

Cisco Discovery Protocol Version 2

Cisco Discovery Protocol (formerly known as CDP) is a Layer 2, media-independent, and network-independent protocol that runs on Cisco devices and enables networking applications to learn about directly connected devices nearby. 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 each other.

This module describes Cisco Discovery Protocol Version 2 and how it functions with Simple Network Management Protocol (SNMP).

- Prerequisites for Using Cisco Discovery Protocol, on page 1
- Restrictions for Using Cisco Discovery Protocol, on page 1
- Information About Using Cisco Discovery Protocol, on page 2
- How to Use Cisco Discovery Protocol Version 2, on page 5
- Configuration Examples for Cisco Discovery Protocol Version 2, on page 14
- Additional References for Cisco Discovery Protocol Version 2, on page 14

Prerequisites for Using Cisco Discovery Protocol

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

Restrictions for Using Cisco Discovery Protocol

- Cisco Discovery Protocol functions only on Cisco devices.
- Cisco Discovery Protocol is not supported on Frame Relay multipoint subinterfaces.
- If a neighbor has no IP address on an interface enabled with Cisco Discovery Protocol, the IP address of another interface will be updated as IP address for the non-IP address interface.
- Cisco Discovery Protocol is *not* supported on encapsulation default interface.
- Cisco Discovery Protocol packets are received untagged when the connected switch trunk port uses the default native VLAN.
- Cisco Discovery Protocol packets are received with 802.1Q VLAN 1 tag when the connected switch trunk port uses non-default native VLAN.

- When connecting a router to a switch trunk port configured with a non-default native VLAN, you must configure an encapsulation dot1q 1 Ethernet Flow Point (EFP) instance on the router to process Cisco Discovery Protocol packets correctly.

Information About Using Cisco Discovery Protocol

VLAN Trunking Protocol

VLAN Trunking Protocol (VTP) is a discovery technique used by switches. A switch advertises its management domain, configuration revision number, VLANs, and their specific parameters on its trunk ports. A VTP domain is made up of a single device or interconnected devices that share the same VTP domain name. A switch can belong to only one VTP domain.

Type-Length-Value Fields

Type-Length-Value (TLV) fields are blocks of information embedded in Cisco Discovery Protocol 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 Cisco Discovery Protocol Version 2

TLV	Definition
Address TLV	Contains network addresses of both receiving and sending devices.
Application TLV	Provides a mechanism to send an application-specific TLV through Cisco Discovery Protocol.
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 or Half Duplex TLV	Indicates the duplex configuration of the Cisco Discovery Protocol broadcast interface. This information is used by network operators to diagnose connectivity problems between adjacent network devices.
IP Network Prefix TLV	Contains a list of network prefixes to which a sending device can forward IP packets. A prefix includes the interface protocol and the port number. For example, Ethernet 1/0.

TLV	Definition
Location TLV	Delivers location-based information to endpoint devices through access devices (switches or routers) by using Cisco Discovery Protocol. The location TLV can send the following types of information: • Civic location information—Provides the civic address information and the postal information. Examples include street address, road name, and postal community name. • 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 Cisco Discovery Protocol can deliver location-based information to endpoint devices. For more information about configuring location TLV, see the *Using Link Layer Discovery Protocol in Multivendor Networks* module.
Location-Server TLV	Provides a mechanism for location servers to transfer the required information to neighboring devices.
Native VLAN TLV	Indicates, per interface, the assumed VLAN for untagged packets on the interface. Cisco Discovery Protocol 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 Cisco Discovery Protocol packet is sent.
Version TLV	Contains the device software release information.
VTP Management Domain TLV	Advertises the configured VLAN Trunking Protocol (VTP)-management-domain name of the system. This name is used by network operators to verify VTP-domain configuration in adjacent network nodes.

Cisco Discovery Protocol

Cisco Discovery Protocol is a Layer 2, media-independent, and network-independent protocol that networking applications use to learn about nearby, directly connected devices. Cisco Discovery Protocol is enabled by default. Each device configured for Cisco Discovery Protocol advertises at least one address at which the device 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 other devices are up or go down.

Advertisements contain time-to-live information, which indicates the length of time a receiving device should hold Cisco Discovery Protocol information before discarding it. Advertisements supported and configured in Cisco software are sent, by default, every 60 seconds on interfaces that support Subnetwork Access Protocol (SNAP) headers. Cisco devices never forward Cisco Discovery Protocol packets. Cisco devices that support Cisco Discovery Protocol store the information received in a table. Information in this table is refreshed every time an advertisement is received, and information about a device is discarded after three advertisements from that device are missed.

The information contained in Cisco Discovery Protocol advertisements varies based on the type of device and the installed version of the operating system. Some of the information that Cisco Discovery Protocol can learn includes:

- Cisco IOS version running on Cisco devices
- Hardware platform of devices
- IP addresses of interfaces on devices
- Locally connected devices advertising Cisco Discovery Protocol
- Interfaces active on Cisco devices, including encapsulation type
- Hostname
- Duplex setting
- VLAN Trunking Protocol (VTP) domain
- Native VLAN

Cisco Discovery Protocol Version 2 provides more intelligent, device-tracking features than those available in Version 1. One of the features available 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.

You can use **show** commands for getting detailed output on VTP management domains and duplex modes of neighboring devices, counters related to Cisco Discovery Protocol, and VLAN IDs of connecting ports.

Using Cisco Discovery Protocol with SNMP

Using Cisco Discovery Protocol with Simple Network Management Protocol (SNMP) allows network management applications to learn the type of device and the SNMP agent address of neighboring devices. Applications can also send SNMP queries to these neighboring devices.

The SNMP management application learns protocol addresses and types of neighboring devices by retrieving the Cisco Discovery Protocol tables from SNMP agents on 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 CISCO-CDP-MIB.

Cisco Discovery Protocol and On-Demand Routing Support for ATM PVCs

Cisco Discovery Protocol and On-Demand Routing (ODR) support exists for ATM point-to-point permanent virtual circuits (PVCs). ODR uses Cisco Discovery Protocol to propagate IP address information in hub-and-spoke topologies. When ODR is enabled, spoke routers automatically advertise their subnets by using Cisco Discovery Protocol.

Cisco Discovery Protocol is disabled by default on ATM PVC interfaces. To enable Cisco Discovery Protocol, use the **cdp run** command in global configuration mode and the **cdp enable** command in interface configuration mode 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 on the spoke routers. For details about configuring ODR, see the "Configuring On-Demand Routing" section in the *IP Routing: ODR Configuration Guide*.

Cisco Discovery Protocol Support in IPv6

Cisco Discovery Protocol in IPv6 functions in the same way as in IPv4 and offers the same benefits. The IPv6 enhancement allows Cisco Discovery Protocol to exchange IPv6 and neighbor addressing information. The enhancement also provides IPv6 information to network management products and troubleshooting tools.

Benefits of Cisco Discovery Protocol

Cisco Discovery Protocol provides the following benefits:

- Allows systems using different network layer protocols to learn about one another.
- Facilitates management of Cisco devices by discovering them and discovering how they are configured.
- Assists with troubleshooting Type-Length-Value Fields (TLV) fields.
- Works with SNMP by learning SNMP agent addresses and sending SNMP queries.

How to Use Cisco Discovery Protocol Version 2

Disabling and Enabling Cisco Discovery Protocol on a Cisco Device



Note Upon system restart, CDP will be disabled by default. If CDP is enabled, then the CDP TLV application will also be enabled by default. Should CDP be disabled, the CDP app TLV will be disabled as well. However, if CDP is re-enabled, "no CDP app TLV" will be displayed, which diverges from the default behavior.

Disabling Cisco Discovery Protocol on a Supported Device

SUMMARY STEPS

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

4. **end**

DETAILED STEPS

Procedure

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

Enabling Cisco Discovery Protocol on a Supported Device

SUMMARY STEPS

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

DETAILED STEPS

Procedure

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

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**cdp run** **Example:** `Device(config)# cdp run`	Enables Cisco Discovery Protocol on a supported device.
Step 4	**end** **Example:** `Device(config)# end`	Exits configuration mode and returns to privileged EXEC mode.

Disabling and Enabling Cisco Discovery Protocol on a Supported Interface

Disabling Cisco Discovery Protocol on a Supported Interface

If the encapsulation of an interface is changed, Cisco Discovery Protocol is reenabled on that interface even if Cisco Discovery Protocol was previously disabled. For example, when interface encapsulation changes from PPP to High-Level Data Link Control (HDLC), Cisco Discovery Protocol is reenabled on that interface even though it was 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 the default Cisco Discovery Protocol state of being enabled, assuming that Cisco Discovery Protocol 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

Procedure

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

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* [*name-tag*] **Example:**	Configures the specified interface and enters interface configuration mode.
Step 4	**no cdp enable** **Example:** `Device(config-if)# no cdp enable`	Disables Cisco Discovery Protocol on the interface. **Note** If the encapsulation of an interface is changed, Cisco Discovery Protocol is reenabled on that interface even if Cisco Discovery Protocol was previously disabled.
Step 5	**end** **Example:** `Device(config-if)# end`	Exits to privileged EXEC mode.

Example

In the following example, Cisco Discovery Protocol is first disabled on an interface:

```
Device(config)#
Device(config-if)# no ip address

Device(config-if)# shutdown
Device(config-if)# no cdp enable
! Cisco Discovery Protocol is disabled.
Device(config-if)# end
```

Enabling Cisco Discovery Protocol on a Supported Interface



Note If the encapsulation of an interface is changed, Cisco Discovery Protocol is reenabled on that interface, even if Cisco Discovery Protocol was previously disabled.

SUMMARY STEPS

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

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* [*name-tag*] **Example:** `Device(config)# interface Gigabitethernet 1/0/1`	Configures the specified interface and places the CLI in interface configuration mode. **Note** If the encapsulation of an interface is changed, Cisco Discovery Protocol is reenabled on that interface, even if Cisco Discovery Protocol was previously disabled.
Step 4	**cdp enable** **Example:** `Device(config-if)# cdp enable`	Enables Cisco Discovery Protocol on the interface.
Step 5	**end** **Example:** `Device(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 Cisco Discovery Protocol transmissions and the hold time for Cisco Discovery Protocol packets.

SUMMARY STEPS

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

DETAILED STEPS

Procedure

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

Disabling and Reenabling Cisco Discovery Protocol Version 2 Advertisements

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

Disabling Cisco Discovery Protocol Version 2 Advertisements

SUMMARY STEPS

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

DETAILED STEPS

Procedure

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

Enabling Cisco Discovery Protocol Version 2 Advertisements

SUMMARY STEPS

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

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	`Device# configure terminal`	
Step 3	**cdp advertise-v2** **Example:** `Device(config)# cdp advertise-v2`	Enables the broadcasting of Cisco Discovery Protocol Version 2 advertisements.
Step 4	**end** **Example:** `Device(config)# end`	Exits to privileged EXEC mode.

Monitoring and Maintaining Cisco Discovery Protocol

Perform this task to monitor and maintain Cisco Discovery Protocol on a device. This task and all its steps are optional, and the steps can be performed in any sequence.

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

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**clear cdp counters** **Example:** `Device# clear cdp counters`	Resets Cisco Discovery Protocol traffic counters to zero.

	Command or Action	Purpose
Step 3	**clear cdp table** **Example:** `Device# clear cdp table`	Clears the table that contains Cisco Discovery Protocol information about neighbors.
Step 4	**show cdp** **Example:** `Device# show cdp`	Displays the interval between advertisements, the number (in seconds) for which an advertisement is valid for a given port, and the version of the advertisement.
Step 5	**show cdp entry** *device-name* [**protocol** | **version**] **Example:** `Device# show cdp entry test-device protocol`	Displays information about a specific neighbor.
Step 6	**show cdp interface** [*type number*] **Example:** `Device# show cdp interface`	Displays information about interfaces on which Cisco Discovery Protocol is enabled.
Step 7	**show cdp neighbors** [*type number*] [**detail**] **Example:** `Device# 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 time (in seconds) the Cisco Discovery Protocol advertisement is valid for the interface, the device type, the device product number, and the port ID. • The **detail** keyword displays information about the native VLAN ID, the duplex mode, and the VTP domain name associated with neighboring devices.
Step 8	**show cdp traffic** **Example:** `Device# show cdp traffic`	Displays information about Cisco Discovery Protocol traffic, including the number of packets sent and received and checksum errors.
Step 9	**show debugging** **Example:** `Device# show debugging`	Displays information about the types of debugging that are enabled for the device.

Configuration Examples for Cisco Discovery Protocol Version 2

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 used to verify that the update is effective:

```
Device(config)# cdp timer 30
Device(config)# end
Device# 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 used to verify that the update is effective:

```
Device(config)# cdp holdtime 90
Device(config)# end
Device# 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 Cisco Discovery Protocol

The following example shows a series of commands that you can use to view Cisco Discovery Protocol information:

Additional References for Cisco Discovery Protocol Version 2

Related Documents

Related Topic	Document Title
Cisco Discovery Protocol commands	Cisco IOS Cisco Discovery Protocol Command Reference
SNMP support configuration tasks	“Configuring SNMP Support” module
On-Demand Routing configuration tasks	“Configuring On-Demand Routing” module
Debug commands	Cisco IOS Debug Command Reference

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

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