CHAPTER 10

Configuring Interfaces

This chapter defines the types of interfaces on the Cisco ME 3400E Ethernet Access switch and describes how to configure them.

Note For complete syntax and usage information for the commands used in this chapter, see the switch command reference for this release and the online *Cisco IOS Interface Command Reference, Release 12.2.*

Understanding Interface Types

UNI, NNI, and ENI Port Types

The Cisco ME switch supports user-network interfaces (UNIs), network node interfaces (NNIs), and enhanced network interfaces (ENIs). UNIs are typically connected to a host, such as a PC or a Cisco IP phone. NNIs are typically connected to a router or to another switch. ENIs have the same functionality as UNIs, but can be configured to support protocol control packets for Cisco Discovery Protocol (CDP), Spanning-Tree Protocol (STP), Link Layer Discovery Protocol (LLDP), and EtherChannel Link Aggregation Control Protocol (LACP) or Port Aggregation Protocol (PAgP). By default, the 10/100 ports and the dual-purpose ports are configured as UNIs, and the SFP-only module uplink ports are configured as NNIs. No ports are ENIs by default.

Note On the Cisco ME 3400E-24TS-M switch, the dual-purpose ports serve as the uplink ports and are NNIs by default.

If the switch is running the metro access image, only four ports on the switch can be configured as NNIs at one time. If the switch is running the metro IP access image, there is no limit to the number of NNIs that can be configured on the switch. All ports on the switch can be configured as UNIs or ENIs.

The default state for a UNI or ENI is administratively down to prevent unauthorized users from gaining access to other ports as you configure the switch. Traffic is not switched between these ports, and all arriving traffic at UNIs or ENIs must leave on NNIs to prevent a user from gaining access to another user's private network. If it is appropriate for two or more UNIs or ENIs to exchange traffic within the switch, the UNIs and ENIs can be assigned to a community VLAN. See Chapter 12, "Configuring VLANs," for instructions on how to configure community VLANs.

Note Even though the default state for a UNI or ENI is shutdown, entering the **default interface** *interface-id*

A port can be reconfigured from UNI to NNI or ENI and the reverse. When a port is reconfigured as another interface type, it inherits all the characteristics of that interface type. When you reconfigure a UNI or ENI to be an NNI, you must enable the port before it becomes active.

Changing the port type from UNI to ENI does not affect the administrative state of the port. If the UNI status is shut down, it remains shut down when reconfigured as an ENI; if the port is in a no shutdown state, it remains in the no shutdown state. At any time, all ports on the Cisco ME switch are either UNI, NNI, or ENI.

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. For more information about VLANs, see Chapter 12, "Configuring VLANs." 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 associated with the VLAN ID or when a user creates te VLAN ID.

To isolate VLANs of different customers in a service-provider network, the Cisco ME switch uses UNI-ENI VLANs. UNI-ENI VLANs isolate user network interfaces (UNIs) or enhanced network interfaces (ENIs) on the switch from UNIs or ENIs that belong to other customer VLANs. There are two types of UNI-ENI VLANs:

- UNI-ENI isolated VLAN—This is the default VLAN state for all VLANs created on the switch. Local switching does not occur among UNIs or ENIs on the switch that belong to the same UNI-ENI isolated VLAN.
- UNI-ENI community VLAN—Local switching is allowed among UNIs and ENIs on the switch that belong to the same UNI community VLAN. If UNIs or ENIs belong to the same customer, and you want to switch packets between the ports, you can configure the common VLAN as a UNI-ENI community VLAN.

Note Local switching takes place between ENIs and UNIs in the same community VLAN. Because you can enable spanning tree on ENIs, but not on UNIs, you should use caution when configuring ENIs and UNIs in the same community VLAN. UNIs are always in the forwarding state.

For more information about UNI VLANs, see the "UNI-ENI VLANs" section on page 12-5.

To configure VLANs, use the **vlan** *vlan-id*

Extended-range VLANs (VLAN IDs 1006 to 4094) are not added to the VLAN database. VLAN configuration is saved in the switch running configuration, and you can save it in the switch startup configuration file by entering the **copy running-config startup-config** privileged EXEC command.

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.

For a tunnel port, set and define the VLAN ID for the customer-specific VLAN tag. See Chapter 14, "Configuring IEEE 802.1Q Tunneling, VLAN Mapping, and Layer 2 Protocol Tunneling."

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, a trunk port, a private-VLAN port, or a tunnel port. You can configure a port as an access port or trunk port. You configure a private VLAN port as a host or promiscuous port that belongs to a private-VLAN primary or secondary VLAN. (Only NNIs can be configured as promiscuous ports.) You must manually configure tunnel ports as part of an asymmetric link connected to an IEEE 802.1Q trunk port. 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. Use the **switchport** command with no keywords to put an interface that is in Layer 3 mode into Layer 2 mode.

Note 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.

For detailed information about configuring access port and trunk port characteristics, see Chapter 12, "Configuring VLANs." For more information about tunnel ports, see Chapter 14, "Configuring IEEE 802.1Q Tunneling, VLAN Mapping, and Layer 2 Protocol Tunneling."

Access Ports

An access port belongs to and carries the traffic of only one VLAN. 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 an IEEE 802.1Q tagged packet, the packet is dropped, and the source address is not learned. IEEE 802.1x can also be used for VLAN assignment.

Two types of access ports are supported:

- Static access ports are manually assigned to a VLAN.
- VLAN membership of dynamic access ports is learned through incoming packets. By default, a dynamic access port is a member of no VLAN, and forwarding to and from the port is enabled only when the VLAN membership of the port is discovered. UNIs begin forwarding packets as soon as they are enabled. 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 Cisco ME switch cannot be a VMPS server. Dynamic access ports for VMPS are only supported on UNIs and ENIs.

Trunk Ports

An IEEE 802.1Q trunk port carries the traffic of multiple VLANs and by default is a member of all VLANs in the VLAN database. A 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 multiple VLANs, 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 the VLAN is in the enabled state.

For more information about trunk ports, see Chapter 12, "Configuring VLANs."

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.

For more information about tunnel ports, see Chapter 14, "Configuring IEEE 802.1Q Tunneling, VLAN Mapping, and Layer 2 Protocol Tunneling."

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 STP.

Configure routed ports by putting the interface into Layer 3 mode with the interface configuration command. Then assign an IP address to the port, enable routing, and assign routing protocol characteristics by using the and *protocol* global configuration commands.

Note Entering a 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.

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. See the "Configuring Layer 3 Interfaces" section on page 10-25 for information about what happens when hardware resource limitations are reached.

For more information about IP unicast and multicast routing and routing protocols, see Chapter 36, "Configuring IP Unicast Routing" and Chapter 41, "Configuring IP Multicast Routing."

Note For full Layer 3 routing, you must have the metro IP access image installed on the switch

Ethernet Management Port

The Ethernet management port, also referred to as the *Fa0 or fastethernet0 port*, is a Layer 3 host port to which you can connect a PC. You can use the Ethernet management port instead of the switch console port for network management.

See the "Using the Ethernet Management Port" section on page 10-12 for more information.

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. Only one SVI can be associated with a VLAN, but you need to configure an SVI for a VLAN only when you wish 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; in Layer 3 mode, you can configure routing across SVIs.

Although the 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. See the "Configuring Layer 3 Interfaces" section on page 10-25 for information about what happens when hardware resource limitations are reached.

SVIs are created the first time that you enter the interface configuration command for a VLAN interface. The VLAN corresponds to the VLAN tag associated with data frames on an 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. For more information, see the "Manually Assigning IP Information" section on page 3-14.

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

SVIs support routing protocols. For more information about configuring IP routing, see Chapter 36, "Configuring IP Unicast Routing," and Chapter 41, "Configuring IP Multicast Routing."

Note Routed ports (or SVIs) are supported only when the metro IP access image is installed on the switch.

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, 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 Cisco Discovery Protocol (CDP), Link Aggregation Control Protocol (LACP), and the Port Aggregation Protocol (PAgP), which operate only on physical NNI or ENI 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 global configuration command. Then you manually assign an interface to the EtherChannel by using the interface configuration command. For Layer 2 interfaces, use the interface configuration command to dynamically create the port-channel logical interface. This command binds the physical and logical ports together. For more information, see Chapter 35, "Configuring EtherChannels and Link-State Tracking."

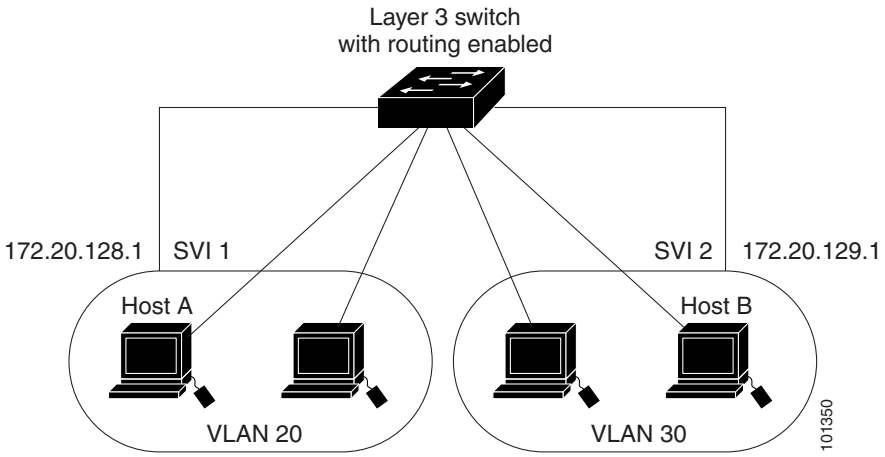
Dual-Purpose Ports

Each dual-purpose port is considered as a single interface with dual front ends (an RJ-45 connector and an SFP module connector). The dual front ends are not redundant interfaces; the switch activates only one connector of the pair.

By default, dual-purpose ports are user-network interfaces (UNIs) and SFP-only module ports are network node interfaces (NNIs). By default, the switch dynamically selects the dual-purpose port media type that first links up. However, you can use the **media-type**

Connecting Interfaces

Figure 10-1 Connecting VLANs with the Switch



When the metro IP access image is running on the switch, routing can be enabled on the switch. Whenever possible, to maintain high performance, forwarding is done by the switch hardware. However, only IP Version 4 packets with Ethernet II encapsulation can be routed in hardware. The routing function can be enabled on all SVIs and routed ports. The switch routes only IP traffic. When IP routing protocol parameters and address configuration are added to an SVI or routed port, any IP traffic received from these ports is routed. For more information, see Chapter 36, "Configuring IP Unicast Routing," Chapter 41, "Configuring IP Multicast Routing," and Chapter 42, "Configuring MSDP."

Using Interface Configuration Mode

-
-
-

-

-
-

Procedures for Configuring Interfaces

Step 1

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#
```

Step 2

```
Switch(config)#           fastethernet0/1
Switch(config-if)#
```

Note

fastethernet 0/1 fastethernet0/1 fa 0/1 fa0/1

Step 3 **no shutdown**

```
Switch(config-if)# no shutdown
```

Step 4 **interface**

end

interface range **interface range macro**

Step 5 **show**

---

show interfaces

Configuring a Range of Interfaces

interface range

	Command	Purpose
Step 1		
Step 2		• • •
Step 3		
Step 4		
Step 5		
Step 6	[ ]	Verify the configuration of the interfaces in the range.
Step 7		(Optional) Save your entries in the configuration file.

interface range

- *port-range*
  - **vlan** *vlan-ID* *vlan-ID*
  - **fastethernet** module/{first *port*} - {*last port*}, where the module is always 0

gigabitethernet

port-channel *port-channel-number* *port-channel-number* *port-channel-number*

interface range

interface range
interface vlan **show running-config**
show running-config
interface range

interface range

```
interface range fastethernet0/1 - 2
         no shutdown
         speed 100
```

```
configure terminal
        interface range fastethernet0/1 - 3 , gigabitethernet0/1 - 2
                 flowcontrol receive on
```

macro_name *interface-range*	*macro_name* *interface-range*

show running-config | include define	
copy running-config startup-config	

macro_name

interface-range

vlan-ID *vlan-ID*

port *last port*

first port *last port*

port-channel-number *port-channel-number* *port-channel-number*

interface-range **0/1 - 2** **gigabitethernet0/1-2**

interface vlan **show running-config**

show running-config *interface-ranges*

enet_list

```
define interface-range enet_list gigabitethernet0/1 - 2
end
show running-config | include define
define interface-range enet_list GigabitEthernet0/1 - 2
```

Using the Ethernet Management Port

-
-
-
-

Understanding the Ethernet Management Port

Figure 10-2 Connecting a Switch to a PC

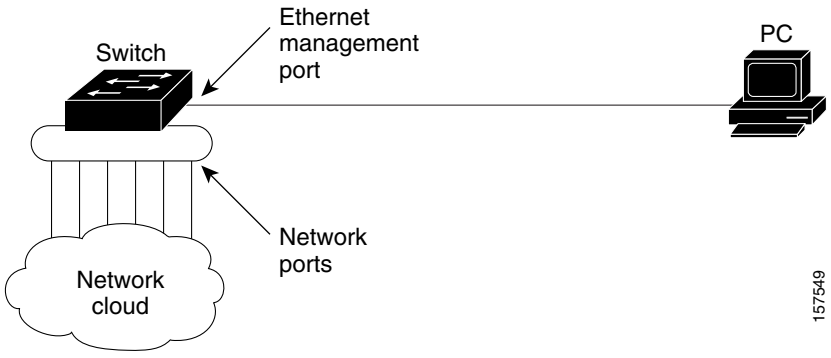
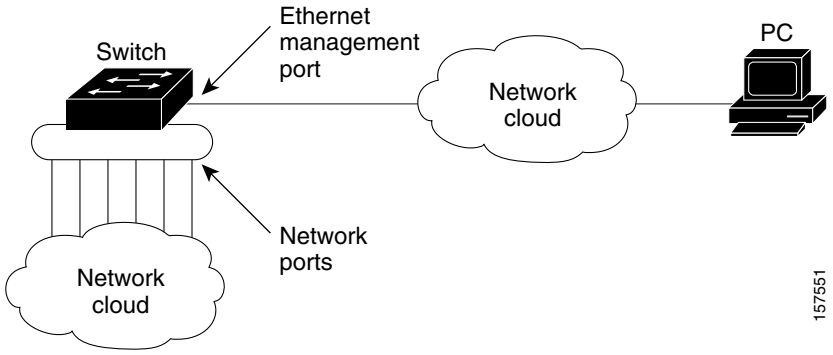


Figure 10-3 Network Example with Routing Protocols Enabled



-
-

Supported Features on the Ethernet Management Port

-
-
-
-
-
-
-
-
-

-
-
-
-

Caution

Configuring the Ethernet Management Port

TFTP and the Ethernet Management Port

Table 1 Boot Loader Commands

Command	Description
	[1] table when this command is entered without the parameter. Enables ARP to associate a MAC address with the specified IP address when this command is entered with the parameter.
mgmt_clr	Clears the statistics for the Ethernet management port.
mgmt_init	Starts the Ethernet management port.
mgmt_show	Displays the statistics for the Ethernet management port.
ping	Sends ICMP ECHO_REQUEST packets to the specified network host.
boot tftp*:/file-url ...*	Loads and boots an executable image from the TFTP server and enters the command-line interface. For more details, see the command reference for this release.
tftp:/*source-file-url* *filesystem***:/***destination-file-url*	

1. ARP = Address Resolution Protocol.

switchport

Default Ethernet Configuration for NNIs

Feature	Default Setting
	VLANs 1– 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 access (Layer 2 interfaces only).
Port enable state	Enabled.
Port description	None defined.
Speed	Autonegotiate.
Duplex mode	Autonegotiate.
IEEE 802.3x flow control	Flow control is set to : . It is always off for sent packets.
EtherChannel	Disabled on all Ethernet ports. See Chapter 35, "Configuring EtherChannels and Link-State Tracking."
Port blocking (unknown multicast and unknown unicast traffic)	Disabled (not blocked) (only Layer 2 interfaces). See the "Configuring Port Blocking" section on page 23-6.

Table 10-2 Default Ethernet Configuration for NNIs (continued)

Broadcast, multicast, and unicast storm control	Disabled. See the "Default Storm Control Configuration" section on page 23-3.
Port security	Disabled (only Layer 2 interfaces). See the "Default Port Security Configuration" section on page 23-10.
Port Fast	Disabled. See the "Default Optional Spanning-Tree Configuration" section on page 17-5.
Auto-MDIX	Enabled.
Cisco Discovery Protocol (CDP)	Enabled.
VMPS	Not configured.

Default Ethernet Configuration for UNIs and ENIs

Operating mode	Layer 2 or switching mode (command).
Allowed VLAN range	VLANs 1– 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 access (Layer 2 interfaces only).
Dynamic VLAN	Enabled.
Port enable state	Disabled when no configuration file exists.
Port description	None defined.
Speed	Autonegotiate.
Duplex mode	Autonegotiate.
IEEE 802.3x flow control	Flow control is set to : . It is always off for sent packets.
EtherChannel	Disabled on all Ethernet ports. See Chapter 35, "Configuring EtherChannels and Link-State Tracking."
Port blocking (unknown multicast and unknown unicast traffic)	Disabled (not blocked) (only Layer 2 interfaces). See the "Configuring Port Blocking" section on page 23-6.
Broadcast, multicast, and unicast storm control	Disabled. See the "Default Storm Control Configuration" section on page 23-3.
Port security	Disabled (only Layer 2 interfaces). See the "Default Port Security Configuration" section on page 23-10.
Auto-MDIX	Enabled.

By default, all the 10/100 ports on the Cisco ME switch are configured as UNIs, and the SFP module ports are configured as NNIs. You can also configure the port type as ENI. An ENI has the same characteristics as a UNI, but it can be configured to support CDP, STP, LLDP, and Etherchannel LACP and PAgP.

You use the interface configuration command to change the port types. If the switch is running the metro access image, only four ports on the switch can be configured as NNIs at one time.If the switch is running the metro IP access image, there is no limit to the number of NNIs that can be configured on the switch. All ports on the switch can be configured as UNIs or ENIs.

When a port is changed from an NNI to a UNI or ENI, it inherits the configuration of the assigned VLAN, either in isolated or community mode. For more information about configuring UNI-ENI isolated and UNI-ENI community VLANs, see Chapter 12, "Configuring VLANs."

When you change a port from NNI to UNI or ENI or the reverse, any features exclusive to the port type revert to the default configuration. For Layer 2 protocols, such as STP, CDP, and LLDP, the default for UNIs and ENIs is disabled (although they can be enabled on ENIs) and the default for NNIs is enabled.

By default, the switch sends keepalive messages on UNI s and ENIs and does not send keepalive messages on NNIs. Changing the port type from UNI or ENI to NNI or from NNI to UNI or ENI has no effect on the keepalive status. You can change the keepalive state from the default setting by entering the [ ] **keepalive** **keepalive**

no keepalive

| | }	Change a port to an ENI, NNI, or UNI.
	Return to privileged EXEC mode.
	Verify the interface IEEE 802.3x flow control settings.
	(Optional) Save your entries in the configuration file.

no port-type **default port-type**

```
                    port-type nni
                    no shutdown
5d20h: %SYS-5-CONFIG_I: Configured from console by console
Switch(config-if)# end
Switch# copy running-config startup-config
```

Configuring Interface Speed and Duplex Mode

Ethernet interfaces on the switch operate at 10, 100, or 1000 Mbps 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-Mbps ports operate in half-duplex mode, which means that stations can either receive or send traffic.

Switch models include combinations of Fast Ethernet (10/100-Mbps) ports, Gigabit Ethernet (10/100/1000-Mbps) ports, and small form-factor pluggable (SFP) module slots supporting SFP modules.

These sections describe how to configure the interface speed and duplex mode:

- Speed and Duplex Configuration Guidelines, page 10-18
- Setting the Interface Speed and Duplex Parameters, page 10-19

Speed and Duplex Configuration Guidelines

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

- You can configure interface speed on Fast Ethernet (10/100-Mbps) and Gigabit Ethernet (10/100/1000-Mbps) ports. You can configure Fast Ethernet ports to full-duplex, half-duplex, or to autonegotiate mode. You can configure Gigabit Ethernet ports to full-duplex mode or to autonegotiate. You also can configure Gigabit Ethernet ports to half-duplex mode if the speed is 10 or 100 Mbps. Half-duplex mode is not supported on Gigabit Ethernet ports operating at 1000 Mbps.
- With the exception of when 1000BASE-T SFP modules are installed in the SFP module slots, you cannot configure speed on SFP module ports, but you can configure speed to not negotiate ( ) if connected to a device that does not support autonegotiation.

  However, when a 1000BASE-T SFP module is in the SFP module slot, you can configure speed as 10, 100, or 1000 Mbps, or auto, but not as .

  On a 100BASE-FX SFP module, you cannot configure the speed as .
- You cannot configure duplex mode on SFP module ports; they operate in full-duplex mode except in these situations:

  When a Cisco1000BASE-T SFP module is in the SFP module slot, you can configure duplex mode to or . Half-duplex mode is supported with the setting.

  When a Cisco100BASE-FX SFP module is in the SFP module slot, you can configure duplex mode to or . Although the keyword is available, it puts the interface in half-duplex mode (the default for this SFP module) because the 100BASE-FX SFP module does not support autonegotiation.
- If both ends of the line support autonegotiation, we highly recommend the default setting of negotiation.
- If one interface supports autonegotiation and the other end does not, configure duplex and speed on both interfaces; do not use the 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. On the Cisco ME switch, STP is supported on NNIs by default and can be enabled on ENIs. UNIs do not support STP.

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

Setting the Interface Speed and Duplex Parameters

Beginning in privileged EXEC mode, follow these steps to set the speed and duplex mode for a physical interface.

Note On dual-purpose ports, changing the interface type by entering the interface configuration command removes the speed and duplex configurations. See the "Configuring a Dual-Purpose Port" section on page 10-20 for information about speed and duplex setting on these ports.

	Command	Purpose
Step 1		Enter global configuration mode.
Step 2		Specify the physical interface to be configured, and enter interface configuration mode.
Step 3		Enable the port, if necessary. By default, UNIs and ENIs are disabled, and NNIs are enabled.
Step 4	{ [| |] }	Enter the appropriate speed parameter for the interface: • Enter , , or to set a specific speed for the interface. The keyword is available only for 10/100/1000 Mbps ports or SFP module ports with a 1000BASE-T SFP module. • Enter to enable the interface to autonegotiate speed with the connected device. If you use the , , or the keywords with the keyword, the port autonegotiates only at the specified speeds. • The keyword is available only for SFP module ports. SFP module ports operate only at 1000 Mbps but can be configured to not negotiate if connected to a device that does not support autonegotiation. **Note** When a Cisco1000BASE-T SFP module is in the SFP module slot, the speed can be configured to , , , or to , but not to .
Step 5	**duplex auto | full | half**	**auto** • **auto full** • **full half auto**
Step 6	**end**	

	Command	Purpose
	show interfaces	
Step 8	copy running-config startup-config	

no speed no duplex

default

interface

```
duplex half
```

```
configure terminal
        interface gigabitethernet0/2
           speed 100
```

system mtu jumbo

media-type

auto-select

	Command	Purpose
Step 1	configure terminal	
Step 2	interface	
Step 3	media-type auto-select rj45 sfp	• auto-select • rj45 • sfp
Step 4	end	
Step 5	show interfaces transceiver properties	
Step 6	copy running-config startup-config	

no media-type

auto-select

speed duplex

sfp rj45

auto-select

Note

•

•

- shutdown no shutdown

media-type

Configuring IEEE 802.3x Flow Control

Note

flowcontrol receive
on off desired off
desired

- receive on desired
- receive off

Note

flowcontrol

	Command	Purpose
Step 1	configure terminal	
Step 2	interface	
Step 3	no shutdown	
Step 4	flowcontrol receive on off desired	
Step 5	end	
Step 6	show interfaces	
Step 7	copy running-config startup-config	

flowcontrol receive off

Configuring Auto-MDIX on an Interface

auto

Table 10-4 Link Conditions and Auto-MDIX Settings

Local Side Auto-MDIX	Remote Side Auto-MDIX	With Correct Cabling	With Incorrect Cabling

	Command	Purpose
Step 1		
Step 2		
Step 3		
Step 4		
Step 5		
Step 6		
Step 7		
Step 8		
Step 9		

To disable auto-MDIX, use the interface configuration command.

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

Adding a Description for an Interface

You can add a description about an interface to help you remember its function. The description appears in the output of these privileged EXEC commands: , , and .

Beginning in privileged EXEC mode, follow these steps to add a description for an interface:

Use the interface configuration command to delete the description.

This example shows how to add a description on a port and how to verify the description:

```
                description Connects to Marketing
                end
        show interfaces gigabitethernet0/2 description
Interface Status         Protocol Description
Gi 0/2   admin down     down     Connects to Marketing
```

Configuring Layer 3 Interfaces

-

  Note

-
-
-
-
- VLAN is rejected.

  If the switch 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 switch sends a message that this was due to insufficient hardware resources.

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 interface configuration command to put the interface into Layer 3 mode. Entering a 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

Beginning in privileged EXEC mode, follow these steps to configure a Layer 3 interface:

	Command	Purpose
Step 1		
Step 2		
Step 3		
Step 4		
Step 5	*ip_address subnet_mask*	
	interface-id *interface-id* *interface-id*	

To remove an IP address from an interface, use the interface configuration command.

This example shows how to configure a port as a routed port and to assign it an IP address:

```
ip address 192.20.135.21 255.255.255.0
```

Configuring the System MTU

Note

egress

bytes	
bytes	

system mtu routing	
end	
copy running-config startup-config	
reload	

```
                system mtu jumbo 1800
                exit
        reload
```

```
                system mtu jumbo 25000
                                 ^
% Invalid input detected at '^' marker.
```

show ?

Table 10-5 Show Commands for Interfaces

show interfaces [*interface-id]* *number*	*interface-id*– **detail**– **dom-supported-list**– **module** *number*– **properties**– **threshold-table**–
show port-type eni nni |	
interface-id	
interface-id	

Table 10-6 lists the privileged EXEC mode commands that you can use to clear counters and reset interfaces.

Table 10-6 Clear Commands for Interfaces

To clear the interface counters shown by the privileged EXEC command, use the privileged EXEC command. The command clears all current interface counters from the interface unless you specify optional arguments that clear only a specific interface type from a specific interface number.

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

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.

Beginning in privileged EXEC mode, follow these steps to shut down an interface:

Use the interface configuration command to enable an interface.

To verify that an interface is disabled, enter the privileged EXEC command. A disabled interface is shown as *administratively down* in the display.