

Configure CDP

- Feature History for CDP, on page 1
- Prerequisites for Using Cisco Discovery Protocol, on page 1
- Restrictions for Using Cisco Discovery Protocol, on page 2
- Cisco Discovery Protocol, on page 2
- Cisco Discovery Protocol Bypass, on page 4
- Cisco Discovery Protocol IPv6 Support, on page 5

Feature History for CDP

This table provides release and platform support information for the features explained in this module.

These features are available in all the releases subsequent to the one they were introduced in, unless noted otherwise.

Table 1:

Release	Feature Name and Description	Supported Platform
Cisco IOS XE 26.2.1ea	Cisco Discovery Protocol: CDP feature support has been introduced.	Cisco C9550 Series Smart Switches
Cisco IOS XE 17.18.1	Cisco Discovery Protocol (CDP) is a proprietary Layer 2 network protocol that operates on Cisco devices. It enables devices to discover directly connected Cisco equipment and gather vital information about neighboring devices, facilitating network management and troubleshooting.	Cisco C9350 Series Smart Switches Cisco C9610 Series Smart Switches

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.

Cisco Discovery Protocol

Cisco Discovery Protocol (CDP) is a proprietary Layer 2 network protocol that operates on Cisco devices. It enables devices to discover directly connected Cisco equipment and gather vital information about neighboring devices, facilitating network management and troubleshooting.

CDP operates in two primary versions:

- **CDPv1:** This initial version provides basic information about directly connected Cisco devices. This includes details such as their device ID, the local interface connected, the platform type, the device's capabilities (e.g., router, switch, host), its Cisco IOS version, and its IP address.
- **CDPv2:** This enhanced version builds upon CDPv1 by adding more detailed information. This includes the VLAN Trunking Protocol (VTP) domain name, the native VLAN used on the connected port, the duplex mode of the interface, and power consumption details for Power over Ethernet (PoE) devices.

CDP offers several advantages for network administrators, enhancing network visibility and simplifying operations:

- **Network Topology Discovery:** CDP automatically maps the network topology by identifying how Cisco devices connect to each other. This eliminates the need for manual mapping, which is particularly beneficial in large or complex network environments.
- **Troubleshooting Connectivity Issues:** By displaying comprehensive information about directly connected devices and their configurations, CDP helps you quickly identify and resolve common connectivity problems, such as duplex mismatches or incorrect VLAN assignments.
- **Inventory Management:** CDP provides a real-time inventory of connected Cisco devices, including their specific hardware platforms and software versions. This assists in asset tracking and compliance.
- **Simplified Configuration:** CDP can facilitate the auto-configuration of certain devices, such as Cisco IP phones, by providing them with necessary network parameters like VLAN information.

After understanding Cisco Discovery Protocols, you will be able to:

- Identify the version of CDP running on your devices.
- Verify information about directly connected Cisco devices.
- Leverage CDP for network discovery and basic troubleshooting.

How Cisco Discovery Protocol Works

CDP-enabled devices periodically send multicast advertisements to directly connected neighboring devices. These advertisements contain various pieces of information about the sending device, including its identity, capabilities, and configuration details. Receiving devices store this information in a local CDP table. You can then view this table using Command Line Interface (CLI) commands to gain insights into your network's immediate connections.

Configure Cisco Discovery Protocol

Procedure

	Command or Action	Purpose

Step 1	cdp run
	Example:
	`Device# configure terminal`
	`Device(config)# cdp run`
	`Device(config)# end`
		To enable CDP globally on a device, enter global configuration mode. Use the cdp run command.

Step 2	no cdp run
	Example:
	`Device# configure terminal`
	`Device(config)# no cdp run`
	`Device(config)# end`
		To disable CDP globally, enter global configuration mode. Use the no cdp run command.

Step 3	cdp enable
	Example:
	`Device# configure terminal`
	`Device(config)# interface GigabitEthernet0/1`
	`Device(config-if)# cdp enable`
	`Device(config-if)# end`
		To enable CDP on a specific interface, enter interface configuration mode for the desired interface. Use the cdp enable command.

Step 4	no cdp enable
	Example:
	`Device# configure terminal`
	`Device(config)# interface GigabitEthernet0/1`
	`Device(config-if)# no cdp enable`
	`Device(config-if)# end`
		To disable CDP on a specific interface, enter interface configuration mode for the desired interface. Use the no cdp enable command.

Verify Cisco Discovery Protocol

You can verify CDP status and view the information about neighboring devices using various show cdp commands.

Procedure

	Command or Action	Purpose

Step 1	show cdp neighbors
	Example:
	`Router# show cdp neighbors`
	`Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge, S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone, D - Remote, C - CVTA, M - Two-port Mac Relay`
	`Device ID Local Intrfce Holdtme Capability Platform Port ID`
	`Switch1 GigabitEthernet0/1 120 S I WS-C9350-24P GigabitEthernet1/0/1`
	`IP_Phone GigabitEthernet0/2 175 H P IP Phone Port 1`
		To view information about directly connected Cisco devices, enter the show cdp neighbors command in privileged EXEC mode.

Cisco Discovery Protocol Bypass

Cisco Discovery Protocol (CDP) Bypass describes scenarios or configurations where the standard CDP discovery mechanism is intentionally or unintentionally circumvented, preventing devices from exchanging information about their neighbors. This concept is crucial for understanding network visibility and security implications.

Understanding CDP Bypass enables you to:

- **Manage Network Visibility:** Control which devices are discoverable via CDP, particularly in multi-vendor environments or security-sensitive zones.
- **Enhance Security Posture:** Prevent the leakage of network topology and device information to unauthorized entities or across specific network boundaries.
- **Troubleshoot Connectivity:** Identify why certain devices are not appearing in CDP neighbor tables, which might be due to intentional bypass configurations.

After understanding CDP Bypass, you will be able to:

- Evaluate the implications of CDP's presence or absence on network segments.
- Implement configurations that align with your network's security and operational requirements regarding device discovery.

Scenarios of CDP Bypass

CDP Bypass typically occurs in the following situations:

- **CDP is Disabled:**
  - **Globally on a Device:** When CDP is turned off for the entire switch or router, it will neither send nor receive CDP advertisements, effectively bypassing any CDP discovery.
  - **On a Specific Interface:** CDP can be disabled on individual interfaces. This is common for interfaces connecting to untrusted networks, non-Cisco devices, or in security zones where information disclosure is undesirable.
- **Non-Cisco Devices:** CDP is a proprietary Cisco protocol. Devices from other vendors do not support CDP and therefore inherently "bypass" its discovery capabilities. They will not send or process CDP advertisements.
- **Security Zone Boundaries:** In network designs that enforce strict security boundaries, CDP is often intentionally disabled on interfaces connecting different security zones (e.g., connecting a DMZ to an internal network) to prevent internal network topology details from being exposed.

Implications of CDP Bypass

When CDP is bypassed, either intentionally or unintentionally, consider these implications:

- **Reduced Automated Discovery:** You lose the benefit of automatic network topology mapping and rapid neighbor identification that CDP provides.
- **Increased Security:** By limiting the information exchanged, you reduce the attack surface and prevent potential reconnaissance by malicious actors.
- **Manual Documentation Required:** Without CDP, maintaining accurate network documentation becomes a manual process, requiring up-to-date records of device connections and configurations.
- **Impact on Features:** Some Cisco features, such as Power over Ethernet (PoE) negotiation for IP phones or certain auto-configuration capabilities, may rely on CDP. Disabling CDP might impact the functionality of these features.

Managing Cisco Discovery Protocol

You can manage CDP's operation to achieve a "bypass" state when required.

Cisco Discovery Protocol IPv6 Support

Cisco Discovery Protocol (CDP) IPv6 support refers to the capability of CDP to discover and exchange IPv6 address information between directly connected Cisco devices. This feature extends CDP's traditional IPv4 discovery functions to modern IPv6 networks, providing comprehensive visibility and simplifying management in dual-stack or IPv6-only environments.

CDP IPv6 support enables you to:

- **Gain Visibility in IPv6 Networks:** Discover neighboring Cisco devices and their IPv6 addresses, including link-local and global unicast addresses, in networks where IPv6 is deployed.

- **Simplify Troubleshooting:** Quickly identify IPv6 connectivity issues, verify neighbor reachability, and confirm interface configurations by leveraging CDP's neighbor discovery capabilities.
- **Enhance Network Management:** Maintain an accurate inventory of devices and their IPv6 addressing schemes, crucial for network planning and operational efficiency in IPv6 deployments.

After understanding CDP IPv6 support, you will be able to:

- Verify IPv6 neighbor information using CDP.
- Troubleshoot basic IPv6 connectivity issues between Cisco devices.
- Incorporate CDP IPv6 information into your network documentation and management practices.

How Cisco Discovery Protocol IPv6 Support Works

When CDP IPv6 support is enabled on a device and its interfaces, CDP messages (advertisements) are updated to include IPv6 address information in addition to IPv4 details. These advertisements are sent periodically as multicast frames (both IPv4 and IPv6 multicast addresses are used) to directly connected CDP-enabled neighbors. Receiving devices parse these messages and update their local CDP neighbor tables with the discovered IPv6 addresses, along with other device details.

This allows network administrators to use familiar CDP commands to inspect IPv6 neighbor information, providing a consistent operational experience across IPv4 and IPv6 addressing schemes.

Configure Cisco Discovery Protocol IPv6 Support

Procedure

	Command or Action	Purpose

Step 1	cdp run
	Example:
	`Device# configure terminal`
	`Device(config)# cdp run`
	`Device(config)# end`
		To enable CDP globally, enter global configuration mode. Use the cdp run command.

Step 2	cdp enable
	Example:
	`Device(config)# interface GigabitEthernet1/0/1`
	`Device(config-if)# cdp enable`
	`Device(config-if)# end`
		To enable CDP on a specific interface, enter interface configuration mode. Use the cdp enable command.

Verify Cisco Discovery Protocol IPv6 Support

You can verify CDP IPv6 support and view the IPv6 addresses of neighboring devices using the show cdp neighbors detail command.

Procedure

	Command or Action	Purpose

Step 1	show cdp neighbors detail
	Example:
	`Router# show cdp neighbors detail`
	`------------------------`
	`Device ID: Switch2`
	`Entry address(es):`
	`  IP address: 192.168.1.2`
	`  IPv6 address: 2001:DB8:0:1::2`
	`Platform: cisco WS-C9350-24P,`
	`Capabilities: Switch IGMP`
	`Interface: GigabitEthernet1/0/1, Port ID`
	`(outgoing port): GigabitEthernet1/0/2`
	`Holdtime : 162 sec`
		To view detailed information about directly connected Cisco devices, including their IPv6 addresses, enter the show cdp neighbors detail command in privileged EXEC mode.

Considerations for CDP IPv6 Support

- **Link-Local Addresses:** CDP frequently exchanges link-local IPv6 addresses, which are automatically configured on interfaces and are only valid for communication on the local link. These are essential for neighbor discovery even without global unicast addresses.
- **Security:** As with IPv4, CDP can reveal network topology information. In security-sensitive environments, consider disabling CDP on interfaces connected to untrusted networks to prevent information leakage.
- **Resource Usage:** CDP uses minimal network and CPU resources. However, in very large-scale deployments, managing CDP on all interfaces might require careful planning.