CHAPTER 26

Configuring Cisco Discovery Protocol

This chapter describes how to configure Cisco Discovery Protocol (CDP) on the Cisco MWR 2941 router.

Note For complete syntax and usage information for the commands used in this chapter, see the *Cisco MWR 2941 Mobile Wireless Edge Router IOS Command Reference, Release 15.0(1)MR* and the *Configuration Fundamentals Configuration Guide, Cisco IOS Release 15.0S*.

Note The Cisco MWR 2941 does not necessarily support all of the commands described in the Release 15.0(1)S documentation.

Understanding CDP

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

CDP runs on all media that support Subnetwork Access Protocol (SNAP). Because CDP runs over the data-link layer only, two systems that support different network-layer protocols can learn about each other.

Each CDP-configured device sends periodic messages to a multicast address, advertising at least one address at which it can receive SNMP messages. The advertisements also contain time-to-live, or holdtime information, which is the length of time a receiving device holds CDP information before discarding it. Each device also listens to the messages sent by other devices to learn about neighboring devices.

For a router and connected endpoint devices running Cisco Medianet

- CDP identifies connected endpoints that communicate directly with the router.
- To prevent duplicate reports of neighboring devices, only one wired switch reports the location information.
- The wired switch and the endpoints both send and receive location information.

  For information, go to http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_cdp_discover.html.

The router supports CDP Version 2.

Configuring CDP

Default CDP Configuration

Table 26-1 shows the default CDP configuration.

Table 26-1 Default CDP Configuration

Feature	Default Setting
CDP global state	Enabled.
CDP interface state	Enabled only on NNIs; disabled on ENIs **Note** CDP is not supported on UNIs.
CDP timer (packet update frequency)	60 seconds
CDP holdtime (before discarding)	180 seconds
CDP Version-2 advertisements	Enabled

Configuring the CDP Characteristics

You can configure the frequency of CDP updates, the amount of time to hold the information before discarding it, and whether or not to send Version-2 advertisements.

Beginning in privileged EXEC mode, follow these steps to configure the CDP timer, holdtime, and advertisement type.

Note Steps 2 through 4 are all optional and can be performed in any order.

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**cdp timer** *seconds*	(Optional) Sets the transmission frequency of CDP updates in seconds. The range is from 5–254; the default is 60 seconds.
Step 3	**cdp holdtime** *seconds*	(Optional) Specifies the amount of time a receiving device should hold the information sent by your device before discarding it. The range is from 10–255 seconds; the default is 180 seconds.
Step 4	**cdp advertise-v2**	(Optional) Configures CDP to send Version-2 advertisements. This is the default state.
Step 5	**end**	Returns to privileged EXEC mode.
Step 6	**show cdp**	Verifies your settings.
Step 7	**copy running-config startup-config**	(Optional) Saves your entries in the configuration file.

Use the **no** form of the CDP commands to return to the default settings.

This example shows how to configure CDP characteristics.

```
Router# configure terminal
Router(config)# cdp timer 50
Router(config)# cdp holdtime 120
Router(config)# cdp advertise-v2
Router(config)# end
```

For additional CDP **show** commands, see the "Monitoring and Maintaining CDP" section on page 26-5.

Disabling and Enabling CDP

CDP is enabled by default on NNIs. It is disabled by default on ENIs but can be enabled.

Note Cisco devices (such as Cisco IP Phones) regularly exchange CDP messages with connected devices. Disabling CDP can interrupt device connectivity.

Beginning in privileged EXEC mode, follow these steps to globally disable the CDP device discovery capability:

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**no cdp run**	Disables CDP.
Step 3	**end**	Returns to privileged EXEC mode.

Beginning in privileged EXEC mode, follow these steps to globally enable CDP when it has been disabled:

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**cdp run**	Enables CDP after disabling it.
Step 3	**end**	Returns to privileged EXEC mode.

This example shows how to globally enable CDP if it has been disabled:

```
Router# configure terminal
Router(config)# cdp run
Router(config)# end
```

Disabling and Enabling CDP on an Interface

CDP is enabled by default on NNIs to send and to receive CDP information. You can enable CDP on ENIs, but it is not supported on UNIs. Beginning in privileged EXEC mode, follow these steps to disable CDP on a port:

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**interface** *interface-id*	Specifies the interface on which you are disabling CDP, and enter interface configuration mode.
Step 3	**no cdp enable**	Disables CDP on the interface.
Step 4	**end**	Returns to privileged EXEC mode.
Step 5	**copy running-config startup-config**	(Optional) Saves your entries in the configuration file.

Beginning in privileged EXEC mode, follow these steps to enable CDP on a port when it has been disabled:

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**interface** *interface-id*	Specifies the interface on which you are enabling CDP, and enter interface configuration mode.
Step 3	**cdp enable**	Enables CDP on the interface after disabling it.
Step 4	**end**	Returns to privileged EXEC mode.
Step 5	**copy running-config startup-config**	(Optional) Saves your entries in the configuration file.

This example shows how to enable CDP on a port when it has been disabled:

```
Router# configure terminal
Router(config)# interface gigabitethernet0/1
Router(config-if)# cdp enable
Router(config-if)# end
```

This example shows how to change a UNI to an ENI and enable CDP on the port.

```
Router# configure terminal
Router(config)# interface fastethernet0/1
Router(config-if)# cdp enable
Router(config-if)# end
```

Monitoring and Maintaining CDP

To monitor and maintain CDP on your device, perform one or more of these tasks, beginning in privileged EXEC mode:

Command	Description
clear cdp counters	Resets the traffic counters to zero.
clear cdp table	Deletes the CDP table of information about neighbors.
show cdp	Displays global information, such as frequency of transmissions and the holdtime for packets being sent.
show cdp entry *entry-name* [**protocol** | **version**]	Displays information about a specific neighbor. You can enter an asterisk (*) to display all CDP neighbors, or you can enter the name of the neighbor about which you want information. You can also limit the display to information about the protocols enabled on the specified neighbor or information about the version of software running on the device.
show cdp interface [*interface-id*]	Displays information about interfaces where CDP is enabled. You can limit the display to the interface about which you want information.
show cdp neighbors [*interface-id*] [**detail**]	Displays information about neighbors, including device type, interface type and number, holdtime settings, capabilities, platform, and port ID. You can limit the display to neighbors of a specific interface or expand the display to provide more detailed information.
show cdp traffic	Displays CDP counters, including the number of packets sent and received and checksum errors.