Configure IOS Catalyst Switches to Connect Cisco IP Phones Configuration Example

Document ID: 69632

Contents

Introduction

This document provides sample configurations on Catalyst switches in order to connect to Cisco IP phones. This document includes the switch port, power inline, and quality of service (QoS) configurations. The switch port configuration uses a predefined macro which configures the switch port and QoS settings with minimum commands.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

This document is not restricted to specific software and hardware versions.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Background Information

This document explains the configuration of the switches that connect the PCs and IP phones on a switch port. The Cisco IP phone contains an integrated three−port 10/100 switch. The ports are dedicated connections.

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

Note: Only two ports are physically viewable. The other port is an internal port and is not physically viewable. In this section, port 2 is not viewable.

The switch has two VLANs: one carries data traffic and one carries voice traffic. The switch port can be either access VLAN or trunk VLAN, but you need to configure a voice VLAN to carry the voice traffic.

If your switch has a module that can provide Power over Ethernet (PoE) to end stations, you can set each interface on the module to automatically detect and apply PoE if the end station requires power. By default, when the switch detects a powered device on an interface, it assumes that the powered device consumes the maximum port it can provide. The maximum is 7 W on a legacy PoE module and 15.4W on the IEEE PoE modules introduced in Cisco IOS® Software Release 12.2(18)EW. When the switch receives a Cisco Discovery Protocol (CDP) packet from the powered device, the wattage automatically adjusts downward to the specific amount required by that device. Normally, this automatic adjustment works well, and no further configuration is required or recommended. However, you can specify the consumption of the powered device for the entire switch (or for a particular interface) to provide extra functionality from your switch. This is useful when CDP is disabled or not available.

Because the sound quality of an IP phone call can deteriorate if the data is sent unevenly, the switch uses 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. Refer to Configuring QoS for more information on QoS. Cisco AutoQoS automates consistent deployment of QoS features across Cisco routers and switches. It enables various Cisco QoS components based on the network environment and Cisco best−practice recommendations.

Configure

In this section, you are presented with the information to configure the features described in this document.

Note: Use the Command Lookup Tool (registered customers only) to obtain more information on the commands used in this section.

Network Diagram

This document uses this network setup:

Configurations

The configuration of the Catalyst switch contains these configurations:

- Configure the Switch Port to Carry Both Voice and Data Traffic
- Configure Inline Power Support
- Configure QoS

    - Configure QoS on the Layer 2 Uplink
    - Configure QoS on the Layer 3 Uplink
- Configure the Switch Using Cisco Predefined Macro

Configure the Switch Port to Carry Both Voice and Data Traffic

When you connect an IP phone to a switch using a trunk link, it can cause high CPU utilization in the switches. As all the VLANs for a particular interface are trunked to the phone, it increases the number of STP instances the switch has to manage. This increases the CPU utilization. Trunking also causes unnecessary broadcast / multicast / unknown unicast traffic to hit the phone link.

In order to avoid this, remove the trunk configuration and keep the voice and access VLAN configured along with Quality of Service (QoS). Technically, it is still a trunk, but it is called a Multi−VLAN Access Port (MVAP). Because voice and data traffic can travel through the same port, you should specify a different VLAN for each type of traffic. You can configure a switch port to forward voice and data traffic on different VLANs. Configure IP phone ports with a voice VLAN configuration. This configuration creates a pseudo trunk, but does not require you to manually prune the unnecessary VLANs.

The voice VLAN feature enables access ports to carry IP voice traffic from an IP phone. The voice VLAN feature is disabled by default. The Port Fast feature is automatically enabled when voice VLAN is configured. When you disable voice VLAN, the Port Fast feature is not automatically disabled. These are the options in the voice VLAN configuration:

```
Switch(config-if)#switchport voice vlan ?
  <1-4094>  Vlan for voice traffic
  dot1p     Priority tagged on PVID
  none      Do not tell telephone about voice vlan
  untagged  Untagged on PVID
```

- Enter a voice VLAN ID in order to send CDP packets that configure the 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 for voice traffic and 3 for voice control traffic). Valid VLAN IDs are from 1 to 4094. The switch puts the 802.1Q voice traffic into the voice VLAN.
- Enter the **dot1p** keyword in order to send CDP packets that configure the 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 in order to send CDP packets that configure the IP phone to transmit untagged voice traffic. The switch puts the untagged voice traffic into the access VLAN.
- Enter the **none** keyword in order to allow the IP phone to use its own configuration and transmit untagged voice traffic. The switch puts the untagged voice traffic into the access VLAN.

This example details that VLAN 10 carries data traffic, and VLAN 20 carries voice traffic:

Configure the Catalyst Switch to Carry Both Voice and Data Traffic

```
Switch#configure terminal

Switch(config)#interface fastethernet 2/5

Switch(config-if)#switchport mode access

Switch(config-if)#Switchport access vlan 10

Switch(config-if)#switchport voice vlan 20


!--- Configures the IP phone to transmit voice traffic in
!--- 802.1Q frames tagged with voice VLAN ID 20.


end
```

Note: You cannot disable the PC port span feature in 7960/40 phones.

Configure Inline Power Support

Cisco offers a comprehensive range of Catalyst switches that support PoE with 802.3af compliant, which also supports Cisco pre–standard PoE implementation. IEEE 802.3af–2003 describes five power classes that a device can belong to. The default power classification within IEEE 802.3af delivers 15.4W per power device. Delivery of PoE that uses the IEEE 802.3af default classification can significantly increase the power requirements on both the Power Sourcing Equipment (PSE) switch and the power infrastructure. In order to provide PoE in a cost effective and efficient manner, Catalyst switches support intelligent power management in addition to IEEE 802.3af classification. This enables a powered device and PSE to negotiate their respective capabilities in order to explicitly manage how much power is required for the device, and also how the PSE–capable switch manages the allocation of power to individual powered devices.

Issue this **show power inline** command in order to view the default power consumption a switch can supply:

```
        Switch#show power inline consumption default
        Default PD consumption : 15400 mW
```

By default, all the switch ports are configured to automatically detect and power the PoE devices. Issue this **show power inline** command in order to view the power inline configuration status of any port:

```
        Switch#show power inline FastEthernet 2/5
        Interface Admin  Oper        Power   Device              Class Max
                                      (Watts)

        --------- ------ ----------  ------- ------------------- ----- ----
        Fa2/5     auto   on          7.0     IP Phone 7960       n/a   15.4


        !--- You can see the Admin status as auto. This is the default configuration.
```

You can issue the **power inline** command in order to configure the inline power of an individual port. This shows the power inline configuration options:

```
        Switch(config-if)#power inline ?
          auto         Automatically detect and power inline devices
          consumption  Configure the inline device consumption
          never        Never apply inline power
          static       High priority inline power interface
```

- Auto By default, PoE–capable ports are configured to auto. The powered devices are powered up on a first–come, first–serve basis. If not enough inline power is available from the power supplies for all the powered devices in auto mode, there is no guarantee which powered devices are powered up.
- Static Static ports have a higher priority than auto ports in terms of power allocation and shutdown. The switch allocates power for a static port when it is configured. Power is then reserved for the port even when nothing is connected. The amount of power allocated can either use the default maximum value (15.4W) or can be specified when this option is used. This allocated amount is never adjusted by IEEE class or by CDP messages.
- Never The supervisor engine does not direct the switching module to power up the port even if a non–powered phone is connected.

With the static mode, the powered device is guaranteed to come online when plugged in. This is typically used for higher–priority users, such as corporate executives or wireless access points. However, if the IEEE class wattage of the powered device is greater than the maximum wattage of the static port, the powered device is not powered up. Similarly, in the case of a Cisco prestandard PoE, if the CDP message from the powered device indicates that the wattage required is greater than the maximum allocated on the static port, the port is powered down. In situations where the number of static ports desired exceeds the capabilities of the power supply, a newly designated static port is placed in an error–disable state, and 0W are allocated. If the switch needs to shut down powered devices because a power supply fails and there is insufficient power, auto–powered devices are shut before static–powered devices.

This example shows the power inline configuration of a switch port. As explained earlier in this section, the default power inline configuration of a port is auto. If the default configuration is changed and you want to configure the port back to auto, configure the port as described here:

Configure Inline Power Support for the Catalyst Switch that runs Cisco IOS
| ```
Switch#configure terminal

Switchj(config)#interface fastethernet 2/5

Switch(config-if)#power inline auto


!--- Configures inline power support on fast Ethernet port 2/5.
``` |

Configure QoS

You can use the auto–QoS feature to simplify the deployment of QoS features that exist. Auto–QoS makes assumptions about the network design. As a result, the switch can prioritize different traffic flows and appropriately use the egress queues instead of using the default QoS behavior. The default is that QoS is disabled. Then, the switch offers best–effort service to each packet, regardless of the packet content or size, and sends it from a single queue.

Auto–QoS configures QoS classification and configures egress queues. Before you configure auto–QoS, make sure you do not have any QoS configured on the switch. When you configure auto–QoS for the first time on the switch, QoS is enabled on the switch if it is disabled, and configures queues and thresholds in the global configuration. Finally, it configures the switch port to trust the incoming CoS parameters and configures the traffic–shaping parameters for that port. After this, every time you configure any port with auto–QoS, it only configures the switch port with QoS parameters.

Enable the **debug auto qos** command in the enable mode and configure the auto–qos on the switch port in order to find out what QoS configurations are applied during auto–QoS configuration. The debug **auto qos**

shows the commands that are applied on the switch.

After you issue the **auto qos** command, you can change the QoS configuration as per your requirement. However, this is not recommended. You can see the options available for the **auto qos voice** command here:

```
Switch(config-if)#auto qos voip ?
  cisco-phone       Trust the QoS marking of Cisco IP Phone
  cisco-softphone   Trust the QoS marking of Cisco IP SoftPhone
  trust             Trust the DSCP/CoS marking
```

Configure Auto−QoS for the Catalyst Switches that run IOS
Switch#**configure terminal** Switch(config)#**interface fastethernet 2/5** Switch(config-if)#**auto qos voip cisco-phone**   *!--- Configures the port to trust the CoS labels* *!--- in the incoming packets and configures the* *!--- traffic-shaping parameters.*

Although the **auto qos** command syntax is same on all the Catalyst switches, the QoS configurations, which are applied on the Catalyst switches by auto−QoS, are different amongst the Catalyst switches.

Configure QoS on the Layer 2 Uplink

If the voice traffic is going to cross the switch via the trunk links, you need to configure the QoS parameters on the trunk ports. In this case, you need to issue the **auto qos voip trust** command instead of the **auto qos voip cisco−phone** command.

Configure Auto−QoS on the Trunk Links of the Catalyst Switches that run IOS
Switch#**configure terminal** Switch(config)#**interface gigabitethernet 1/1** Switch(config-if)#**auto qos voip trust**   *!--- Configures the port to trust the CoS labels* *!--- in the incoming packets and configures the* *!--- traffic-shaping parameters.*

Configure QoS on the Layer 3 Uplink

If the voice traffic crosses the Layer 3 link, you need to configure the port with the **auto qos voip trust** command and you need to configure the port to **trust dscp**. This example shows the configuration of the Layer 3 port to carry voice traffic:

Configure Auto−QoS on the Layer 3 Port in the Catalyst Switch that runs IOS
Switch#**configure terminal** Switch(config)#**interface gigabitethernet 1/1**

```
Switch(config-if)#auto qos voip trust



!--- Configures the port to trust the CoS labels
!--- in the incoming packets and configures the
!--- traffic-shaping parameters.




Switch(config-if)#mls qos trust dscp



!--- Configures the port to trust the DSCP labels
!--- in the incoming packets. This command is for
!--- Catalyst 3560/3750/6500 Switches.




                              or

Switch(config-if)#qos trust dscp



!--- Configures the port to trust the DSCP labels
!--- in the incoming packets. This command is for
!--- Catalyst 4500 Switches.
```

Configure the Switch Using a Predefined Macro

In Catalyst 3560, 3750, and 4500 Switches that run Cisco IOS Software Release 12.2 and later, there are few predefined macros available to configure the switch ports. These are examples of macros and their roles in the configuration of switch port to support IP phones:

- cisco−phone This macro is for the switch port where the IP phone is directly connected to it and a PC can be connected to the phone. This macro configures the port with the access VLAN, voice VLAN, port security, spanning−tree portfast/bpduguard, and auto qos voip cisco−phone.
- cisco−switch This macro is for the uplink ports from the access switch to the distribution layer switch. If your voice traffic crosses the switch across the trunk links, you can use the cisco−switch macro in order to configure the uplink port. This macro configures the port with dot1q trunk, spanning−tree link−type point−to−point, and auto qos voip trust. This macro should not be used with the etherchannel/port groups.

Note: These switches support two types of macros:

- Smartport macros This macro is discussed in this section. For more information, refer to Configuring Smartports Macros.
- Interface macros This macro is user−defined and is used to automatically select a range of interfaces for configuration. For more information, refer to Configuring and Using Interface Range Macros.

Issue this **show** command in order to see the available macro:

```
Switch#show parser macro brief
```

```
      default global   : cisco-global
      default interface: cisco-desktop
      default interface: cisco-phone
      default interface: cisco-switch
      default interface: cisco-router
      default interface: cisco-wireless
```

Issue this **show** command in order to view the script of the macro:

```
Switch#show parser macro name cisco-phone

# Cisco IP phone + desktop template

# macro keywords $access_vlan $voice_vlan

# VoIP enabled interface - Enable data VLAN
# and voice VLAN
# Recommended value for access vlan should not be 1
switchport access vlan $access_vlan
switchport mode access

# Update the Voice VLAN value which should be
# different from data VLAN
# Recommended value for voice vlan should not be 1
switchport voice vlan $voice_vlan

# Enable port security limiting port to a 2 MAC
# addressess -- One for desktop on data vlan and
# one for phone on voice vlan
switchport port-security
switchport port-security maximum 2

# Ensure port-security age is greater than one minute
# and use inactivity timer
switchport port-security violation restrict
switchport port-security aging time 2
switchport port-security aging type inactivity

# Enable auto-qos to extend trust to attached Cisco phone
auto qos voip cisco-phone

# Configure port as an edge network port
spanning-tree portfast
spanning-tree bpduguard enable
```

This example shows the configuration of switch ports in the IP phone environment:

Configure the Switch Using a Predefined Macro

```
Switch#configure terminal

Switch(config)#interface gigabitethernet 2/5

Switch(config-if)#macro apply $access_vlan 10 $voice_vlan 20


!--- Configures the access port to connect the IP phone.
!--- The PC connects to the IP phone. It configures the port that
!--- belongs to access VLAN 10 and voice VLAN 20. It also configures
!--- auto qos voip cisco-phone.




Switch(config-if)#exit
```

```
Switch(config)#interface gigabitethernet 1/1

Switch(config-if)#macro apply cisco-switch $native_vlan 10



!--- Configures the uplink port as dot1q trunk port
!--- with native VLAN 10. It also configures auto qos voip trust.
```

Verify

Issue this **show interface** command in order to confirm that the configuration works properly on switches that run Cisco IOS:

```
Switch#show interface fastethernet 2/5 switchport

Name:Fa2/5
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 10 (VLAN0010)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: 20 (VLAN0020)
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL

Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
```

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

Troubleshoot

Catalyst 3560G: No Power to IP Phone After the Non−PoE Device is Unplugged

The Catalyst 3560G does not provide inline power to an IP phone connected to a port where a non−powered device was previously connected and unplugged from the port. This problem occurs with PoE settings of both auto and static on the port. This issue can also occur in 3750 Series Switches. It has been identified in Cisco bug ID CSCsc10999 (registered customers only) .

The workaround is to issue shutdown/no shutdown on the port. Then, the switch provides power to the IP phone. This issue has been resolved in Cisco IOS Software Release 12.2(25)SED1.

The 7935 IP Conference Phone Receives Data IP Address Instead of Voice IP Address

If the 7935 IP Conference Phone is connected to a switch, the conference phone receives the IP address from the data VLAN. If the 7960 IP Phone is connected on the same switch port as the 7935 IP Conference Phone, the 7960 receives the IP address on the voice VLAN.

This issue is due to the design of the 7935 IP Conference Phones. This conference phone does not have a 10/100 port to connect a PC like other 7900 Series IP Phones have. The concept of voice VLAN or auxiliary VLAN does not directly apply to the 7935 IP Conference Phones.

Refer to 7935 IP Conference Phone Optimal Performance Configuration for the detailed explanation and the solution.

IP Phones Do Not Come Up with MAC Authentication Bypass (MAB)

In a switch that uses MAB to grant access to network devices, all IP phone MAC addresses learned through CDP are allowed on the auxiliary (voice) VLAN. However, if the IP phone is alone (without any PC connected to it) and connected to a port configured with both data and voice VLANs, then the IP phone is placed on the data VLAN. Therefore, the IP phone will face issues when it registers with Cisco CallManager.

In order to overcome this issue, either configure the access VLAN of port with the ID of voice VLAN, or connect a PC to the IP phone.

IP Phones Do Not Get IP Address From DHCP Server

If Dynamic Address Resolution Protocol (ARP) Inspection (DAI) is enabled in the switch, it depends on the entries in the DHCP snooping binding database to verify IP−to−MAC address bindings in incoming ARP requests and ARP responses. Make sure to enable DHCP snooping in order to permit ARP packets that have dynamically assigned IP addresses.

Also, the ARP Access Control Lists (ACLs) take precedence over entries in the DHCP snooping binding database. The switch uses ACLs only if you configure them by using the **ip arp inspection filter vlan** global configuration command. The switch first compares ARP packets to user−configured ARP ACLs. If the ARP ACL denies the ARP packet, the switch also denies the packet even if a valid binding exists in the database populated by DHCP snooping.

Related Information

- **Configuring Cisco IP Phone Support**
- **Configuring Power over Ethernet**
- **Configuring PFC QoS in Catalyst 6500**
- **Configuring QoS in Catalyst 4500**
- **Configuring QoS in Catalyst 3750**
- **Switches Product Support**
- **LAN Switching Technology Support**
- **Technical Support & Documentation − Cisco Systems**

Updated: Aug 30, 2006   Document ID: 69632