CHAPTER 7

Configuring the Switch Ports

This chapter provides information about changing port configuration settings. It includes command-line interface (CLI) procedures for using commands that have been specifically created or changed for the Catalyst 2900 XL or Catalyst 3500 XL switches. For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 2900 Series XL and Catalyst 3500 Series XL Command Reference*.

Note Certain port features can conflict with one another. Review the "Avoiding Configuration Conflicts" section on page 9-2 before you change the port settings.

This chapter does not repeat the concepts and CLI procedures provided in the standard Cisco IOS Release 12.0 documentation. For switch features that use standard Cisco IOS Release 12.0 commands, refer to the Cisco IOS Release 12.0 documentation on Cisco.com for additional information and CLI procedures.

For information about configuring these settings from Cluster Management Suite (CMS), refer to the online help.

Note Some features can be implemented only by using the CLI.

Changing the Port Speed and Duplex Mode

Caution If you reconfigure the port through which you are managing the switch, a Spanning Tree Protocol (STP) reconfiguration could cause a temporary loss of connectivity.

Note The Ethernet link settings on the Long-Reach Ethernet (LRE) ports have special considerations and different default settings than from the 10/100 ports. For this information, see the "LRE Ethernet Links" section on page 7-25.

Follow these guidelines when configuring the duplex and speed settings:

- Gigabit Ethernet ports are always set to 1000 Mbps but can negotiate full or half duplex with the attached device.
- Gigabit Ethernet ports that do not match the settings of an attached device lose connectivity and do not generate statistics.
- Asynchronous Transfer Mode (ATM) ports are always set to full duplex and do not autonegotiate duplex or speed settings.
- GigaStack-to-GigaStack stack connections operate in half-duplex mode, and GigaStack-to-GigaStack point-to-point connections operate in full-duplex mode.
- If STP is enabled, the switch can take up to 30 seconds to check for loops when a port is reconfigured. The port LED is amber while STP reconfigures.

Connecting to Devices That Do Not Autonegotiate

To connect to a remote 100BASE-T device that does not autonegotiate, set the duplex setting to **Full** or **Half**, and set the speed setting to **Auto**. Autonegotiation for the speed setting selects the correct speed even if the attached device does not autonegotiate, but the duplex setting must be explicitly set.

To connect to a remote Gigabit Ethernet device that does not autonegotiate, disable autonegotiation on the local device, and set the duplex and flow control parameters to be compatible with the other device.

Setting Speed and Duplex Parameters

Beginning in privileged EXEC mode, follow these steps to set the speed and duplex parameters on a port:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface*	Enter interface configuration mode, and enter the port to be configured.
Step 3	**speed** {**10** | **100** | **auto**}	Enter the speed parameter for the port. You cannot enter the speed on Gigabit Ethernet or ATM ports.
Step 4	**duplex** {**full** | **half** | **auto**}	Enter the duplex parameter for the port.
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**show running-config**	Verify your entries.
Step 7	**copy running-config startup-config**	(Optional) Save your entry in the configuration file. This retains the configuration when the switch restarts.

Configuring Flow Control on Gigabit Ethernet Ports

Beginning in privileged EXEC mode, follow these steps to configure flow control on a Gigabit Ethernet port.

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface*	Enter interface configuration mode, and enter the port to be configured.
Step 3	**flowcontrol** [**asymmetric** | **symmetric**]	Configure flow control for the port.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show running-config**	Verify your entries.
Step 6	**copy running-config startup-config**	(Optional) Save your entry in the configuration file. This retains the configuration when the switch restarts.

Configuring Flooding Controls

You can use the following flooding techniques to block the forwarding of unnecessary flooded traffic:

- Enable storm control for unicast, multicast, or broadcast packets
- Block the forwarding of unicast and broadcast packets on a per-port basis
- Flood all unknown packets to a network port (configured only by using CLI)

Enabling Storm Control

A packet storm occurs when a large number of broadcast, unicast, or multicast packets are received on a port. Forwarding these packets can cause the network to slow down or to time out. Storm control is configured for the switch as a whole but operates on a per-port basis. By default, storm control is disabled.

Storm control uses high and low thresholds to block and then restore the forwarding of broadcast, unicast, or multicast packets. You can also set the switch to shut down the port when the rising threshold is reached.

The rising threshold is the number of packets that a switch port can receive before forwarding is blocked. The falling threshold is the number of packets below which the switch resumes normal forwarding. In general, the higher the threshold, the less effective the protection against broadcast storms. The maximum half-duplex transmission on a 100BASE-T link is 148,000 packets per second, but you can enter a threshold of up to 4294967295 broadcast packets per second.

With the exception of the **broadcast** keyword, the following procedure could also be used to enable storm control for unicast or multicast packets.

Beginning in privileged EXEC mode, follow these steps to enable broadcast-storm control.

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface*	Enter interface configuration mode, and enter the port to configure.
Step 3	**port storm-control broadcast** [**threshold** {**rising** *rising-number* **falling** *falling-number*}]	Enter the rising and falling thresholds for broadcast packets. Make sure the rising threshold is greater than the falling threshold.
Step 4	**port storm-control trap**	Generate an SNMP trap when the traffic on the port crosses the rising or falling threshold.
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**show port storm-control** [*interface*]	Verify your entries.

Disabling Storm Control

Beginning in privileged EXEC mode, follow these steps to disable broadcast-storm control.

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface*	Enter interface configuration mode, and enter the port to configure.
Step 3	**no port storm-control broadcast**	Disable port storm control.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show port storm-control** [*interface*]	Verify your entries.

Blocking Flooded Traffic on a Port

By default, the switch floods packets with unknown destination MAC addresses to all ports. Some configurations do not require flooding. For example, a port that has only manually assigned addresses has no unknown destinations, and flooding serves no purpose. Therefore, you can disable the flooding of unicast and multicast packets on a per-port basis. Ordinarily, flooded traffic does not cross VLAN boundaries, but multi-VLAN ports flood traffic to all VLANs they belong to.

Beginning in privileged EXEC mode, follow these steps to disable the flooding of multicast and unicast packets to a port:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface*	Enter interface configuration mode, and enter the port to configure.
Step 3	**port block multicast**	Block unknown multicast forwarding to the port.
Step 4	**port block unicast**	Block unknown unicast flooding to the port.
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**show port block** {**multicast** | **unicast**} *interface*	Verify your entries, entering the appropriate command once for the **multicast** option and once for the **unicast** option.

Resuming Normal Forwarding on a Port

Beginning in privileged EXEC mode, follow these steps to resume normal forwarding on a port:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface*	Enter interface configuration mode, and enter the port to configure.
Step 3	**no port block multicast**	Enable unknown multicast forwarding to the port.
Step 4	**no port block unicast**	Enable unknown unicast flooding to the port.
Step 5	**end**	Return to privileged EXEC mode
Step 6	**show port block** {**multicast** | **unicast**} *interface*	Verify your entries, entering the appropriate command once for the **multicast** option and once for the **unicast** option.

Enabling a Network Port

Network ports are assigned per VLAN and can reduce flooded traffic on your network. The switch forwards all traffic with unknown destination addresses to the network port instead of flooding the traffic to all ports in the VLAN.

When you configure a port as the network port, the switch deletes all associated addresses from the address table and disables learning on the port. If you configure other ports in the VLAN as secure ports, the addresses on those ports are not aged. If you move a network port to a VLAN without a network port, it becomes the network port for the new VLAN.

You cannot change the settings for unicast and multicast flooding on a network port. You can assign only one network port per VLAN. For the restrictions that apply to a network port, see the "Changing the Password" section on page 6-15.

Caution A network port cannot link cluster members.

Beginning in privileged EXEC mode, follow these steps to define a network port:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface*	Enter interface configuration mode, and enter the port to be configured.
Step 3	**port network**	Define the port as the network port.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show running-config**	Verify your entry.

Disabling a Network Port

Beginning in privileged EXEC mode, follow these steps to disable a network port:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface*	Enter interface configuration mode, and enter the port to be configured.
Step 3	**no port network**	Disable the port as the network port.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show running-config**	Verify your entry.

Configuring UniDirectional Link Detection

UniDirectional Link Detection (UDLD) is a Layer 2 protocol that detects and shuts down unidirectional links. You can configure UDLD on the entire switch or on an individual port. Use the **udld reset** command to reset all ports that have been shut down by UDLD.

Beginning in privileged EXEC mode, follow these steps to configure UDLD on a switch:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**udld enable**	Enable UDLD on all switch ports. Use the **udld** interface configuration command to enable UDLD on a specific port.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show running-config**	Verify the entry by displaying the running configuration.

Creating EtherChannel Port Groups

Fast EtherChannel (FEC) and Gigabit EtherChannel port groups act as single, logical ports for high-bandwidth connections between switches or between switches and servers.

Note You can create port groups of either Gigabit Ethernet ports or 100BASE-TX ports, but you cannot create a port group that has both port speeds.

For the restrictions that apply to port groups, see the "Avoiding Configuration Conflicts" section on page 9-2.

Understanding EtherChannel Port Grouping

This software release supports two different types of port groups: source-based forwarding port groups and destination-based forwarding port groups.

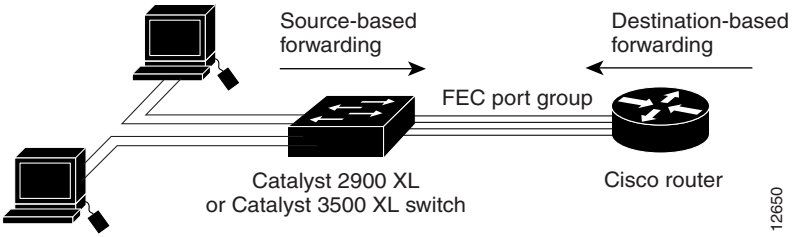
Source-based forwarding port groups distribute packets forwarded to the group based on the source address of incoming packets. You can configure up to eight ports in a source-based forwarding port group. Source-based forwarding is enabled by default.

Destination-based port groups distribute packets forwarded to the group based on the destination address of incoming packets. You can configure an unlimited number of ports in a destination-based port group.

You can create up to 12 port groups. All ports in each group must be of the same type; for example, they must be all source-based or all destination-based. You can have source-based port groups and destination-based source groups. You can independently configure port groups that link switches, but you must consistently configure both ends of a port group.

In Figure 7-1, a port group of two workstations communicates with a router. Because the router is a single-MAC-address device, source-based forwarding ensures that the switch uses all available bandwidth to the router. The router is configured for destination-based forwarding because the large number of stations ensures that the traffic is evenly distributed through the port-group ports on the router.

Figure 7-1 Source-Based Forwarding



The switch treats the port group as a single logical port; therefore, when you create a port group, the switch uses the configuration of the first port for all ports added to the group. If you add a port and change the forwarding method, it changes the forwarding for all ports in the group. After the group is created, changing STP or VLAN membership parameters for one port in the group automatically changes the parameters for all ports. Each port group has one port that carries all unknown multicast, broadcast, and STP packets.

Port Group Restrictions on Static-Address Forwarding

The following restrictions apply to entering static addresses that are forwarded to port groups:

- If the port group forwards based on the source MAC address (the default), configure the static address to forward to all ports in the group. This method eliminates the chance of lost packets.
- If the port group forwards based on the destination address, configure the static address to forward to only one port in the port group. This method avoids the possible transmission of duplicate packets. For more information, see the "Adding Static Addresses" section on page 6-59.

Creating EtherChannel Port Groups

Beginning in privileged EXEC mode, follow these steps to create a two-port group:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface*	Enter interface configuration mode, and enter the port of the first port to be added to the group.
Step 3	**port group 1 distribution destination**	Assign the port to group 1 with destination-based forwarding.
Step 4	**interface** *interface*	Enter the second port to be added to the group.
Step 5	**port group 1 distribution destination**	Assign the port to group 1 with destination-based forwarding.
Step 6	**end**	Return to privileged EXEC mode.
Step 7	**show running-config**	Verify your entries.

Configuring Protected Ports

Some applications require that no traffic be forwarded by the Layer 2 protocol between ports on the same switch. In such an environment, there is no exchange of unicast, broadcast, or multicast traffic between ports on the switch, and traffic between ports on the same switch is forwarded through a Layer 3 device such as a router.

To meet this requirement, you can configure Catalyst 2900 XL and Catalyst 3500 XL ports as protected ports (also referred to as private VLAN edge ports). Protected ports do not forward any traffic to protected ports on the same switch. This means that all traffic passing between protected ports—unicast, broadcast, and multicast—must be forwarded through a Layer 3 device. Protected ports can forward any type of traffic to nonprotected ports, and they forward as usual to all ports on other switches.

Note Sometimes unknown unicast traffic from a nonprotected port is flooded to a protected port because a MAC address has timed out or has not been learned by the switch. Use the **port block** command to guarantee that in such a case no unicast and multicast traffic is flooded to the port. See the "Configuring Flooding Controls" section on page 7-4 for more information.

Beginning in privileged EXEC mode, follow these steps to define a port as a protected port:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface*	Enter interface configuration mode, and enter the port to be configured.
Step 3	**port protected**	Enable protected port on the port.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show port protected**	Verify that the protected port option is enabled.

Use the **no** version of the **port protected** interface configuration command to disable the protected port option.

Enabling Port Security

Secured ports restrict a port to a user-defined group of stations. When you assign secure addresses to a secure port, the switch does not forward any packets with source addresses outside the group of addresses you have defined. If you define the address table of a secure port to contain only one address, the workstation or server attached to that port is guaranteed the full bandwidth of the port. As part of securing the port, you can also define the size of the address table for the port.

Secured ports generate address-security violations under the following conditions:

- The address table of a secured port is full and the address of an incoming packet is not found in the table.
- An incoming packet has a source address assigned as a secure address on another port.

Limiting the number of devices that can connect to a secure port has the following advantages:

- Dedicated bandwidth—If the size of the address table is set to 1, the attached device is guaranteed the full bandwidth of the port.
- Added security—Unknown devices cannot connect to the port.

The following options validate port security or indicate security violations:

Interface	Port to secure.
Security	Enable port security on the port.
Trap	Issue a trap when an address-security violation occurs.
Shutdown Port	Disable the port when an address-security violation occurs.
Secure Addresses	Number of addresses in the address table for this port. Secure ports have at least one address.
Max Addresses	Number of addresses that the address table for the port can contain.
Security Rejects	The number of unauthorized addresses seen on the port.

For the restrictions that apply to secure ports, see the "Avoiding Configuration Conflicts" section on page 9-2.

Defining the Maximum Secure Address Count

A secure port can have from 1 to 132 associated secure addresses. Setting one address in the MAC address table for the port ensures that the attached device has the full bandwidth of the port.

Enabling Port Security

Beginning in privileged EXEC mode, follow these steps to enable port security.

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface*	Enter interface configuration mode for the port you want to secure.
Step 3	**port security max-mac-count 1**	Secure the port and set the address table to one address.
Step 4	**port security action shutdown**	Set the port to shutdown when a security violation occurs.
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**show port security**	Verify the entry.

Disabling Port Security

Beginning in privileged EXEC mode, follow these steps to disable port security.

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface*	Enter interface configuration mode for the port you want to unsecure.
Step 3	**no port security**	Disable port security.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show port security**	Verify the entry.

Enabling SPAN

You can use Switch Port Analyzer (SPAN) to monitor traffic on a given port by forwarding incoming and outgoing traffic on the port to another port in the same VLAN. A SPAN port cannot monitor ports in a different VLAN, and a SPAN port must be a static-access port. You can define any number of ports as SPAN ports, and any combination of ports can be monitored.

For the restrictions that apply to SPAN ports, see the "Avoiding Configuration Conflicts" section on page 9-2.

Beginning in privileged EXEC mode, follow these steps to enable SPAN:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface*	Enter interface configuration mode, and enter the port that acts as the monitor port.
Step 3	**port monitor** *interface*	Enable port monitoring on the port.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show running-config**	Verify your entries.

Disabling SPAN

Beginning in privileged EXEC mode, follow these steps to disable SPAN:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface*	Enter interface configuration mode, and enter the port number of the monitor port.
Step 3	**no port monitor** *interface*	Disable port monitoring on the port.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show running-config**	Verify your entries.

Configuring Voice Ports

The Catalyst 2900 XL and Catalyst 3500 XL switches can connect to a Cisco 7960 IP Phone and carry IP voice traffic. If necessary, the Catalyst 3524-PWR XL can supply electrical power to the circuit connecting it to the Cisco 7960 IP Phone.

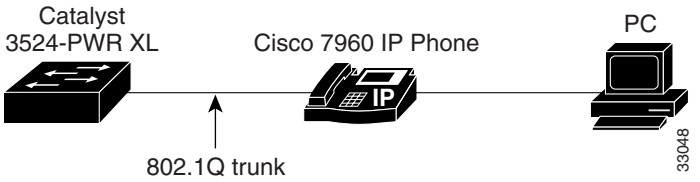
Because the sound quality of an IP telephone call can deteriorate if the data is unevenly transmitted, this release of IOS supports quality of service (QoS) based on IEEE 802.1p class of service (CoS). QoS uses classification and scheduling to transmit network traffic from the switch in a predictable manner. The Cisco 7960 IP Phone itself is also a configurable device, and you can configure it to forward traffic with an 802.1p priority. You can use the CLI to configure the Catalyst 3524-PWR XL to honor or ignore a traffic priority assigned by a Cisco 7960 IP Phone.

The Cisco 7960 IP Phone contains an integrated three-port 10/100 switch. The ports are dedicated connections to the following devices:

- Port 1 connects to the Catalyst 3524-PWR XL switch or other voice-over-IP device.
- Port 2 is an internal 10/100 interface that carries the phone traffic.
- Port 3 connects to a PC or other device.

Figure 7-2 shows one way to configure a Cisco 7960 IP Phone.

Figure 7-2 Cisco 7960 IP Phone Connected to a Catalyst 3524-PWR XL Switch



Preparing a Port for a Cisco 7960 IP Phone Connection

Before you configure a Catalyst 3524-PWR XL port to carry IP voice traffic, configure the port as an 802.1Q trunk and as a member of the voice VLAN (VVID). See the "Configuring a Trunk Port" section on page 8-38 for instructions.

Configuring a Port to Connect to a Cisco 7960 IP Phone

Because a Cisco 7960 IP Phone also supports connection to a PC or other device, a port connecting a Catalyst 3524-PWR XL switch to a Cisco 7960 IP Phone can carry mixed traffic. There are three configurations for a port connected to a Cisco 7960 IP Phone:

- All traffic is transmitted according to the default COS priority of the port. This is the default.
- Voice traffic is given a higher priority by the phone, and all traffic is in the same VLAN.
- Voice and data traffic are carried on separate VLANs, and voice traffic always has a CoS priority of 5.

Beginning in privileged EXEC mode, follow these steps to configure a port to instruct the phone to give voice traffic a higher priority and to forward all traffic through the 802.1Q native VLAN.

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface*	Enter interface configuration mode, and enter the port to be configured.
Step 3	**switchport voice vlan dot1p**	Instruct the switch to use 802.1p priority tagging for voice traffic and to use VLAN 0 (default native VLAN) to carry all traffic.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show interface** *interface* **switchport**	Verify the port configuration.

Overriding the CoS Priority of Incoming Frames

A PC or other data device can connect to a Cisco 7960 IP Phone port. The PC can generate packets with an assigned CoS value. If you want, you can use the Catalyst 3524-PWR XL CLI to override the priority of frames arriving on the phone port from connected devices. You can also set the phone port to accept (trust) the priority of frames arriving on the port.

Beginning in privileged EXEC mode, follow these steps to override the CoS priority setting received from the non-voice port on the Cisco 7960 IP Phone:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface*	Enter interface configuration mode, and enter the switch port to be configured.
Step 3	**switchport priority extend cos 3**	Set the phone port to override the priority received from the PC or the attached device and forward the received data with a priority of 3.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show interface** *interface* **switchport**	Verify the change.

Use the **no switchport priority extend** command to return the port to its default setting.

Configuring Voice Ports to Carry Voice and Data Traffic on Different VLANs

The Cisco 7960 IP Phone has an integrated three-port 10/100 switch that can connect to a PC or other device. You can configure a switch port to instruct the phone to forward voice and data traffic on different virtual LANs (VLANs).

In the following configuration, VLAN 1 carries data traffic, and VLAN 2 carries voice traffic. In this configuration, you must connect all Cisco IP Phones and other voice-related devices to switch ports that belong to VLAN 2.

Beginning in privileged EXEC mode, follow these steps to configure a port to receive voice and data from a Cisco IP Phone in different VLANs:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface*	Enter interface configuration mode, and enter the port to be configured.
Step 3	**switchport priority default (0)**	Assign an IEEE 802.1p priority to untagged traffic that is received on the switch port. The Cisco IP Phone forwards this traffic through the native VLAN, VLAN 1.
Step 4	**switchport voice vlan (2)**	Instruct the Cisco IP Phone to forward all voice traffic through VLAN 2. The Cisco IP Phone forwards the traffic with an 802.1p priority of 5.
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**show interface** *interface* **switchport**	Verify the configuration.

Configuring Inline Power on the Catalyst 3524-PWR Ports

The Catalyst 3524-PWR XL can supply inline power to the Cisco 7960 IP Phone, if necessary. The Cisco 7960 IP Phone can also be connected to an AC power source and supply its own power to the voice circuit. When the Cisco 7960 IP Phone supplies its own power, any Catalyst 2900 XL or Catalyst 3500 XL can forward IP voice traffic to and from the phone.

The Catalyst 3524-PWR XL senses if it is connected to a Cisco 7960 IP Phone. If there is *no* power on the circuit, the switch supplies the power. If there is power on the circuit, the switch does not supply it.

You can configure the switch to never supply power to the Cisco 7960 IP Phone and to disable the detection mechanism. See the "Configuring Voice Ports" section on page 7-17 for the CLI commands that you use to supply inline power to a Cisco 7960 IP Phone.

Beginning in privileged EXEC mode, follow these steps to configure a port to never supply power to Cisco 7960 IP Phones.

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface*	Enter interface configuration mode, and enter the port to be configured.
Step 3	**power inline never**	Permanently disable inline power on the port. To enable inline power when a Cisco 7960 IP Phone is detected, use the **power inline auto** command.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show power inline** *interface* **configured**	Verify the change.

Configuring the LRE Ports

The Catalyst 2900 LRE XL switches use Long-Reach Ethernet (LRE) technology to transfer data and voice traffic over existing standard telephone lines. Connecting a switch LRE switch port to a remote Ethernet device requires two types of connections:

- LRE link—This is the connection between the switch LRE port and the WALL port on the Cisco 575 LRE customer premises equipment (CPE). This connection can be through a standard telephone line (categorized and noncategorized unshielded twisted-pair cable) and can extend to distances of up to 4921 ft (1500 m).
- Ethernet link—This is the connection between the 10/100 Ethernet port on the CPE and an Ethernet device, such as a PC. This connection is through standard Category 5 cabling and can extend to distances of up to 328 ft (100 m).

The actual link rate between an LRE port and a remote Ethernet device, in either direction, depends on the active profile for the LRE port and the Ethernet link speed. For example, if a PC Ethernet port is configured to 100 Mbps and the LRE port is configured with an upstream link rate of 5.69 Mbps, the actual upload rate provided to the PC user is 5.69 Mbps, not 100 Mbps. Conversely, if the PC Ethernet port is configured to 10 Mbps and the LRE port is configured with an upstream link rate of 17.06 Mbps, the actual upload rate provided to the PC user is 17.06 Mbps.

LRE Links and LRE Profiles

The LRE link settings on the LRE ports define the connection between the switch LRE port and the WALL port on the Cisco 575 LRE CPE. The LRE link provides symmetric and asymmetric bandwidth for voice and data traffic. Symmetrical transmission is when the downstream and upstream bandwidth are the same. Asymmetrical transmission is when the downstream and the upstream bandwidth differ. Downstream transmission refers to the data traveling from the LRE port to the CPE. Upstream transmission refers to the data traveling from the CPE to the LRE port.

Bandwidth within the LRE link is controlled by the switch by using configurations called *profiles*. An LRE profile configures the upstream and downstream rates on the LRE link. Depending on the profile, the upstream and downstream bands on an LRE link can be approximately 5, 10, or 15 Mbps.

You can assign profiles on a per-port or switch-wide basis. When the LRE port establishes a link with the CPE, the switch downloads its profile settings to the CPE port so that both ports on both devices operate with the same configuration.

The Catalyst 2900 LRE XL switches are shipped with predefined profiles (Table 7-1) categorized as public (global) mode and private (per-port) mode profiles. By default, all LRE ports on the switch are enabled with the LRE-10 private profile in effect.

- Public—We strongly recommend using a public profile if the switch is used with equipment connected to a Public Switched Telephone Network (PSTN). When the switch is configured with a public profile, all LRE ports use the same configuration to prevent the switch from causing interference with the other lines on the PSTN.

  The standards for spectral profiles have not yet been ratified. The PUBLIC-ANSI profile corresponds to ANSI Plan 998. The PUBLIC-ETSI profile corresponds to ETSI Plan 997. Both plans are draft standards. Contact Cisco Systems for the latest information about standards ratification or for updates to the public profiles.

- Private—You can use a private profile if the LRE switch is not used with equipment connected to a PSTN. Three private profiles offer different link speeds and maximum distances. In general, the higher the link speed, the shorter the maximum distance. Private profiles are assigned on a per-port basis. The ports on an LRE switch can be assigned the same or different private profiles.

Note Use the rates and distances in Table 7-1 as guidelines only. Factors such as the type of cable you use, how it is bundled, and the interference and noise on the LRE link can affect the actual LRE link performance. Contact Cisco Systems for information about limitations and optimization of LRE link performance.

The net data rates in Table 7-1 are slightly less than the gross data rates displayed by the **show controllers lre profile names** privileged EXEC command.

Table 7-1 LRE Profiles

Profile Name	Profile Type	LRE Link Downstream Rate (Mbps)	LRE Link Upstream Rate (Mbps)	Maximum Distance between the LRE Port and the CPE
PUBLIC-ANSI	Public	15.17	4.27	4101 ft (1250 m)
PUBLIC-ETSI	Public	11.38	4.27	4101 ft (1250 m)
LRE-5	Private	5.69	5.69	4921 ft (1500 m)
LRE-10 (default)	Private	11.38	11.38	4101 ft (1250 m)
LRE-15	Private	15.17	17.06	3445 ft (1050 m)

When assigning a profile to an LRE port, keep the following considerations in mind:

- An LRE port always has a private profile assigned to it. However, public profiles have priority over private profiles.

  If you assign a public profile to the switch, the switch ignores the private profile settings and uses the public profile settings on all LRE ports. If you assign a different public profile, the change immediately takes effect.

  If a public profile is configured on the switch and you want the LRE ports to use private profiles, you must first disable the public profile by using CMS or by using the **no lre profile global** global configuration command.

  If no public profile is configured on the switch, the LRE port uses its private profile. If you assign a different private profile to the LRE port, the change immediately takes effect.

- A configuration conflict occurs if a switch cluster has LRE switches using both private and public profiles. If one LRE switch in a cluster is assigned a public profile, all LRE switches in that cluster must have that same public profile. Before you add an LRE switch to a cluster, make sure that you assign it the same public profile used by other LRE switches in the cluster.

  A cluster can have a mix of LRE switches using different private profiles.

  For more information about clusters, see Chapter 5, "Clustering Switches."

Use the **show controllers lre** privileged EXEC commands to display the LRE link statistics and profile information on the LRE ports. For information about these commands, refer to the *Catalyst 2900 Series XL and Catalyst 3500 Series XL Command Reference*.

LRE Ethernet Links

The Ethernet link settings on the LRE ports are for configuring the remote CPE Ethernet port, and they define the connection between the Ethernet port on the Cisco 575 LRE CPE and an Ethernet device such as a PC or a television set-top box. You can set the CPE Ethernet port to operate at 10 or 100 Mbps and at half- or full-duplex mode, depending on the capability of the remote Ethernet device. Autonegotiation for port speed and duplex mode is supported. The default speed for the CPE Ethernet port is auto; the default duplex mode is half duplex.

When configuring the Ethernet link on the LRE ports, keep in mind the following guidelines:

- The speeds on the LRE and Ethernet links do not need to match. However, to prevent the possible loss of data when the LRE link is configured to be slower than the Ethernet link, choose one of the following:
  - Configure the LRE port to use half-duplex mode, which is the default.
  - Use duplex autonegotiation or full-duplex mode only if the remote device supports 802.1x full-duplex flow control.

Note You cannot configure the flow control setting on the LRE ports. The flow control setting on the remote CPE Ethernet port is automatically disabled on LRE ports in half-duplex mode, and is automatically enabled on LRE ports in full-duplex mode.

The PC user should notice no significant difference in performance between 100-Mbps half duplex and 100-Mbps full duplex.

- Enable CDP either globally on the LRE switch or on the specific LRE ports.
- The switch 10/100 port defaults are not the same as the defaults for the Ethernet link on the LRE ports.

Note We recommend that you use the **lre shutdown** interface configuration command to disable the LRE chipset transmitter on any LRE ports that are not connected to a CPE. This prevents access to the LRE port and prevents the power emitted from the port from affecting other ports.

Use the **show controllers ethernet-controller** privileged EXEC command to display the internal switch statistics, the statistics collected by the switch LRE chipset, and the statistics collected by the CPE LRE chipset. For information about this command, refer to the *Catalyst 2900 Series XL and Catalyst 3500 Series XL Command Reference*.

Assigning a Public Profile to All LRE Ports

Public profiles are set on a switch-wide (global) basis. The public profile you select should be compatible with the PSTN to which the LRE switch is connected.

Public profiles have priority over private profiles. If you assign a public profile to the switch, the switch ignores the private profile settings and uses the public profile settings on all LRE ports. To disable the public profile on the switch, use the **no lre profile global** global configuration command.

Changes to the public profile settings are immediately put in effect, and the public mode automatically becomes the active mode.

Beginning in privileged EXEC mode, follow these steps to assign a public profile to the LRE ports:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**lre profile global** *profile_name*	Enter the public profile name: PUBLIC-ANSI or PUBLIC-ETSI.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show controllers lre profile mapping**	Verify the change.

Use the **show controllers lre** commands to display the LRE link statistics and profile information on the LRE ports. For information about these commands, refer to the *Catalyst 2900 Series XL and Catalyst 3500 Series XL Command Reference*.

Assigning a Private Profile to an LRE Port

Private profiles are set on a per-port basis. You can assign the same private profile or different private profiles to the LRE ports on the switch. The default active private profile on all LRE ports is LRE-10.

The switch resets the ports with the updated profile settings.

Beginning in privileged EXEC mode, follow these steps to assign a private profile to an LRE port:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *LRE-interface*	Enter interface configuration mode, and enter the number of the LRE port to be configured.
Step 3	**lre profile** *profile_name*	Enter the private profile name: LRE-5, LRE-10, or LRE-15. The default profile is LRE-10.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show controllers lre profile mapping**	Verify the change.

Use the **show controllers lre** commands to display the LRE link statistics and profile information on the LRE ports. For information about these commands, refer to the *Catalyst 2900 Series XL and Catalyst 3500 Series XL Command Reference*.