



# Configuring Cisco Discovery Protocol

---

This chapter describes how the Cisco Discovery Protocol (CDP) works with Simple Network Management Protocol (SNMP) to identify other devices in your network in Cisco IOS Release 12.2.

For further details on the commands mentioned in this chapter, refer to the *Cisco IOS Configuration Fundamentals Command Reference*.

## Configuring the Cisco Discovery Protocol

CDP is primarily used to obtain protocol addresses of neighboring devices and discover the platform of those devices. CDP can also be used to display information about the interfaces your router uses. CDP is media- and protocol-independent, and runs on all Cisco-manufactured equipment including routers, bridges, access servers, and switches.

Use of SNMP with the CDP MIB allows network management applications to learn the device type and the SNMP agent address of neighboring devices, and to send SNMP queries to those devices. CDP uses the CISCO-CDP-MIB.

CDP runs on all media that support Subnetwork Access Protocol (SNAP), including LAN, Frame Relay, and ATM physical media. CDP runs over the data link layer only. Therefore, two systems that support different network-layer protocols can learn about each other.

Each device configured for CDP sends periodic messages, known as advertisements, to a multicast address. Each device advertises at least one address at which it can receive SNMP messages. The advertisements also contain time-to-live, or holdtime, information, which indicates the length of time a receiving device should hold CDP information before discarding it. Each device also listens to the periodic CDP messages sent by others in order to learn about neighboring devices and determine when their interfaces to the media go up or down.

CDP Version-2 (CDPv2) is the most recent release of the protocol and provides more intelligent device tracking features. These features include a reporting mechanism that allows for more rapid error tracking, thereby reducing costly downtime. Reported error messages can be sent to the console or to a logging server, and cover instances of unmatching native VLAN IDs (IEEE 802.1Q) on connecting ports, and unmatching port duplex states between connecting devices. Refer to the *Cisco IOS Software System Error Messages* document for detailed examples of CDP error messages.

CDPv2 **show** commands can provide detailed output on VLAN Trunking Protocol (VTP) management domain and duplex modes of neighbor devices, CDP-related counters, and VLAN IDs of connecting ports.

VTP is a discovery technique deployed by switches where each switch advertises its management domain on its trunk ports, its configuration revision number, and its known VLANs and their specific parameters. A VTP domain is made up of one or more interconnected devices that share the same VTP domain name. A switch can be configured to be in only one VTP domain.

Type-Length-Value fields (TLVs) are blocks of information embedded in CDP advertisements. [Table 19](#) summarizes the TLV definitions for CDP advertisements.

**Table 21** *Type-Length-Value Definitions for CDPv2*

TLV	Definition
Device-ID TLV	Identifies the device name in the form of a character string.
Address TLV	Contains a list of network addresses of both receiving and sending devices.
Port-ID TLV	Identifies the port on which the CDP packet is sent.
Capabilities TLV	Describes the functional capability for the device in the form of a device type, for example, a switch.
Version TLV	Contains information about the software release version on which the device is running.
Platform TLV	Describes the hardware platform name of the device, for example, Cisco 4500.
IP Network Prefix TLV	Contains a list of network prefixes to which the sending device can forward IP packets. This information is in the form of the interface protocol and port number, for example, Eth 1/0.
VTP Management Domain TLV	Advertises the system's configured VTP management domain name-string. Used by network operators to verify VTP domain configuration in adjacent network nodes.
Native VLAN TLV	Indicates, per interface, the assumed VLAN for untagged packets on the interface. CDP learns the native VLAN for an interface. This feature is implemented only for interfaces that support the IEEE 802.1Q protocol.
Full/Half Duplex TLV	Indicates status (duplex configuration) of CDP broadcast interface. Used by network operators to diagnose connectivity problems between adjacent network elements.

## CDP Configuration Task List

To configure CDP, perform any of the optional tasks in the following sections:

- [Setting the CDP Transmission Timer and Hold Time](#)
- [Reenabling CDP on a Local Router](#)
- [Reenabling CDP Version-2 Advertisements](#)
- [Reenabling CDP on an Interface](#)
- [Monitoring and Maintaining CDP](#)

The the end of this chapter for “[CDP Configuration Examples](#).”

**Note**

The **cdp enable**, **cdp timer**, and **cdp run** global configuration commands affect the operation of the IP on-demand routing feature (that is, the **router odr** global configuration command). For more information on the **router odr** command, see the “On-Demand Routing Commands” chapter in the Release 12.2 *Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols* document.

## Setting the CDP Transmission Timer and Hold Time

To set the frequency of CDP transmissions and the hold time for CDP packets, use the following commands in global configuration mode:

	Command	Purpose
Step 1	Router(config)# <b>cdp timer</b> <i>seconds</i>	Specifies frequency of transmission of CDP updates.
Step 2	Router(config)# <b>cdp holdtime</b> <i>seconds</i>	Specifies the amount of time a receiving device should hold the information sent by your device before discarding it.

## Reenabling CDP on a Local Router

CDP is enabled on Cisco devices by default. If you prefer not to use the CDP device discovery capability, you can disable it with the **no cdp run** command.

To reenble CDP after disabling it, use the following command in global configuration mode:

Command	Purpose
Router(config)# <b>cdp run</b>	Enables CDP on the system.

## Reenabling CDP Version-2 Advertisements

The broadcasting of CDPv2 advertisements is enabled on Cisco routers by default. You can disable CDPv2 advertisements with the **no cdp advertise-v2** command.

To reenble CDPv2 advertisements, use the following command in global configuration mode:

Command	Purpose
Router(config)# <b>cdp advertise-v2</b>	Enables CDPv2 advertising functionality on the system.

## Reenabling CDP on an Interface

CDP is enabled by default on all supported interfaces (except for Frame Relay multipoint subinterfaces) to send and receive CDP information. However, some interfaces, such as ATM interfaces, do not support CDP.

You can disable CDP on an interface that supports CDP by using the **no cdp enable** command.

To reenable CDP on an interface after disabling it, use any of the following command in interface configuration mode, as needed:

Command	Purpose
Router(config-if)# <b>cdp enable</b>	Enables CDP on an interface.

## Monitoring and Maintaining CDP

To monitor and maintain CDP on your device, use one or more of the following commands in privileged EXEC mode:

Command	Purpose
Router# <b>clear cdp counters</b>	Resets the traffic counters to zero.
Router# <b>clear cdp table</b>	Deletes the CDP table of information about neighbors.
Router# <b>show cdp</b>	Displays the interval between transmissions of CDP advertisements, the number of seconds the CDP advertisement is valid for a given port, and the version of the advertisement.
Router# <b>show cdp entry</b> <i>device-name</i> [ <b>protocol</b>   <b>version</b> ]	Displays information about a specific neighbor. Display can be limited to protocol or version information.
Router# <b>show cdp interface</b> [ <b>type number</b> ]	Displays information about interfaces on which CDP is enabled.
Router# <b>show cdp neighbors</b> [ <i>type number</i> ] [ <b>detail</b> ]	Displays the type of device that has been discovered, the name of the device, the number and type of the local interface (port), the number of seconds the CDP advertisement is valid for the port, the device type, the device product number, and the port ID. Issuing the <b>detail</b> keyword displays information on the native VLAN ID, the duplex mode, and the VTP domain name associated with neighbor devices.
Router# <b>show cdp traffic</b>	Displays CDP counters, including the number of packets sent and received and checksum errors.
Router# <b>show debugging</b>	Displays information about the types of debugging that are enabled for your router. Refer to the <i>Cisco IOS Debug Command Reference</i> for more information about CDP <b>debug</b> commands.

## CDP Configuration Examples

The following sections provide CDP configuration examples:

- [Example: Setting the CDP Transmission Timer and Hold Time](#)
- 

### Example: Setting the CDP Transmission Timer and Hold Time

In the following example, the user sets the cdp timer to send updates every 30 seconds to neighboring routers and sets the router to show that the updates are working correctly:

```

Router(config)# cdp timer 30
Router(config)# exit
Router# show cdp interface
Serial0 is up, line protocol is up
Encapsulation is HDLC
Sending CDP packets every 30 seconds
Holdtime is 180 seconds

```

In the following example, the user sets the holdtime to be 90 seconds and sets the router to show that the updates are working correctly:

```

Router(config)# cdp holdtime 90
Router(config)# exit
Router# show cdp interface
Serial0 is up, line protocol is up
Encapsulation is HDLC
Sending CDP packets every 30 seconds
Holdtime is 90 seconds

```

## Example: Monitoring and Maintaining CDP

The following example shows a typical series of steps for viewing information about CDP neighbors.

[Table 20](#) describes the significant fields shown in the output of the **show cdp neighbors** command.

```

C3660-2> show cdp
Global CDP information:
    Sending CDP packets every 60 seconds
    Sending a holdtime value of 180 seconds
    Sending CDPv2 advertisements is enabled

C3660-2> 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
C2950-1            Fas 0/0          148        S I         WS-C2950T-Fas 0/15
RX-SWV.cisco.com  Fas 0/1          167        T S         WS-C3524-XFas 0/13

C3660-2> show cdp neighbors detail
-----
Device ID: C2950-1
Entry address(es):
Platform: Cisco WS-C2950T-24, Capabilities: Switch IGMP
Interface: FastEthernet0/0, Port ID (outgoing port): FastEthernet0/15
Holdtime : 139 sec

Version :
Cisco IOS C2950 Software (C2950-I6Q4L2-M), Version 12.1(9)EA1, RELEASE SOFTWARE
.
.
.
C3660-2> show cdp traffic
CDP counters :
    Total packets output: 81684, Input: 81790
    Hdr syntax: 0, Chksum error: 0, Encaps failed: 0

```

```

No memory: 0, Invalid packet: 0, Fragmented: 0
CDP version 1 advertisements output: 0, Input: 0
CDP version 2 advertisements output: 81684, Input: 81790

```

C3660-2>

Table 20 describes the significant fields shown in the output of the show cdp neighbors command.

**Table 22** *show cdp neighbors Field Descriptions*

Field	Definition
Device ID	The name of the neighbor device and either the MAC address or the serial number of this device.
Local Intrfce	The protocol being used by the connectivity media.
Holdtme	The remaining amount of time (in seconds) the current device will hold the CDP advertisement from a sending router before discarding it.
Capability (Capability Codes)	<p>Capability (type of routing device) of the listed neighboring device.</p> <p>The capability types that can be discovered are:</p> <ul style="list-style-type: none"> <li>R—Router</li> <li>T—Transparent bridge</li> <li>B—Source-routing bridge</li> <li>S—Switch</li> <li>H—Host</li> <li>I— device is using IGMP</li> <li>r—Repeater</li> </ul>
Platform	The product number of the device.
Port ID	The protocol and port number of the device.