CHAPTER 13

Configuring Interface Characteristics

This chapter defines the types of interfaces on the IE 3000 switch and describes how to configure them.

The chapter consists of these sections:

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

Understanding Interface Types

Port-Based VLANs

Chapter 15, "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 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 normal-range VLANs (VLAN IDs 1 to 1005), use the **vlan** *vlan-id* **vlan database** privileged EXEC command to enter VLAN database configuration mode. The VLAN configurations for VLAN IDs 1 to 1005 are saved in the VLAN database. To configure extended-range VLANs (VLAN IDs 1006 to 4094), you must use config-vlan mode with VTP mode set to transparent. Extended-range VLANs are not added to the VLAN database. When VTP mode is transparent, the VTP and 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**

switchport

Switch Ports

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.

Configure switch ports by using the interface configuration commands.

For detailed information about configuring access port and trunk port characteristics, see Chapter 15, "Configuring VLANs."

Access Ports

packet (IEEE 802.1Q tagged), the packet is dropped, and the source address is not learned.

Two types of access ports are supported:

- Static access ports are manually assigned to a VLAN (or through a RADIUS server for use with IEEE 802.1x. For more information, see the "802.1x Authentication with VLAN Assignment" section on page 12-14.)

  VLAN membership of dynamic access ports is learned through incoming packets. By default, a dynamic access port is not a member of any VLAN, and forwarding to and from the port is enabled only when the VLAN membership of the port is discovered. Dynamic access ports on the switch are assigned to a VLAN by a VLAN Membership Policy Server (VMPS). The VMPS can be a Catalyst 6500 series switch; the IE 3000 switch cannot be a VMPS server.

You can also configure an access port with an attached Cisco IP Phone to use one VLAN for voice traffic and another VLAN for data traffic from a device attached to the phone. For more information about voice VLAN ports, see Chapter 17, "Configuring Voice VLAN."

Trunk Ports

Only IEEE 802.1Q trunk ports are 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.

For more information about trunk ports, see Chapter 15, "Configuring VLANs."

EtherChannel Port Groups

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. 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 38, "Configuring EtherChannels and Link-State Tracking."

Dual-Purpose Uplink Ports

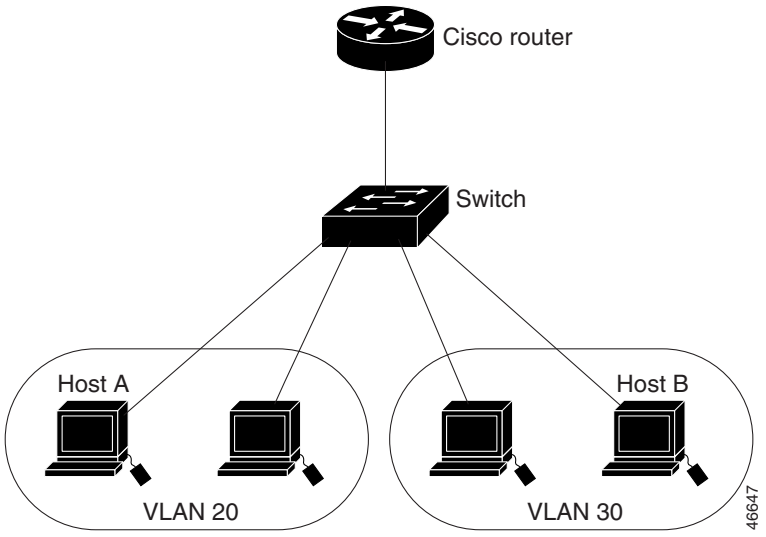
interface with dual front ends—an RJ-45 connector and a small form-factor pluggable (SFP) module connector. The dual front ends are not redundant interfaces, and the switch activates only one connector of the pair.

By default, the switch dynamically selects the interface type that first links up. However, you can use the interface configuration command to manually select the RJ-45 connector or the SFP module connector. For information about configuring speed and duplex settings for a dual-purpose uplink, see the "Setting the Interface Speed and Duplex Parameters" section on page 13-14.

Each uplink port has two LEDs: one shows the status of the RJ-45 port, and one shows the status of the SFP module port. The port LED is on for whichever connector is active. For more information about the LEDs, see the hardware installation guide.

Connecting Interfaces

Figure 13-1 Connecting VLANs with Layer 2 Switches



Using Interface Configuration Mode

-
-
-

Fast Ethernet (fastethernet or fa) for 10/100 Mb/s Ethernet, Gigabit Ethernet (gigabitethernet or gi) for 10/100/1000 Mb/s Ethernet ports, or small form-factor pluggable (SFP) module Gigabit Ethernet interfaces.

Module number—The module number on the switch. The module number (1 to 3) depends on how the module is connected to the switch or to other modules.

–

–

–

switch model are 1–4 for the Fast Ethernet ports and 1–2 for the Gigabit Ethernet ports. The port numbers for the IE-3000-8TC switch model are 1–8 for the Fast Ethernet ports and 1–2 for the Gigabit Ethernet ports. Table 13-1 shows the switch and module combinations and the interface numbers.

Table 13-1 Switch Interface Numbers

Switch Model	Module Number	Interface Numbering Scheme

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

Step 1

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

Step 2

```
Switch(config)#           gigabitethernet1/1
Switch(config-if)#
```

gigabitethernet 1/1 gigabitethernet1/1 gi 1/1 gi1/1

Step 3

Step 4

Configuring a Range of Interfaces

	Command	Purpose
Step 1		
Step 2	| *macro_name*	*port-range* *port-range*
Step 5	[ ]	Verify the configuration of the interfaces in the range.
Step 6		(Optional) Save your entries in the configuration file.

port-range

vlan-ID

stack member/module/{first *port*} - { }, where the module is always 0

module/{ } - { }

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

```
interface range gigabitethernet1/1 - 2
         speed 100
```

```
configure terminal
        interface range fastethernet1/1 - 3, gigabitethernet1/1 - 2
                 flowcontrol receive on
```

Configuring and Using Interface Range Macros

	Command	Purpose
Step 1		
Step 2		• • •
Step 3		
Step 4		
Step 5	show running-config | include define	
	copy running-config startup-config	

•

/1 - 4 fastethernet /1-4

interface vlan show running-config

show running-config

```
        define interface-range enet_list gigabitethernet1/1 - 2
        end
show running-config | include define
define interface-range enet_list gigabitethernet1/1 - 2
```

```
configure terminal
        define interface-range macro1 fastethernet1/1 - 2, gigabitethernet1/1 - 2
        end
```

```
configure terminal
        interface range macro enet_list
```

```
configure terminal
        no define interface-range enet_list
        end
show run | include define
```

Configuring Ethernet Interfaces

-
-
-
-
-
-

Default Ethernet Interface Configuration

Default Layer 2 Ethernet Interface Configuration

Feature	Default Setting

Default Layer 2 Ethernet Interface Configuration (continued)

	Note
Keepalive messages	Disabled on SFP module ports; enabled on all other ports.

Setting the Type of a Dual-Purpose Uplink Port

rj45 sfp	
	auto-select
	rj45
	sfp
end	
show interfaces transceiver properties	
copy running-config startup-config	

duplex

shutdown

no shutdown

x *x*

x

x

x

Configuring Interface Speed and Duplex Mode

-
-

Speed and Duplex Configuration Guidelines

-
-
-

  is -BX, -CWDM, -LX, -SX, and -ZX) SFP module ports support the keyword in the interface configuration command. Duplex options are not supported.

  The 1000BASE-T SFP module ports support the same speed and duplex options as the 10/100/1000-Mb/s ports.

  The 100BASE- (where - is -BX, -CWDM, -LX, -SX, and -ZX) SFP module ports support only 100 Mb/s. These modules support full- and half- duplex options but do not support autonegotiation.

  For information about which SFP modules are supported on your switch, see the product release notes.
- 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.

Caution

Setting the Interface Speed and Duplex Parameters

	Command	Purpose
Step 1		
Step 2		
Step 3	10 | 100 | 1000 | auto 10 100 1000 | nonegotiate	10 100 1000 1000 auto 10 100 1000 auto nonegotiate
	duplex auto | full | half	
	end	
	show interfaces	
Step 7		

```
duplex half
```

```
configure terminal
        interface gigabitethernet1/2
           speed 100
```

Configuring IEEE 802.3x Flow Control

Note

interface configuration command to set the interface's ability to pause frames to , , or . The default state is .

When set to , 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:

- (or): 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.
- : 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 interface configuration command in the command reference for this release.

Beginning in privileged EXEC mode, follow these steps to configure flow control on an interface:

	Command	Purpose
Step 1		Enter global configuration mode.
Step 2		Specify the physical interface to be configured, and enter interface configuration mode.
Step 3	{ } { | | }	Configure the flow control mode for the port.
Step 4		Return to privileged EXEC mode.
Step 5		Verify the interface flow control settings.
Step 6		(Optional) Save your entries in the configuration file.

To disable flow control, use the interface configuration command.

This example shows how to turn on flow control on a port:

Configuring Auto-MDIX on an Interface

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		

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:

	Enter global configuration mode.
	Specify the interface for which you are adding a description, and enter interface configuration mode.
	Add a description (up to 240 characters) for an interface.
	Return to privileged EXEC mode.
or	Verify your entry.
	(Optional) Save your entries in the configuration file.

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 gigabitethernet1/2 description
Interface Status         Protocol Description
Gi1/2   admin down     down     Connects to Marketing
```

Configuring the System MTU

jumbo frames on all Gigabit Ethernet interfaces by using the global configuration command.

Gigabit Ethernet ports are not affected by the command; 10/100 ports are not affected by the command. If you do not configure the command, the setting of the command applies to all Gigabit Ethernet interfaces.

You cannot set the MTU size for an individual interface; you set it for all 10/100 or all Gigabit Ethernet interfaces on the switch. When you change the system or jumbo MTU size, you must reset the switch before the new configuration takes effect.

Frames sizes that can be received by the switch CPU are limited to 1998 bytes, no matter what value was entered with the or commands. Although frames that are forwarded are typically not received by the CPU, in some cases packets are sent to the CPU, such as traffic sent to control traffic, SNMP, or Telnet.

If Gigabit Ethernet interfaces are configured to accept frames greater than the 10/100 interfaces, jumbo frames received on a Gigabit Ethernet interface and sent on a 10/100 interface are dropped.

Beginning in privileged EXEC mode, follow these steps to change MTU size for all 10/100 or Gigabit Ethernet interfaces:

bytes	
bytes	

If you enter a value that is outside the allowed range for the specific type of interface, the value is not accepted.

Once the switch reloads, you can verify your settings by entering the privileged EXEC command.

This example shows how to set the maximum packet size for a Gigabit Ethernet port to 1800 bytes:

```
                system mtu jumbo 1800
                exit
        reload




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

show ?

Documentation Cisco IOS Software 12.2 Mainline Command References

Table 13-4 Show Commands for Interfaces

clear

Table 13-5 Clear Commands for Interfaces

vlan-id *interface-id* *port-channel-number*	

administratively down