Configuring Cisco IP Phone Support

This chapter describes how to configure support for Cisco IP phones on the Catalyst 6500 series switches. This information may be helpful in configuring support for non-Cisco IP phones, but we recommend that you see the manufacturer's documentation for those devices.

Note
- Cisco ME 6500 Series Ethernet switches are not typically used to support Cisco IP phones.
- For complete syntax and usage information for the commands used in this chapter, see the Cisco IOS Software Releases 12.2SX Command References at this URL:

  http://www.cisco.com/en/US/docs/ios/mcl/122sx_mcl.html

This chapter consists of these sections:

Understanding Cisco IP Phone Support

These sections describe Cisco IP phone support:

Cisco IP Phone Connections

The Cisco IP phone contains an integrated 3-port 10/100 switch. The ports are dedicated connections to these devices:

- Port 1 connects to the switch.
- Port 2 is an internal 10/100 interface that carries the Cisco IP phone traffic.
- Port 3 connects to a PC or other device.

Figure 12-1 shows a Cisco IP phone connected between a switch and a PC.

Figure 12-1   Cisco IP Phone Connected to a Switch

Cisco IP Phone Voice Traffic

The Cisco IP phone transmits voice traffic with Layer 3 IP precedence and Layer 2 CoS values, which are both set to 5 by default. The sound quality of a Cisco IP phone call can deteriorate if the voice traffic is transmitted unevenly. To provide more predictable voice traffic flow, you can configure QoS to trust the Layer 3 IP precedence or Layer 2 CoS value in the voice traffic (see Chapter 36, "Configuring PFC QoS").

Note   You can configure the ports on WS-X6548-RJ-45 and WS-X6548-RJ-21 switching modules to trust received Layer 2 CoS values (QoS port architecture 1p1q0t/1p3q1t). The WS-X6548-RJ-45 and WS-X6548-RJ-21 switching modules cannot supply power to Cisco IP phones. Configure QoS policies that use the Layer 3 IP precedence value on other switching modules.

You can configure a Layer 2 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 Cisco IP phone.

You can configure Layer 2 access ports on the switch to send Cisco Discovery Protocol (CDP) packets that instruct an attached Cisco IP phone to transmit voice traffic to the switch in any of the following ways:

- In the voice VLAN, tagged with a Layer 2 CoS priority value
- In the access VLAN, tagged with a Layer 2 CoS priority value
- In the access VLAN, untagged (no Layer 2 CoS priority value)

> **Note**   In all configurations, the voice traffic carries a Layer 3 IP precedence value (the default is 5 for voice traffic and 3 for voice control traffic).

You cannot use Cisco IOS software commands to configure the frame type used by data traffic sent from a device attached to the access port on the Cisco IP phone.

Cisco IP Phone Data Traffic

> **Note**
> - The ability to either trust or mark tagged data traffic from the device attached to the access port on the Cisco IP phone is called the trusted boundary feature.
> - Untagged traffic from the device attached to the Cisco IP phone passes through the Cisco IP phone unchanged, regardless of the trust state of the access port on the Cisco IP phone.

To process tagged data traffic (traffic in 802.1Q or 802.1p frame types) from the device attached to the access port on the Cisco IP phone (see Figure 12-1), you can configure Layer 2 access ports on the switch to send CDP packets that instruct an attached Cisco IP phone to configure the access port on the Cisco IP phone to either of these two modes:

- Trusted mode—All traffic received through the access port on the Cisco IP phone passes through the Cisco IP phone unchanged.
- Untrusted mode—All traffic in 802.1Q or 802.1p frames received through the access port on the Cisco IP phone is marked with a configured Layer 2 CoS value. The default Layer 2 CoS value is 0. Untrusted mode is the default.

IP Phone Power Configurations

These sections describe IP phone power configurations:

Locally Powered IP Phones

There are two sources of local power:

- From a power supply connected to the IP phone
- From a power supply through a patch panel over the twisted-pair Ethernet cable to the IP phone

When a locally powered IP phone is present on a switching module port, the switching module cannot detect its presence. The supervisor engine can discover a locally powered Cisco IP phone through CDP messaging with the Cisco IP phone.

If a locally powered IP phone loses local power, the switching module can discover and supply inline power to the IP phone if the inline power mode is set to **auto**.

Inline-Powered IP Phones

Switching modules that support an inline power daughtercard can supply power over the twisted-pair Ethernet cable to external devices such as IP phones, IP cameras, and wireless access points. Cisco inline power modules are available to support one or both of the two most common implementations of Power over Ethernet (PoE):

- Cisco Prestandard Inline Power
- IEEE 802.3af standard

With an inline power card installed, a switching module can automatically detect and provision a powered device that adheres to a PoE implementation supported by the card. The switching module can supply power to devices supporting other PoE implementations only through manual configuration.

Only one device can be powered per port, and the device must be connected directly to the switch port. For example, if a second IP phone is daisy chained off a phone that is connected to the switch port, the second phone cannot be powered by the switch.

Note   For information about switching modules that support inline power, see the *Release Notes for Cisco IOS Release Release Notes for Cisco IOS Release 12.2(33)SXH and Later Releases* publication at this URL: http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/ol_4164.htm

Inline Power Management

Each inline-powered device, such as an IP phone, requires power to be allocated from the chassis power budget. Because each powered device can have unique power requirements, more devices can be supported if the system's power management software can intelligently allocate the necessary power on a per-port basis.

With Release 12.2(33)SXH and later releases, you can configure the switching module to allocate and apply inline power to individual ports:

- When an attached inline-powered device is discovered, at a power level based on information sensed from the device or at a default or specified maximum power level (**auto** mode)
- At a fixed default or specified level, whether or not an inline-powered device is present on the port (**static** mode)

The Cisco Prestandard PoE implementation defines a method to sense an attached inline-powered device and to apply an initial power level. After activation, a Cisco Prestandard device that supports CDP can negotiate a lower or higher power allocation using CDP messaging.

The IEEE 802.3af PoE standard defines a method to sense an attached device and to immediately classify the device's power requirement into three power ranges:

- Class 1: Up to 4 W per port
- Class 2: Up to 7 W per port
- Class 3: Up to 15.4 W per port

The IEEE standard contains no provision for subsequent readjustment of a device's power allocation. Newer inline power daughtercards (such as the WS-F6K-48-AF) add the ability to accurately measure the power provided by the port to the powered device, and to enable power policing on a port. With power measurement and policing, you can safely override the IEEE 802.3af power classification of a device that requires a power level at the lower end of its IEEE power classification range. Cisco inline-powered devices that support IEEE 802.3af and CDP can use CDP to override the IEEE 802.3af power classification.

A switching module whose inline power card supports both PoE implementations will attempt both detection methods in parallel. If the attached device responds to both detection methods, the module will consider the device to be an IEEE 802.3af device.

⚠
Caution   When an IP phone cable is plugged into a port and the power is turned on, the supervisor engine has a 4-second timeout waiting for the link to go up on the line. During those 4 seconds, if the IP phone cable is unplugged and a network device is plugged in, the network device could be damaged. We recommend that you wait at least 10 seconds between unplugging a network device and plugging in another network device.

Example: Cisco Prestandard IP Phone

When a switching module port detects an unpowered Cisco Prestandard IP phone, the switching module reports to the supervisor engine that an unpowered Cisco IP phone is present and indicates which module and port the phone is on. If the port is configured in **auto** mode, the supervisor engine determines whether there is enough system power available to power up the Cisco IP phone. The power allocation will be the lower of default power or the configured port maximum if a maximum has been specified. If there is sufficient power available, the supervisor engine removes the allocated power from the total available system power and sends a message to the switching module instructing it to provide power to the port. If there is not enough available power for the Cisco IP phone, the supervisor engine sends a message to the switching module indicating that power is denied to the port.

Cisco IP phones may have different power requirements. Unless a lower maximum power level has been configured for the port, the supervisor engine initially allocates the configured default of 7 W (167 mA at 42 V) to the Cisco IP phone. When the correct amount of power is determined from the CDP messaging with the Cisco IP phone, the supervisor engine reduces or increases the allocated power.

For example, the default allocated power is 7 W. A Cisco IP phone requiring 6.3 W is plugged into a port. The supervisor engine allocates 7 W for the Cisco IP phone and powers it up. Once the Cisco IP phone is operational, it sends a CDP message with the actual power requirement to the supervisor engine. The supervisor engine then decreases the allocated power to the required amount.

When you power off the Cisco IP phone through the CLI or SNMP or remove it, the supervisor engine sends a message to the switching module to turn off the power on the port. That power is then returned to the available system power.

Example: IEEE 802.3af IP Phone

When a switching module port detects an unpowered IEEE 802.3af-compliant IP phone, the module detects the phone's IEEE 802.3af power classification and notifies the supervisor engine of the phone's location and power requirement. If there is sufficient system power available, the supervisor engine allocates the power level indicated by the IEEE class and sends a message to the switching module approving power to the port. If there is not enough available power for the IP phone, the supervisor engine sends a message to the switching module indicating that power is denied to the port.

For example, an IEEE 802.3af-compliant IP phone consuming 7.1 W is plugged into a port. The switching module detects the phone and determines that its IEEE power classification is Class 3, which requires between 7.0 W and 15.4 W. The switching module notifies the supervisor engine of the port location and the IEEE classification of the phone. If there is sufficient power available, the supervisor engine removes 15.4 W from the system power and approves power to the port. For this phone, the system is required to reserve an unnecessary 8.3 W due to the broad ranges of the IEEE classification system. If the **auto** mode is selected for this port with a maximum power level lower than 15.4 W, the Class 3 phone will be denied power.

By using a newer inline power card (WS-F6K-48-AF and later) that supports power measurement and policing, the situation described in this example can be managed with greater efficiency. By enabling power policing, you can safely set a lower maximum power allocation for the port because the module will monitor the power consumption of each port and will remove inline power to the port if the configured maximum power setting is exceeded.

In this example, you can enable power policing and configure the port for a maximum of 7.5 W. When the Class 3 phone is connected to this port, the supervisor engine will allocate only 7.5 W from the system power rather than 15.4 W, which leaves more power available for other powered devices. The port power consumption will be monitored, and if the phone later draws more than 7.5 W, the supervisor engine will remove inline power to the port and generate a syslog error message.

Default Cisco IP Phone Support Configuration

Cisco IP phone support is disabled by default.

When the voice VLAN feature is enabled, all untagged traffic is sent with the default CoS priority of the port.

The CoS is not trusted for 802.1P or 802.1Q tagged traffic.

Cisco IP Phone Support Configuration Guidelines and Restrictions

The following guidelines and restrictions apply when configuring Cisco IP phone support:

- You must enable the Cisco Discovery Protocol (CDP) on the port connected to the Cisco IP phone to send configuration information to the Cisco IP phone.

- You can configure a voice VLAN only on a Layer 2 LAN port.

- You can configure the ports on WS-X6548-RJ-45 and WS-X6548-RJ-21 switching modules to trust received Layer 2 CoS values (QoS port architecture 1p1q0t/1p3q1t). The WS-X6548-RJ-45 and WS-X6548-RJ-21 switching modules cannot supply power to Cisco IP phones.

- You cannot configure 10/100 Mbps ports with QoS port architecture 1p4t/2q2t to trust received Layer 2 CoS values. Configure policies to trust the Layer 3 IP precedence value on switching modules with QoS port architecture 1p4t/2q2t.

- The following conditions indicate that the Cisco IP phone and a device attached to the Cisco IP phone are in the same VLAN and must be in the same IP subnet:

  - If they both use 802.1p or untagged frames

  - If the Cisco IP phone uses 802.1p frames and the device uses untagged frames

- – If the Cisco IP phone uses untagged frames and the device uses 802.1p frames

- – If the Cisco IP phone uses 802.1Q frames and the voice VLAN is the same as the access VLAN

- The Cisco IP phone and a device attached to the Cisco IP phone cannot communicate if they are in the same VLAN and subnet but use different frame types, because traffic between devices in the same subnet is not routed (routing would eliminate the frame type difference).

- You cannot use Cisco IOS software commands to configure the frame type used by traffic sent from a device attached to the access port on the Cisco IP phone.

- If you enable port security on a port configured with a voice VLAN and if there is a PC connected to the Cisco IP phone, set the maximum allowed secure addresses on the port to at least 3.

- You cannot configure static secure MAC addresses in the voice VLAN.

- Ports configured with a voice VLAN can be secure ports (see Chapter 54, "Configuring Port Security").

- In all configurations, the voice traffic carries a Layer 3 IP precedence value (the default is 5 for voice traffic and 3 for voice control traffic).

Configuring Cisco IP Phone Support

These sections describe how to configure Cisco IP phone support:

- Configuring Voice Traffic Support, page 12-7
- Configuring Data Traffic Support, page 12-9
- Configuring Inline Power Support, page 12-10

Note Voice VLANs are referred to as *auxiliary VLANs* in the Catalyst software publications.

Configuring Voice Traffic Support

To configure the way in which the Cisco IP phone transmits voice traffic, perform this task:

	Command	Purpose
Step 1	Router(config)# **interface fastethernet** *slot/port*	Selects the port to configure.
Step 2	Router(config-if)# **switchport**	Configures the LAN port for Layer 2 switching.
		Note You must enter the **switchport** command once without any keywords to configure the LAN port as a Layer 2 port before you can enter additional **switchport** commands with keywords.
Step 3	Router(config-if)# **switchport voice vlan** {*voice_vlan_ID*	**dot1p**	**none**	**untagged**}	Configures the way in which the Cisco IP phone transmits voice traffic.
	Router(config-if)# **no switchport voice vlan**	Clears the configuration.

	Command	Purpose
Step 4	`Router(config)# end`	Exits configuration mode.
Step 5	`Router# show interfaces fastethernet slot/port switchport` `Router# show running-config interface fastethernet slot/port`	Verifies the configuration.

When configuring the way in which the Cisco IP phone transmits voice traffic, note the following information:

- Enter a voice VLAN ID to send CDP packets that configure the Cisco IP phone to transmit voice traffic in 802.1Q frames, tagged with the voice VLAN ID and a Layer 2 CoS value (the default is 5). Valid VLAN IDs are from 1 to 4094. The switch puts the 802.1Q voice traffic into the voice VLAN.

- Enter the **dot1p** keyword to send CDP packets that configure the Cisco IP phone to transmit voice traffic in 802.1p frames, tagged with VLAN ID 0 and a Layer 2 CoS value (the default is 5 for voice traffic and 3 for voice control traffic). The switch puts the 802.1p voice traffic into the access VLAN.

- Enter the **untagged** keyword to send CDP packets that configure the Cisco IP phone to transmit untagged voice traffic. The switch puts the untagged voice traffic into the access VLAN.

- Enter the **none** keyword to allow the Cisco IP phone to use its own configuration and transmit untagged voice traffic. The switch puts the untagged voice traffic into the access VLAN.

- In all configurations, the voice traffic carries a Layer 3 IP precedence value (the default is 5).

- See Chapter 36, "Configuring PFC QoS," for information about how to configure QoS.

- See the "Configuring a LAN Interface as a Layer 2 Access Port" section on page 13-15 for information about how to configure the port as a Layer 2 access port and configure the access VLAN.

This example shows how to configure Fast Ethernet port 5/1 to send CDP packets that tell the Cisco IP phone to use VLAN 101 as the voice VLAN:

```
Router# configure terminal
Router(config)# interface fastethernet 5/1
Router(config-if)# switchport voice vlan 101
Router(config-if)# exit
```

This example shows how to verify the configuration of Fast Ethernet port 5/1:

```
Router# show interfaces fastethernet 5/1 switchport
Name: Fa5/1
Switchport: Enabled
Administrative Mode: access
Operational Mode: access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: off
Access Mode VLAN: 100
Voice VLAN: 101
Trunking Native Mode VLAN: 1 (default)
Administrative private-vlan host-association: none
Administrative private-vlan mapping: 900 ((Inactive)) 901 ((Inactive))
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
```

Configuring Data Traffic Support

> **Note**   The trusted boundary feature is implemented with the **mls qos trust extend** command.

To configure the way in which the Cisco IP phone transmits data traffic, perform this task:

	Command	Purpose
Step 1	Router(config)# **interface fastethernet** *slot/port*	Selects the port to configure.
Step 2	Router(config-if)# **mls qos trust extend** [**cos** *cos_value*]	Configures the way in which the Cisco IP phone transmits data traffic.
	Router(config-if)# **no mls qos trust extend**	Clears the configuration.
Step 3	Router(config)# **end**	Exits configuration mode.
Step 4	Router# **show interfaces fastethernet** *slot/port* **switchport** Router# **show running-config interface fastethernet** *slot/port*	Verifies the configuration.

When configuring the way in which the Cisco IP phone transmits data traffic, note the following information:

- To send CDP packets that configure the Cisco IP phone to trust tagged traffic received from a device connected to the access port on the Cisco IP phone, do not enter the **cos** keyword and CoS value.

- To send CDP packets that configure the Cisco IP phone to mark tagged ingress traffic received from a device connected to the access port on the Cisco IP phone, enter the **cos** keyword and CoS value (valid values are 0 through 7).

- You cannot use Cisco IOS software commands to configure whether or not traffic sent from a device attached to the access port on the Cisco IP phone is tagged.

This example shows how to configure Fast Ethernet port 5/1 to send CDP packets that tell the Cisco IP phone to configure its access port as untrusted and to mark all tagged traffic received from a device connected to the access port on the Cisco IP phone with CoS 3:

```
Router# configure terminal
Router(config)# interface fastethernet 5/1
Router(config-if)# mls qos trust extend cos 3
```

This example shows how to configure Fast Ethernet port 5/1 to send CDP packets that tell the Cisco IP phone to configure its access port as trusted:

```
Router# configure terminal
Router(config)# interface fastethernet 5/1
Router(config-if)# mls qos trust extend
```

This example shows how to verify the configuration on Fast Ethernet port 5/1:

```
Router# show queueing interface fastethernet 5/1 | include Extend
  Extend trust state: trusted
```

Configuring Inline Power Support

To configure inline power support, perform this task:

	Command	Purpose
Step 1	`Router(config)# ` **`interface`** `type`[1] `slot/port`	Selects an interface to configure.
Step 2	`Router(config-if)# ` **`power inline`** `{`**`auto`** `| `**`static`** `| ` **`never`**`}[`*`max-milliwatts`*`]`	Configures inline power support and optionally specifies a maximum inline power level in milliwatts for the port.
	`Router(config-if)# ` **`no power inline`**	Clears the configuration.
Step 3	`Router(config-if)# ` `[`**`no`**`] ` **`power inline police`**	Enables inline power policing, if supported.[2]
Step 4	`Router(config)# ` **`end`**	Exits configuration mode.
Step 5	`Router# ` **`show power inline`** `{type slot/port	` **`module`** `slot}[`**`detail`**`]`	Verifies the configuration.

1. *type* = **fastethernet** or **gigabitethernet**

2. Requires a WS-F6K-48-AF or other inline power daughtercard that supports power monitoring and policing.

When configuring inline power support, note the following information:

- To configure auto-detection of an IP phone and auto-allocation of port inline power, enter the **auto** keyword.

- To configure auto-detection of an IP phone but reserve a fixed inline power allocation, enter the **static** keyword.

- To specify the maximum power to allocate to a port, specify the power in milliwatts using the **auto** or **static** keywords. If **auto** is specified, the device may negotiate a lower power allocation.

- To disable auto-detection of an IP phone, enter the **never** keyword.

This example shows how to disable inline power on Fast Ethernet port 5/1:

```
Router# configure terminal
Router(config)# interface fastethernet 5/1
Router(config-if)# power inline never
```

This example shows how to enable inline power on Fast Ethernet port 5/1:

```
Router# configure terminal
Router(config)# interface fastethernet 5/1
Router(config-if)# power inline auto
```

This example shows how to verify the inline power configuration on Fast Ethernet port 5/1:

```
Router# show power inline fastethernet 5/1
Interface  Admin   Oper       Power      Device
                              (Watts)
---------- ----- ---------- ------- -------------------
Fa5/1      auto   on          6.3    cisco phone device
Router#
```

This example shows how to verify the inline power configuration on GigabitEthernet port 1/9 when the line card includes an inline power daughtercard that supports power monitoring and policing:

```
Router# show power inline GigabitEthernet 1/9
Interface  Admin  Oper  Power (Watts)    Device   Class
                        From PS To Device
--------   -----  ----  ------- --------- -------  -----
Gi1/9      auto   on    17.3    15.4      Ieee PD  3
```

```
Interface  AdminPowerMax (Watts) Police   ActualConsumption
---------  --------------------- ------   -----------------
 Gi1/9              15.4            on      5.7
Router#
```

This example shows how to verify the detailed inline power configuration on GigabitEthernet port 1/9 when the line card includes an inline power daughtercard that supports power monitoring and policing:

```
Router# show power inline GigabitEthernet 1/9 detail
Interface: Gi1/9
 Inline Power Mode: auto
 Operational status: on
 Device Detected: yes
 Device Type: Cisco IP Phone 7970
 IEEE Class: 3
 Discovery mechanism used/configured: Ieee and Cisco
 Police: on

 Power Allocated
 Admin Value: 15.3
 Power drawn from the source: 11.5
 Power available to the device: 10.2

 Actual consumption
 Measured at the port: 6.3
 Maximum Power drawn by the device since powered on: 6.7

 Absent Counter: 0
 Over Current Counter: 0
 Short Current Counter: 0
 Invalid Signature Counter: 0
 Power Denied Counter: 0
Router#
```