabling USB Ports

To disable all USB ports, perform this procedure.

Procedure

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	[no] platform usb disable Example: Device(config)# platform usb disable	Disables all the USB ports on the device. Use the no platform usb disable command to reenab the USB ports.
Step 4	exit Example: Device(config)# exit	Exits to privileged EXEC mode.
Step 5	copy running-config startup-config Example: Device# copy running-config startup-config	(Optional) Saves your entries in the configuration file.

Monitoring Interface Characteristics

The following sections provide information about 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 6: show Commands for Interfaces

Command	Purpose
show interfaces interface-id status [err-disabled]	Displays interface status or a list of interfaces in the error-disabled state.

Command	Purpose
show interfaces [<i>interface-id</i>] switchport	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.
show interfaces [<i>interface-id</i>] description	Displays the description configured on an interface or all interfaces and the interface status.
show ip interface [<i>interface-id</i>]	Displays the usability status of all interfaces configured for IP routing or the specified interface.
show interface [<i>interface-id</i>] stats	Displays the input and output packets by the switching path for the interface.
show interface [<i>interface-id</i>] link [module number]	Displays the up time and down time of an interface or all interfaces.
show interfaces <i>interface-id</i>	(Optional) Displays speed and duplex on the interface.
show interfaces transceiver dom-supported-list	(Optional) Displays Digital Optical Monitoring (DOM) status on the connect SFP modules.
show interfaces transceiver properties	(Optional) Displays temperature, voltage, or amount of current on the interface.
show interfaces [<i>interface-id</i>] [{ transceiver properties detail }] <i>module number</i>	Displays physical and operational status about an SFP module.
show running-config interface [<i>interface-id</i>]	Displays the running configuration in RAM for the interface.
show version	Displays the hardware configuration, software version, the names and sources of configuration files, and the boot images.
show controllers ethernet-controller <i>interface-id</i> phy	Displays the operational state of the auto-MDIX feature on the interface.

Clearing and Resetting Interfaces and Counters

Table 7: *clear* Commands for Interfaces

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

The following sections provide examples of interface characteristics configurations.

Example: Adding a Description to an Interface

The following example shows how to add a description to an interface:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTRL/Z.
Device(config)# interface gigabitethernet1/1
Device(config-if)# description Connects to Marketing
Device(config-if)# end
Device# show interfaces gigabitethernet1/1 description

Interface Status          Protocol Description
Gi1/1      admin down      down      Connects to Marketing
```

Example: Setting Interface Speed and Duplex Mode

The following example shows how to set the interface speed to 10 Mbps and the duplex mode to full, on a 10/100/1000 Mbps port:

```
Device# configure terminal
Device(config)# interface gigabitethernet1/4
Device(config-if)# speed 10
Device(config-if)# duplex full
```

The following example shows how to set the interface speed to 100 Mbps on a 10/100/1000 Mbps port:

```
Device# configure terminal
Device(config)# interface gigabitethernet1/4
Device(config-if)# speed 100
```

Example: Configuring a Layer 3 Interface

The following example shows how to configure a Layer 3 interface:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTRL/Z.
Device(config)# interface gigabitethernet1/1
Device(config-if)# no switchport
Device(config-if)# ip address 192.0.2.10 255.255.255.0
Device(config-if)# no shutdown
```

Example: Configuring the Console Media Type

The following example shows how to disable the USB console media type and enable the RJ-45 console media type:

Example: Configuring USB Inactivity Timeout

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

The following example shows how to reverse the previous configuration and immediately activate any USB console that is connected:

```
Device# configure terminal
Device(config)# line console 0
Device(config-line)# no media-type rj45
```

Example: Configuring USB Inactivity Timeout

The following example shows how to configure the inactivity timeout to 30 minutes:

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

```
Device# configure terminal
Device(config)# line console 0
Device(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 a switch is disconnected and reconnected, a log, which is similar to this, appears:

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