Cisco Discovery Protocol Configuration Guide, Cisco IOS Release 12.4T

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

Using Cisco Discovery Protocol 1

- Finding Feature Information 1
- Prerequisites for Using CDP 1
- Restrictions for Using CDP 1
- Information About Using CDP 2
  - VLAN Trunking Protocol 2
  - Type-Length-Value Fields 2
  - CDP 4
    - Using CDP with SNMP 4
    - CDP and On-Demand Routing Support for ATM PVCs 5
    - CDP Support in IPv6 5
    - CDP Enhancements for Location Support 5
  - Benefits of CDP 5
- How to Use CDP 5
  - Disabling and Enabling CDP on a Supported Device 6
    - Disabling CDP on a Supported Device 6
    - Enabling CDP on a Supported Device 7
  - Disabling and Enabling CDP on a Supported Interface 7
    - Disabling CDP on a Supported Interface 8
    - Enabling CDP on a Supported Interface 9
  - Setting the Transmission Timer and Hold Time 10
  - Disabling and Reenabling CDP Version 2 Advertisements 11
    - Disabling CDP Version 2 Advertisements 12
    - Enabling CDP Version 2 Advertisements 12
  - Configuring Location Support on CDP 13
  - Monitoring and Maintaining CDP 15
- Configuration Examples for Using CDP 17
  - Example Setting the Transmission Timer and Hold Time 17
  - Example Monitoring and Maintaining CDP 17

Additional References 18

Feature Information for Using CDP 19

Using Cisco Discovery Protocol

Cisco Discovery Protocol (CDP) is a Layer 2 media-independent and network-independent protocol that runs on Cisco devices and enables networking applications to “learn” about nearby, directly connected devices. This protocol facilitates the management of Cisco devices by discovering these devices, determining how they are configured, and allowing systems using different network-layer protocols to learn about one another.

This module describes CDP and how it functions with Simple Network Management Protocol (SNMP).

- Finding Feature Information, page 1
- Prerequisites for Using CDP, page 1
- Restrictions for Using CDP, page 1
- Information About Using CDP, page 2
- How to Use CDP, page 5
- Configuration Examples for Using CDP, page 17
- Additional References, page 18
- Feature Information for Using CDP, page 19

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Using CDP

- Interfaces must support Subnetwork Access Protocol (SNAP) headers.

Restrictions for Using CDP

- CDP functions only on Cisco devices.
- CDP is not supported on Frame Relay multipoint subinterfaces.

Information About Using CDP

- VLAN Trunking Protocol, page 2
- Type-Length-Value Fields, page 2
- CDP, page 4
- Benefits of CDP, page 5

VLAN Trunking Protocol

VLAN Trunking Protocol (VTP) is a discovery technique that is used by switches. A 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 a single device or interconnected devices that share the same VTP domain name. A switch can be in only one VTP domain.

Type-Length-Value Fields

Type-Length-Value (TLV) fields are blocks of information embedded in CDP advertisements. Information in advertisements varies, and the TLV frame format allows for extending advertisements when needed. The table below summarizes the TLV definitions.

Table 1 Type-Length-Value Definitions for CDP v2

TLV	Definition
Address TLV	Contains the network addresses of both receiving and sending devices.
Application TLV	Provides a mechanism to send an application-specific TLV through CDP.
Capabilities TLV	Identifies the device type, which indicates the functional capability of the device; for example, a switch.
Device-ID TLV	Identifies the device name in the form of a character string.
Full/Half Duplex TLV	Indicates the duplex configuration of the CDP broadcast interface. Used by network operators to diagnose connectivity problems between adjacent network devices.
IP Network Prefix TLV	Contains a list of network prefixes to which the sending device can forward IP packets. A prefix includes the interface protocol and port number; for example, Ethernet 1/0.

TLV	Definition
Location TLV	Delivers location-based information to endpoint devices through switches, routers, or access devices using the CDP mechanism. The location TLV can send the following types of information: • Civic location information--Provides the civic address information and postal information. Examples of civic location information are street address, road name, and postal community name information. • ELIN location information--Provides the location information of a caller. The location is determined by the emergency location identifier number (ELIN), which is a phone number that routes an emergency call to the local public safety answering point (PSAP) and which the PSAP can use to call back the emergency caller. You must configure the location TLV on the device before CDP can deliver location-based information to endpoint devices. For more information on configuring location TLV, refer to *Using Link Layer Discovery Protocol in Multivendor Networks*.
Location-server TLV	Provides a mechanism for location servers to transfer the required information to the neighbor devices.
Native VLAN TLV	Indicates, per interface, the assumed VLAN for untagged packets on the interface. CDP learns the native VLAN for an interface. This field is implemented only for interfaces that support the IEEE 802.1Q protocol.
Platform TLV	Identifies the hardware platform of the device; for example, Cisco 4500.
Port-ID TLV	Identifies the port on which a CDP packet is sent.
Version TLV	Contains information about the software release that is running on the device.
VTP Management Domain TLV	Advertises the system's configured VTP management domain name. Used by network operators to verify VTP domain configuration in adjacent network nodes.

CDP

CDP is a Layer 2 media-independent and network-independent protocol that networking applications use to learn about nearby, directly connected devices. It is enabled by default. Each device configured for CDP advertises at least one address at which it can receive messages and sends periodic advertisements (messages) to the well-known multicast address 01:00:0C:CC:CC:CC. Devices discover each other by listening at that address. They also listen to messages to learn when interfaces on the other devices are up or go down.

Advertisements contain time-to-live information, which indicates the length of time a receiving device should hold CDP information before discarding it. Advertisements supported and configured in the Cisco IOS software are sent by default every 60 seconds on interfaces that support SNAP headers. Cisco devices never forward CDP packets. Each Cisco device that supports CDP stores the information it receives in a table. Information in the table is refreshed each time an advertisement is received, and information about a device is discarded after three advertisements from that device are missed.

The information contained in CDP advertisements varies by the type of device and the version of the operating system running on it. Following is some of the information that CDP can learn:

- Cisco IOS version running on a Cisco device
- Hardware platform of the device
- IP addresses of the interfaces on devices
- Locally connected devices advertising CDP
- Interfaces active on a Cisco device, including encapsulation type
- Hostname
- Duplex setting
- VTP domain
- Native VLAN

CDP version 2 provides more intelligent device tracking features than those available in version 1. One feature is an enhanced reporting mechanism for more rapid error tracking, which helps to reduce network downtime. Errors reported include mismatched native VLAN IDs (IEEE 802.1Q) on connected ports and mismatched port duplex states between connected devices. Messages about reported errors can be sent to the console or to a logging server.

Cisco IOS CDP **show** commands can provide detailed output on VTP management domains and duplex modes of neighboring devices, counters related to CDP, and VLAN IDs of connecting ports.

- Using CDP with SNMP, page 4
- CDP and On-Demand Routing Support for ATM PVCs, page 5
- CDP Support in IPv6, page 5
- CDP Enhancements for Location Support, page 5

Using CDP with SNMP

Using CDP with SNMP 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.

The SNMP management application learns protocol addresses and types of neighboring devices by retrieving the CDP tables from SNMP agents in those devices. When enabled, the network management module (NMM) SNMP agent discovers neighboring devices and builds its local cache with information about these devices. A management workstation can retrieve this cache by sending SNMP requests to access the CISCO-CDP-MIB.

CDP and On-Demand Routing Support for ATM PVCs

In Cisco IOS Release 12.2(8)T CDP and On-Demand Routing (ODR) support was added for ATM point-to-point permanent virtual circuits (PVCs). ODR uses CDP to propagate IP address information in hub-and-spoke topologies. When ODR is enabled, spoke routers automatically advertise their subnets using CDP.

CDP is disabled by default on ATM PVC interfaces. To enable CDP, use the **cdp run** command in global configuration mode and the **cdp enable** command in interface configuration mode command on both ends of the PVC. To enable ODR, use the router odr command in global configuration mode on the hub router and turn off all dynamic routing protocols in the spoke routers. For details on configuring ODR, see http://www.cisco.com/en/US/docs/ios/iproute_odr/configuration/guide/ird_odrconfg.html.

CDP Support in IPv6

CDP in IPv6 functions the same as IPv4 and offers the same benefits as in IPv4. IPv6 enhancements allow CDP to exchange IPv6 and neighbor addressing information, provide IPv6 information to network management products, and provide troubleshooting tools.

CDP Enhancements for Location Support

The CDP Medianet Support feature allows CDP to identify the endpoint devices and provides the ability to exchange the medianet location information between endpoint and switch. Location information can be provisioned statically by the user on the platform, or can be received through updates from the location server, or can be received from the endpoint itself through CDP.

The Propagation of Location Info over CDP feature ensures location information to be transmitted from wired switches over CDP to the attached end devices.

CDP allows only one wired switch to report the location information by identifying and indicating the location of neighbor ports not to report the duplicate location information of the same device.

For more information on location TLVs, refer to *Using Link Layer Discovery Protocol in Multivendor Networks*.

Benefits of CDP

CDP provides the following benefits:

- Allows systems using different network-layer protocols to learn about one another.
- Facilitates managing Cisco devices by discovering them and how they are configured.
- Assists with troubleshooting TLV fields.
- Functions with SNMP to learn SNMP agent addresses and to send SNMP queries.

How to Use CDP

- Disabling and Enabling CDP on a Supported Device, page 6
- Disabling and Enabling CDP on a Supported Interface, page 7
- Setting the Transmission Timer and Hold Time, page 10
- Disabling and Reenabling CDP Version 2 Advertisements, page 11
- Configuring Location Support on CDP, page 13

- Monitoring and Maintaining CDP, page 15

Disabling and Enabling CDP on a Supported Device

Perform the following tasks to disable and enable CDP on a supported device:

- Disabling CDP on a Supported Device, page 6
- Enabling CDP on a Supported Device, page 7

Disabling CDP on a Supported Device

Perform this task to disable CDP on a Cisco device.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **no cdp run**
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**no cdp run** **Example:** `Router(config)# no cdp run`	Disables CDP on a supported device.
Step 4	**end** **Example:** `Router(config)# end`	Returns the command-line interface (CLI) to privileged EXEC mode.

Enabling CDP on a Supported Device

Perform this task to enable CDP on a Cisco device.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cdp run**
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cdp run** **Example:** `Router(config)# cdp run`	Enables CDP on a supported device.
Step 4	**end** **Example:** `Router(config)# end`	Returns the CLI to privileged EXEC mode.

Disabling and Enabling CDP on a Supported Interface

CDP is enabled by default on supported interfaces on a Cisco device. To disable or reenable CDP on an interface, perform these tasks:

- Disabling CDP on a Supported Interface, page 8
- Enabling CDP on a Supported Interface, page 9

Disabling CDP on a Supported Interface

Perform this task to disable CDP on a supported interface.

Note If the encapsulation for an interface is changed, it reenables CDP on that interface, even if CDP is previously disabled. For example, when interface encapsulation changes from PPP to HDLC, CDP becomes active even if it is explicitly disabled with the **no cdp run** command on that interface. This behavior is by design. The encapsulation changes the Layer 2 protocol configured for that interface and resets the interface configuration to its default CDP state of enabled, assuming CDP is enabled globally on the device.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number* [*name-tag*]
4. **no cdp enable**
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* [*name-tag*] **Example:** `Router(config)# interface ethernet 0/1`	Configures the specified interface and places the CLI in interface configuration mode.
Step 4	**no cdp enable** **Example:** `Router(config-if)# no cdp enable`	Disables CDP on the interface. **Note** If the encapsulation for an interface is changed, it reenables CDP on that interface, even if CDP is previously disabled.

	Command or Action	Purpose
Step 5	**end** **Example:** `Router(config-if)# end`	Returns the CLI to privileged EXEC mode.

Example

If the encapsulation for an interface is changed, it reenables CDP on that interface, even if CDP is previously disabled. For example, when the interface encapsulation changes from PPP to HDLC, CDP become active even if it is explicitly disabled with the **no cdp run** command on that interface. This behavior is by design. The encapsulation changes the Layer 2 protocol configured for that interface and resets the interface configuration to its default CDP state of enabled, assuming CDP is enabled globally on the device.

The following examples show that when the encapsulation for an interface is changed, it reenables CDP on that interface, even if CDP is previously disabled:

```
interface POS3/0
no ip address
encapsulation ppp
shutdown
no cdp enable <<<<<<<<<<CDP Disabled
end
```

The following example shows that after CDP is disabled, the encapsulation for the interface is changed from PPP to HDLC:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface fastethernet 3/0
Router(config-if)# encap hdlc
    <<<<<<<<<<<<Encapsulation changed from ppp to hdlc.
Router(config-if)# do show running interface fastethernet 3/0
Current configuration : 49 bytes
!
```

The following example shows that CDP is reenabled after the encapsulation for the interface is changed.

```
interface POS3/0
no ip address
shutdown        <<<<<<<<<<<<CDP is now back on. You don't see it here previously disabled.
end
```

Enabling CDP on a Supported Interface

Perform this task to enable CDP on a supported interface.

Note If the encapsulation for an interface is changed, it reenables CDP on that interface, even if CDP is previously disabled.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number* [*name-tag*]
4. **cdp enable**
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* [*name-tag*] **Example:** `Router(config)# interface ethernet 0/1`	Configures the specified interface and places the CLI in interface configuration mode. **Note** If the encapsulation for an interface is changed, it reenables CDP on that interface, even if CDP is previously disabled.
Step 4	**cdp enable** **Example:** `Router(config-if)# cdp enable`	Enables CDP on the interface.
Step 5	**end** **Example:** `Router(config-if)# end`	Returns the CLI to privileged EXEC mode.

Setting the Transmission Timer and Hold Time

Perform this task to set the frequency of CDP transmissions and the hold time for CDP packets.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cdp timer** *seconds*
4. **cdp holdtime** *seconds*
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cdp timer** *seconds* **Example:** `Router(config)# cdp timer 30`	Specifies the frequency of transmission of CDP packets.
Step 4	**cdp holdtime** *seconds* **Example:** `Router(config)# cdp holdtime 90`	Specifies the amount of time a receiving device should hold information before discarding it.
Step 5	**end** **Example:** `Router(config)# end`	Returns the CLI to privileged EXEC mode.

Disabling and Reenabling CDP Version 2 Advertisements

The broadcasting of CDP version 2 advertisements is enabled by default on Cisco devices. To disable or reenable this broadcasting, perform these tasks.

- Disabling CDP Version 2 Advertisements, page 12
- Enabling CDP Version 2 Advertisements, page 12

Disabling CDP Version 2 Advertisements

Perform this task to disable CDP version 2 advertisements.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **no cdp advertise-v2**
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**no cdp advertise-v2** **Example:** `Router(config)# no cdp advertise-v2`	Disables the broadcasting of CDP version 2 advertisements.
Step 4	**end** **Example:** `Router(config)# end`	Returns the CLI to privileged EXEC mode.

Enabling CDP Version 2 Advertisements

Perform this task to enable CDP version 2 advertisements.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cdp advertise-v2**
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cdp advertise-v2** **Example:** `Router(config)# cdp advertise-v2`	Enables the broadcasting of CDP version 2 advertisements.
Step 4	**end** **Example:** `Router(config)# end`	Returns the CLI to privileged EXEC mode.

Configuring Location Support on CDP

Perform this task to configure location support on CDP.

You must configure the location TLV before configuring location support on CDP. For more information on configuring location TLV, refer to *Using Link Layer Discovery Protocol in Multivendor Networks*.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cdp tlv** {**app** | **location**| **location-server**}
4. **exit**
5. **interface** *type number*
6. **cdp tlv** {**app**[**tlvtype** *tlvtype* **value** *value*]| **location** | **location-server**}
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cdp tlv** {**app**	**location**| **location-server**} **Example:** `Router(config)# cdp tlv app`	Configures location support in CDP.
Step 4	**exit** **Example:** `Router(config-civic)# exit`	Returns the CLI to global configuration mode.
Step 5	**interface** *type number* **Example:** `Router(config)# interface fastethernet 0`	Specifies the interface on which you are configuring the location support for CDP, and enters interface configuration mode.

	Command or Action	Purpose
Step 6	**cdp tlv** {**app**[**tlvtype** *tlvtype* **value** *value*]| **location**	**location-server**} **Example:** `Router(config-if)# cdp tlv tlvtype 20 value test12`	Configures location support in CDP on a specified interface.
Step 7	**end** **Example:** `Router(config-if-port)# end`	Returns the CLI to privileged EXEC mode.

Monitoring and Maintaining CDP

To monitor and maintain CDP on your device, perform the following steps. This task and all steps are optional, and you do not have to perform the steps in the sequence shown.

SUMMARY STEPS

1. **enable**
2. **clear cdp counters**
3. **clear cdp table**
4. **show cdp**
5. **show cdp entry** *device-name* [**protocol** | **version**]
6. **show cdp interface** [*type number*]
7. **show cdp neighbors** [*type number*] [**detail**]
8. **show cdp traffic**
9. **show debugging**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**clear cdp counters** **Example:** `Router# clear cdp counters`	Resets the traffic counters to zero.
Step 3	**clear cdp table** **Example:** `Router# clear cdp table`	Deletes the CDP table of information about neighbors.
Step 4	**show cdp** **Example:** `Router# show cdp`	Displays the interval between advertisements, the number of seconds the advertisement is valid for a given port, and the version of the advertisement.
Step 5	**show cdp entry** *device-name* [**protocol** | **version**] **Example:** `Router# show cdp entry test-device protocol`	Displays information about a specific neighbor. • The output can be limited to protocol or version information.
Step 6	**show cdp interface** [*type number*] **Example:** `Router# show cdp interface`	Displays information about interfaces on which CDP is enabled.
Step 7	**show cdp neighbors** [*type number*] [**detail**] **Example:** `Router# show cdp neighbors`	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 interface, the device type, the device product number, and the port ID. Issuing the **detail** keyword displays information about the native VLAN ID, the duplex mode, and the VTP domain name associated with neighbor devices.
Step 8	**show cdp traffic** **Example:** `Router# show cdp traffic`	Displays CDP counters, including the number of packets sent and received and checksum errors.

	Command or Action	Purpose
Step 9	**show debugging** **Example:** `Router# show debugging`	Displays information about the types of debugging that are enabled for the router.

Configuration Examples for Using CDP

The following examples show how to set transmission timer and hold time values and show commands you can issue to monitor and maintain CDP.

- Example Setting the Transmission Timer and Hold Time, page 17
- Example Monitoring and Maintaining CDP, page 17

Example Setting the Transmission Timer and Hold Time

In the following example, the timer is set to send updates every 30 seconds and a **show cdp interface** command is issued to show that the update is effective:

```
Router(config)# cdp timer 30
Router(config)# end
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 hold time is set to 90 seconds and a **show cdp interface** command is issued to show that the update is effective:

```
Router(config)# cdp holdtime 90
Router(config)# end
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 commands you can issue to view CDP information:

```
Router# show cdp
Global CDP information:
        Sending CDP packets every 60 seconds
        Sending a holdtime value of 180 seconds
        Sending CDPv2 advertisements is enabled

Router# 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 Interfce     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
Router# 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
 .
 .
 .
Router# 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
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS CDP commands	*Cisco IOS Network Management Command Reference*
Configuring SNMP Support	“Configuring SNMP Support” module
Debugging commands	*Cisco IOS Debug Command Reference*
Configuring On-Demand Routing	“Configuring On-Demand Routing” module
Configuring Location TLVs	“Using Link Layer Discovery Protocol in Multivendor Networks” module

Standards

Standard	Title
IEEE 802.1Q	*Virtual LANS*

MIBs

MIB	MIBs Link
• CISCO-CDP MIB	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported, and support for existing RFCs has not been modified.	--

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Using CDP

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 2 Feature Information for Configuring CDP

Feature Name	Releases	Feature Information
CDP Medianet Support	12.2(55)SE	The CDP Medianet Support feature allows CDP to identify the endpoint devices and provides the ability to exchange the medianet location information between endpoint and switch.

Feature Name	Releases	Feature Information
Configuring CDP	10.3, 11.2(1) 12.2(8)T	CDP is a Layer 2 media-independent and network-independent protocol that runs on Cisco devices and enables networking applications to “learn” about nearby, directly connected devices. This protocol facilitates the management of Cisco devices and allows systems using different network-layer protocols to learn about one another.
Propagation of Location Info over CDP	12.2(55)SE	The Propagation of Location Info over CDP ensures location information to be transmitted from wired switches over CDP to the attached end devices. The following commands were introduced or modified: **cdp tlv**, **show cdp tlv**, **debug cdp events**.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.