



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.

- [Understanding Interface Types, page 10-1](#)
 - [Using Interface Configuration Mode, page 10-8](#)
 - [Using the Ethernet Management Port, page 10-12](#)
 - [Configuring Ethernet Interfaces, page 10-15](#)
 - [Configuring Layer 3 Interfaces, page 10-25](#)
 - [Configuring the System MTU, page 10-27](#)
 - [Monitoring and Maintaining the Interfaces, page 10-29](#)



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, page 10-2](#)
- [Port-Based VLANs, page 10-2](#)
- [Switch Ports, page 10-3](#)
- [Routed Ports, page 10-5](#)
- [Switch Ports, page 10-3](#)
- [Switch Virtual Interfaces, page 10-5](#)
- [EtherChannel Port Groups, page 10-6](#)
- [Dual-Purpose Ports, page 10-6](#)
- [Connecting Interfaces, page 10-7](#)

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

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*

copy running-config startup-config privileged EXEC command.

Add ports to a VLAN by using the **switchport**

[“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 `interface` configuration commands. Use the `no` 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.

Routed Ports

protocol



Note

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.



Note



Note

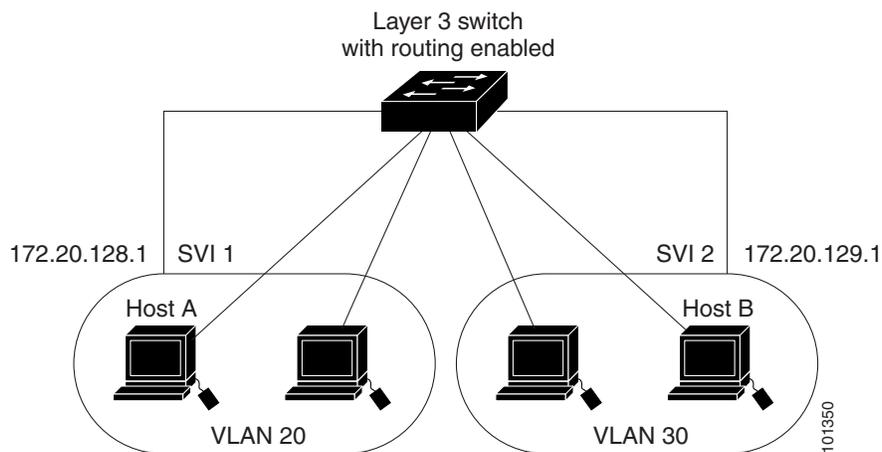
EtherChannel Port Groups

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.

media-type

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)#
```



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

Step 3

no shutdown

no shutdown

Step 4

Step 5

Configuring a Range of Interfaces

	Command	Purpose
Step 1		
Step 2		<ul style="list-style-type: none">•••
Step 3		
Step 4		
Step 5		
Step 6	[]	Verify the configuration of the interfaces in the range.
Step 7		

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

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

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

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

<i>interface-range</i>	<i>macro_name</i>
	<i>macro_name</i>
	<i>interface-range</i>

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

running-config

interface vlan

show

show running-config

```

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*

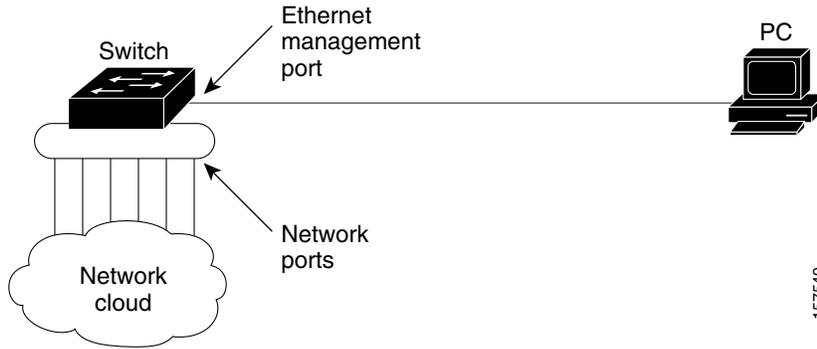
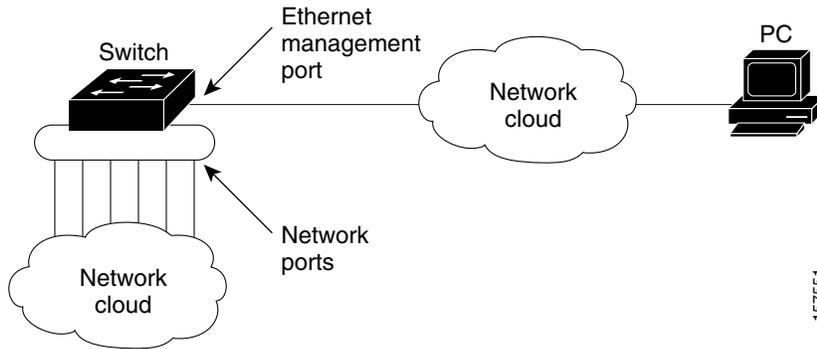


Figure 10-3 *Network Example with Routing Protocols Enabled*



Supported Features on the Ethernet Management Port

-
-
-
-
-
-
-
-
-
-
-
-
-
-
-



Configuring the Ethernet Management Port

TFTP and the Ethernet Management Port



Table 1 **Boot Loader Commands**

	Description
	without the <code>arp</code> parameter. Enables ARP to associate a MAC address with the specified IP address when this command is entered with the <code>ip</code> 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 <code>:/file-url</code>	Sends ICMP ECHO_REQUEST packets to the specified network host.
tftp: <code>/source-file-url</code> <code>filesystem destination-file-url</code>	

1. ARP = Address Resolution Protocol.

Configuring Ethernet Interfaces

-
-
-
-
-
-
-

Default Ethernet Interface Configuration



Note

Default Ethernet Configuration for UNIs and ENIs (continued)

	receive off



keepalive

keepalive

no keepalive



	Command	Purpose
Step 1		
Step 2		
Step 3		
Step 4	}	Change a port to an ENI, NNI, or UNI.
Step 5		Return to privileged EXEC mode.
Step 6		Verify the interface IEEE 802.3x flow control settings.
Step 7		(Optional) Save your entries in the configuration file.

```

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

```

Configuring Interface Speed and Duplex Mode

-
-

Speed and Duplex Configuration Guidelines

-



- 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 (`no speed`) 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 `no speed`.

On a 100BASE-FX SFP module, you cannot configure the speed as `no speed`.

- 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 `full` or `half`. Half-duplex mode is supported with the `duplex` setting.

When a Cisco100BASE-FX SFP module is in the SFP module slot, you can configure duplex mode to `full` or `half`. Although the `duplex` 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 `duplex` 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



Note

	Command	Purpose
Step 1		
Step 2		
Step 3		

Command	Purpose
Step 8	

```
no duplex
```

```
default
```

```
interface
```

```
duplex half
```

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

Configuring a Dual-Purpose Port



Note

```
system mtu jumbo
```



```
media-type  
auto-select
```

<code>configure terminal</code>	
<code>interface</code>	

media-type auto-select rj45 sfp

auto-select

rj45

sfp

end

**show interfaces
transceiver properties**

copy running-config startup-config

no media-type

auto-select

speed duplex

sfp rj45

auto-select



shutdown

no shutdown

media-type

Configuring IEEE 802.3x Flow Control


Note

-
-


Note

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

Configuring Auto-MDIX on an Interface

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		

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

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: `show ip interface`, `show interface`, and `show running-config`.

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

	Command	Purpose
Step 1		
Step 2		
Step 3		
Step 4		
Step 5		
Step 6		

Use the `no description` 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

.

	Command	Purpose
Step 8		
Step 9		

```
ip address 192.20.135.21 255.255.255.0
```

Configuring the System MTU


Note


Note

-
-



Note

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

```
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 [<i>interface-id</i>] <i>number</i>	<i>interface-id-</i> detail- dom-supported-list- module <i>number-</i> properties- threshold-table-
show port-type eni nni	
<i>interface-id</i>	
<i>interface-id</i>	

Table 10-6 Clear Commands for Interfaces



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 counters` 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:

	Enter global configuration mode.
<code>{ <i>vlan-id</i> { <i>interface-id</i> { <i>port-channel-number</i> } } }</code>	Select the interface to be configured.
	Shut down an interface.
	Return to privileged EXEC mode.
	Verify your entry.

Use the `shutdown` interface configuration command to enable an interface.

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

