



Configuring Cisco Discovery Protocol

This chapter describes how to configure Cisco Discovery Protocol and Cisco Discovery Protocol Bypass on the Catalyst 4500 Series Switches. It also provides guidelines, procedures, and configuration examples.

This chapter includes the following major sections:

- [About Cisco Discovery Protocol, page 30-2](#)
- [Configuring Cisco Discovery Protocol, page 30-2](#)
- [About Cisco Discovery Protocol Bypass, page 30-5](#)
- [Configuring Cisco Discovery Protocol Bypass, page 30-5](#)



Note

For complete syntax and usage information for the Cisco IOS commands used in this chapter, refer to the *Cisco IOS Configuration Fundamentals Configuration Guide*, Release 12.4:

http://www.cisco.com/en/US/docs/ios/fundamentals/configuration/guide/12_4/cf_12_4_book.html

and the *Cisco IOS Configuration Fundamentals Command Reference*, Release 12.2:

http://www.cisco.com/en/US/docs/ios/12_2/configfun/command/reference/ffun_r.html



Note

For complete syntax and usage information for the switch commands used in this chapter, see the *Cisco Catalyst 4500 Series Switch Command Reference* and related publications at this location:

<http://www.cisco.com/en/US/products/hw/switches/ps4324/index.html>

If a command is not in the *Catalyst 4500 Series Switch Command Reference*, you can locate it in the Cisco IOS library. See the *Command Reference for the Catalyst 4006 Switch with Supervisor Engine III* and related publications at this location:

<http://www.cisco.com/en/US/products/ps6350/index.html>

About Cisco Discovery Protocol

Cisco Discovery Protocol is a protocol that runs over Layer 2 (the data link layer) on all Cisco routers, bridges, access servers, and switches. Cisco Discovery Protocol allows network management applications to discover Cisco devices that are neighbors of already known devices, in particular, neighbors running lower-layer, transparent protocols. With Cisco Discovery Protocol, network management applications can learn the device type and the SNMP agent address of neighboring devices. Cisco Discovery Protocol enables applications to send SNMP queries to neighboring devices.

Cisco Discovery Protocol runs on all LAN and WAN media that support Subnetwork Access Protocol (SNAP).

Each Cisco Discovery Protocol-configured device sends periodic messages to a multi-cast address. Each device advertises at least one address at which it can receive SNMP messages. The advertisements also contain the time-to-live, or holdtime information, which indicates the length of time a receiving device should hold Cisco Discovery Protocol information before discarding it.

Configuring Cisco Discovery Protocol

The following sections describe how to configure Cisco Discovery Protocol:

- [Enabling Cisco Discovery Protocol Globally, page 30-2](#)
- [Displaying the Cisco Discovery Protocol Global Configuration, page 30-2](#)
- [Enabling Cisco Discovery Protocol on an Interface, page 30-3](#)
- [Displaying the Cisco Discovery Protocol Interface Configuration, page 30-3](#)
- [Monitoring and Maintaining Cisco Discovery Protocol, page 30-4](#)

Enabling Cisco Discovery Protocol Globally

To enable Cisco Discovery Protocol globally, use this command:

Command	Purpose
Switch(config)# [no] cdp run	Enables Cisco Discovery Protocol globally. Use the no keyword to disable Cisco Discovery Protocol globally.

This example shows how to enable Cisco Discovery Protocol globally:

```
Switch(config)# cdp run
```

Displaying the Cisco Discovery Protocol Global Configuration

To display the Cisco Discovery Protocol configuration, use this command:

Command	Purpose
Switch# show cdp	Displays global Cisco Discovery Protocol information.

This example shows how to display the Cisco Discovery Protocol configuration:

```
Switch# show cdp
Global Cisco Discovery Protocol information:
  Sending CDP packets every 120 seconds
  Sending a holdtime value of 180 seconds
  Sending CDPv2 advertisements is enabled
Switch#
```

For additional Cisco Discovery Protocol **show** commands, see the “[Monitoring and Maintaining Cisco Discovery Protocol](#)” section on page 30-4.

Enabling Cisco Discovery Protocol on an Interface

To enable Cisco Discovery Protocol on an interface, use this command:

Command	Purpose
Switch(config-if)# [no] cdp enable	Enables Cisco Discovery Protocol on an interface. Use the no keyword to disable Cisco Discovery Protocol on an interface.

This example shows how to enable Cisco Discovery Protocol on Fast Ethernet interface 5/1:

```
Switch(config)# interface fastethernet 5/1
Switch(config-if)# cdp enable
```

This example shows how to disable Cisco Discovery Protocol on Fast Ethernet interface 5/1:

```
Switch(config)# interface fastethernet 5/1
Switch(config-if)# no cdp enable
```

Displaying the Cisco Discovery Protocol Interface Configuration

To display the Cisco Discovery Protocol configuration for an interface, use this command:

Command	Purpose
Switch# show cdp interface <i>[type/number]</i>	Displays information about interfaces where Cisco Discovery Protocol is enabled.

This example shows how to display the Cisco Discovery Protocol configuration of Fast Ethernet interface 5/1:

```
Switch# show cdp interface fastethernet 5/1
FastEthernet5/1 is up, line protocol is up
  Encapsulation ARPA
```

```

Sending CDP packets every 120 seconds
Holdtime is 180 seconds
Switch#

```

Monitoring and Maintaining Cisco Discovery Protocol

To monitor and maintain Cisco Discovery Protocol on your device, enter one or more of the following commands:

Command	Purpose
Switch# clear cdp counters	Resets the traffic counters to zero.
Switch# clear cdp table	Deletes the Cisco Discovery Protocol table of information about neighbors.
Switch# show cdp	Displays global information such as frequency of transmissions and the holdtime for packets being transmitted.
Switch# show cdp entry <i>entry_name</i> [protocol version]	Displays information about a specific neighbor. The display can be limited to protocol or version information.
Switch# show cdp interface [<i>type/number</i>]	Displays information about interfaces on which Cisco Discovery Protocol is enabled.
Switch# show cdp neighbors [<i>type/number</i>] [detail]	Displays information about neighboring equipment. The display can be limited to neighbors on a specific interface and expanded to provide more detailed information.
Switch# show cdp traffic	Displays Cisco Discovery Protocol counters, including the number of packets sent and received and checksum errors.
Switch# show debugging	Displays information about the types of debugging that are enabled for your switch.

This example shows how to clear the Cisco Discovery Protocol counter configuration on your switch:

```
Switch# clear cdp counters
```

This example shows how to display information about the neighboring equipment:

```

Switch# show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater

Device ID      Local Intrfce  Holdtme  Capability  Platform  Port ID
JAB023807H1   Fas 5/3       127      T S         WS-C2948  2/46
JAB023807H1   Fas 5/2       127      T S         WS-C2948  2/45
JAB023807H1   Fas 5/1       127      T S         WS-C2948  2/44
JAB023807H1   Gig 1/2       122      T S         WS-C2948  2/50
JAB023807H1   Gig 1/1       122      T S         WS-C2948  2/49
JAB03130104   Fas 5/8       167      T S         WS-C4003  2/47
JAB03130104   Fas 5/9       152      T S         WS-C4003  2/48

```

About Cisco Discovery Protocol Bypass

When a Cisco IP Phone is plugged into a port that is configured with a Voice VLAN and single-host mode, the phone will be silently allowed onto the network by way of a feature known as Cisco Discovery Protocol Bypass. The phone (or any device) that sends the appropriate Type Length Value (TLV) in a Cisco Discovery Protocol message will be allowed access to the voice VLAN.

In Cisco Discovery Protocol Bypass mode, Cisco Discovery Protocol packets are received and transmitted unchanged. Received packets are not processed. No packets are generated. In this mode, 'bump-in-the-wire' behavior is applied to Cisco Discovery Protocol packets. This is a backward compatible mode, equivalent to not having Cisco Discovery Protocol support.

In Cisco Discovery Protocol Bypass mode authentication sessions are established in single and multi-host modes for IP Phones. However, if voice VLAN and 802.1x on an interface port is enabled, then Cisco Discovery Protocol Bypass is enabled when the host mode is set to single or multi-host mode.

It is possible to use the Multi-Domain Authentication (MDA) feature instead of Cisco Discovery Protocol Bypass feature as it provides better Access Control, Visibility and Authorization.

**Note**

By default the host mode is set to single mode in legacy mode and multi-authentication in the edge mode.

Cisco Discovery Protocol Enhancement for Second Port Disconnect—Allows a Cisco IP phone to send a Cisco Discovery Protocol message to the switch when a host unplugs from behind the phone. The switch is then able to clear any authenticated session for the indirectly connected host, the same as if the host had been directly connected and the switch had detected a link down event. This is supported in latest IP telephones.

Cisco Discovery Protocol Bypass provides no support for third-party phones—Cisco Discovery Protocol Bypass works only with Cisco phones.

Configuring Cisco Discovery Protocol Bypass

The following sections describe how to configure Cisco Discovery Protocol Bypass

- [Enabling Cisco Discovery Protocol Bypass, page 30-5](#)
- [Displaying Cisco Discovery Protocol Neighbors, page 30-7](#)
- [Disabling Cisco Discovery Protocol Bypass, page 30-7](#)

Enabling Cisco Discovery Protocol Bypass

To enable Cisco Discovery Protocol Bypass, use these commands:

Command	Purpose
enable Example: Switch> enable	Enables privileged EXEC mode. Enter your password if prompted.
configure terminal Example: Switch# configure terminal	Enters the global configuration mode.
interface interface-id Example: Switch(config)# interface GigabitEthernet1/0/12	Specifies a physical port, and enters interface configuration mode. Valid interfaces are physical ports.
switchport mode access Example: Switch(config-if)# switchport mode access	Specifies that the interface is in access mode.
switchport access vlan vlan id Example: Switch(config-if)# switchport access vlan 10	Assigns all ports as static-access ports in the same VLAN If you configure the port as a static-access port, assign it to only one VLAN. The range is 1 to 4094.
switchport voice vlan vlan-id Example: Switch(config-if)# switchport voice vlan 3	Instruct the Cisco IP phone to forward all voice traffic through the specified VLAN. By default, the Cisco IP phone forwards the voice traffic with an 802.1Q priority of 5. Valid VLAN IDs are from 1 to 4094 when the enhanced software image (EI) is installed and 1 to 1001 when the standard software image is installed. Do not enter leading zeros.
authentication port-control auto Example: Switch(config-if)# authentication port-control auto	Enables 802.1x authentication on the port.

Command	Purpose
authentication host-mode {single-host multi-host} Example: Switch(config-if)# authentication host-mode single multi-host	The keywords allow the following: single-host -Single host (client) on an IEEE 802.1X-authorized port. multi-host -Multiple hosts on an 802.1X-authorized port after a authenticating a single host.
dot1x pae authenticator or mab Example: Switch(config-if)# dot1x pae authenticator or Switch(config-if)# mab	Enables 802.1X authentication on the port with default parameters

Cisco Discovery Protocol Bypass is enabled by default once **authentication port-control auto** is configured with dot1x or MAB or if voice vlan is configured on the interface along with single/multiple host mode.

Displaying Cisco Discovery Protocol Neighbors

The following configuration example displays Cisco Discovery Protocol neighbors.

```
Switch# show cdp neighbors g1/0/37 detail
Switch ID: SEP24B657B038DF
Entry address(es):
Platform: Cisco IP Phone 9971, Capabilities: Host Phone Two-port Mac Relay Interface:
GigabitEthernet1/0/37, Port ID (outgoing port): Port 1 Holdtime : 157 sec
Second Port Status: Down<<
Version:sip9971.9-1-1SR1
advertisement version: 2
Duplex: full
Power drawn: 12.804 Watts
Power request id: 57146, Power management id: 4
Power request levels are:12804 0 0 0 0
Total cdp entries displayed : 1
```

Disabling Cisco Discovery Protocol Bypass

To disable Cisco Discovery Protocol Bypass, enter the **no authentication port-control auto** command in interface configuration mode.

