Secure Cisco Discovery Protocol

The Cisco Discovery Protocol does not possess inherent security mechanisms and is vulnerable to attacks. The Secure Cisco Discovery Protocol feature allows users to select the type, length, value (TLV) fields that are sent on a particular interface to filter information sent through Cisco Discovery Protocol packets.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and 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.

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 Secure Cisco Discovery Protocol

The Cisco software image must support basic Cisco Discovery Protocol functions.

Restrictions for Secure Cisco Discovery Protocol

Blocking the type, length, value (TLV) fields on one device can affect the functionality of clients on other devices where Cisco Discovery Protocol packets with blocked TLV fields are received because different clients use different TLV fields.

Information About Secure Cisco Discovery Protocol

Secure Cisco Discovery Protocol

The Cisco Discovery Protocol does not possess inherent security mechanisms and is vulnerable to attacks. The Secure Cisco Discovery Protocol feature provides security by allowing users to select the type, length, value (TLV) fields that are sent on an interface to filter the fields in Cisco Discovery Protocol packets.

This feature supports the following functions:

- TLV lists can be configured globally and also at the interface level, but only one TLV fields list can be configured globally.
- A TLV list configured on an interface is given a higher precedence.
- All TLVs except the Device-ID TLV and the Application TLV can be blocked.
- Information about the Cisco Discovery Protocol TLV list configured on an interface is stored in each Cisco Discovery Protocol interface subblock.
- All TLVs are blocked on the sending side.
- The **cdp tlv-list** and **cdp filter-tlv-list** commands are required to configure a Cisco Discovery Protocol list and apply the list globally or on an interface.
- The **show cdp tlv-list** and **show cdp interface** commands display information about the TLV list.

Supported Type, Length, Value Fields

Table 1: Supported TLV fields

Related command in TLV list configuration mode	TLV Fields	Description
address	Address TLV	Contains a list of device network-layer addresses. If a device uses Simple Network Management Protocol (SNMP), the first address is an address at which the device receives SNMP messages. The device may advertise all of its addresses and may optionally advertise one or more loopback IP addresses.

Related command in TLV list configuration mode	TLV Fields	Description
capability	Capability TLV	Identifies the device type. The device type indicates the functional capability of the device, for example, a switch.
cos	Class of service TLV	Describes the Layer 2 class of service (CoS) value in a Cisco Discovery Protocol packet. All Cisco Discovery Protocol packets received on an untrusted port are marked with a CoS value by a switching device that cannot classify individual packets. This TLV is used only in a Cisco Discovery Protocol packet that contains an Extended Trust TLV, which indicates the absence of extended trust with a CoS TLV that is one byte in length.
default	Default	Specifies the default state of the configuration.
duplex	Duplex TLV	Allows devices to recognize if a point-to-point Ethernet interface is running in full-duplex or in half-duplex mode. Network problems are caused if two ends of a link are in different modes. The TLV value is one byte in length with its least significant bit indicating the mode. A 1 indicates full-duplex and a 0'indicates half-duplex.
exit	Exit	Exits current configuration.
ext-port-id	External Port Id TLV	Identifies the physical connector port on which a Cisco Discovery Protocol packet is transmitted. This TLV is used in devices with optical ports in which signals from multiple hardware interfaces are multiplexed through a single physical port. The value of this TLV must be the same as the MIB object ifName for the ifTable entry for the external port.

Related command in TLV list configuration mode	TLV Fields	Description
hello-protocol	Protocol-Hello TLV	Specifies that a particular protocol has asked Cisco Discovery Protocol to piggyback its "hello" messages within transmitted Cisco Discovery Protocol packets. The value of this TLV protocol is greater than or equal to 5 and lesser than or equal to 32 bytes. The first 5 bytes are the protocol's 5-byte Subnetwork Access Protocol (SNAP) value, which contains three bytes of organizationally unique identifier (OUI) followed by two bytes of protocol ID. A Cisco Discovery Protocol packet may contain multiple protocol-hello TLVs, each for a different protocol.
ip-prefix	IP Network Prefix TLV	Describes a list of stub network prefixes to which the sending stub device can forward IP packets. These packets are used by On-Demand Routing (ODR). Each network prefix is formatted as a 4-byte IP address followed by a 1-byte network mask length. Thus, the length of the value sent by a stub device is a multiple of 5 bytes.

Related command in TLV list configuration mode	TLV Fields	Description
location	Location TLV	Delivers location-based information to endpoint devices through switches, routers, or access devices using the Cisco Discovery Protocol. The Location TLV can send the following types of information: • Custom location—Provides the location and attributes of the endpoint device. • Civic location information—Provides the civic address information and postal information; for example, street address, road name, and postal community 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). The PSAP uses this information to call back. • Geo spatial location information—Provides the longitude, latitude, and altitude information of the endpoint device. You must configure the location TLV on the device before Cisco Discovery Protocol can deliver location-based information to the endpoint devices.
location-server	Location-server TLV	Provides a mechanism for location servers to transfer the required information to the neighbor devices.
mgmt-address	Management Address TLV	Contains a list of network layer addresses encoded similarly to the Address TLV. This TLV contains a list of all the addresses at which the device accepts SNMP messages.
native-vlan	Native VLAN TLV	Indicates the Inter-Switch Link (ISL) number of the native interface VLAN on which the Cisco Discovery Protocol packet is sent, as well as whether the VLAN is enabled on the link and whether the link is a trunk or a host/edge port.
platform	Platform TLV	Describes the hardware platform of the device. Encoded as an ASCII character string. The TLV length determines the length of the string.

Related command in TLV list configuration mode	TLV Fields	Description
port-id	Port-ID TLV	Identifies the port on which the Cisco Discovery Protocol packet is sent. This is encoded as an ASCII character string. The value of this TLV is the same as the MIB object ifName for the ifTable entry on which the Cisco Discovery Protocol packet is sent.
power -available	Power Available TLV	Specifies the information transmitted by all switch interfaces. This information permits a device that needs power to negotiate and select an appropriate power setting. The Power Available TLV includes four fields: • Request-ID field • Available-Power field • Power-Management-ID field • Management-Power-Level field
powernet	Energywise TLV	Discovers neighbor devices, communicates and negotiates power-related parameters with Cisco end devices such as an IP phone and access point.
trust	Extended Trust TLV	Specifies that the trust from the larger switch port is extended to other (external) ports of the simple switching device without explicitly configuring the trust on the simple switching device. Extending trust allows a network administrator to trust a host/server to mark the packets and the port on which this host/server is connected. Packets received on a trusted port are not marked again. The TLV value is one byte in length with its least significant bit indicating the trust mode. A 1 indicates extended trust and a 0 indicates the absence of extended trust. All other bits of the TLV value should be set to 0 on transmission and ignored on receipt. A Cisco Discovery Protocol packet without this TLV indicates the absence of extended trust.

Related command in TLV list configuration mode	TLV Fields	Description
version	Version TLV	Contains information about the Cisco software image version the device is running. This is in the form of a character string. The TLV length determines the length of the string. This information is displayed in the output of the **show version** command.
vtp-mgmt-domain	VTP Management Domain TLV	Specifies the name of the VLAN Trunking Protocol (VTP) management domain for a device running the VTP on the particular interface on which the Cisco Discovery Protocol packet is sent. The length of this TLV determines the length of the VTP management domain name. A length of zero indicates that a device is running VTP but has no management domain name assigned to it.
vvid	Appliance VLAN-ID TLV	Indicates the setting of the local configuration when a local 802.1Q interface has been configured to send and receive VoIP and related packets on a particular VLAN. Devices receiving this TLV may adjust their configuration to match this setting.

Note The Address TLV and Device ID TLV are mandatory TLVs and they cannot be blocked. Hence, they are not available in the Cisco software image for user configuration.

How to Configure Secure Cisco Discovery Protocol

Configuring a TLV List and Adding TLVs to the List

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cdp tlv-list** *tlv-list-name*
4. **ip-prefix**
5. **hello-protocol**
6. **end**
7. **show cdp tlv-list** *tlv-list-name*

DETAILED STEPS

	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 tlv-list** *tlv-list-name* **Example:** `Device(config)# cdp tlv-list group1`	Configures the type, length, value (TLV) list that allows users to select TLVs and enters TLV list configuration mode.
Step 4	**ip-prefix** **Example:** `Device(config-tlv-list)# ip-prefix`	Adds the IP prefix TLV to the TLV list.
Step 5	**hello-protocol** **Example:** `Device(config-tlv-list)# hello-protocol`	Adds the Protocol-Hello TLV to the TLV list. **Note** In TLV list configuration mode, enter the CLI help (**?**) command to view a list of TLVs that are not added to the TLV list.

	Command or Action	Purpose

Step 6	**end**
	Example:
	`Device(config-tlv-list)# end`
		Exits TLV list configuration mode and returns to privileged EXEC mode.

Step 7	**show cdp tlv-list** *tlv-list-name* **Example:** `Device# show cdp tlv-list group1`	Displays information about the TLVs in a TLV list.

Applying TLV List Configurations at the Interface Level

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **cdp filter-tlv-list** *tlv-list-name*
5. **end**
6. **show cdp tlv-list** *tlv-list-name*

DETAILED STEPS

	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* **Example:** `Device# interface ethernet 0/0`	Specifies an interface type and enters interface configuration mode.

	Command or Action	Purpose
Step 4	**cdp filter-tlv-list** *tlv-list-name* **Example:** `Device(config-if)# cdp filter-tlv-list group1`	Applies a TLV list on an interface.

Step 5	**end**
	Example:
	`Device(config-if)# end`
		Exits interface configuration mode and returns to privileged EXEC mode.

Step 6	**show cdp tlv-list** *tlv-list-name* **Example:** `Device# show cdp tlv-list group1`	Displays information about the TLVs in a TLV list.

Applying TLV List Configurations at the Global Level

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cdp filter-tlv-list** *tlv-list-name*
4. **end**
5. **show cdp tlv-list** *tlv-list-name*

DETAILED STEPS

	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.

	Command or Action	Purpose
Step 3	**cdp filter-tlv-list** *tlv-list-name* **Example:** `Device(config)# cdp filter-tlv-list group1`	Applies a TLV list globally.

Step 4	**end**
	Example:
	`Device(config)# end`
		Exits global configuration mode and returns to the privileged EXEC mode.

Step 5	**show cdp tlv-list** *tlv-list-name* **Example:** `Device# show cdp tlv-list group1`	Displays information about the TLVs in a TLV list.

Configuration Examples for Secure Cisco Discovery Protocol

Example: Configuring a TLV List and Adding TLVs to the List

The following example shows how to create a type, length, value (TLV) list, group1 and add TLVs to the list:

```
Device> enable
Device# configure terminal
Device(config)# cdp tlv-list group1
Device(config-tlv-list)# ip-prefix
Device(config-tlv-list)# hello-protocol
Device(config-tlv-list)# trust
Device(config-tlv-list)# capability
```

The following example shows how to create a TLV list, group2 and add TLVs to the list:

```
Device(config)# cdp tlv-list group2
Device(config-tlv-list)# address
Device(config-tlv-list)# duplex
Device(config-tlv-list)# capability
Device(config-tlv-list)# end
```

The following example shows how to view the TLV lists and the TLVs that are added to the lists:

```
Device# show cdp tlv-list group1

Tlv-list : group1
Capability  Hello-protocol  Ip-prefix  Trust

Device# show cdp tlv-list group2

Tlv-list : group2
Address  Capability  Duplex
```

```
Device# show cdp tlv-list *

Tlv-list : group1
Capability  Hello-protocol  Ip-prefix  Trust

Tlv-list : group2
Address  Capability  Duplex
```

Note

- The **show cdp tlv-list *** command displays all configured Cisco Discovery Protocol TLV lists.

Example: Applying TLV List Configurations at Interface Level

The **show cdp interface** command displays Cisco Discovery Protocol TLV lists on all interfaces.

The following example shows how to apply Cisco Discovery Protocol type, length, value (TLV) lists on an interface:

```
Device> enable
Device# configure terminal
Device(config)# interface ethernet 0/0
Device(config-if)# cdp filter-tlv-list group1
03:22:15: %CDP-6-TLV_LIST_INTERFACE: Tlv-list group1 applied on
interface Ethernet0/0
Device(config-if)# exit
Device(config)# interface ethernet 0/1
Device(config-if)# cdp filter-tlv-list group2
03:22:45: %CDP-6-TLV_LIST_INTERFACE: Tlv-list group2 applied on
interface Ethernet0/1
Device(config-if)# end
Device# show cdp tlv-list group1

Tlv-list : group1
Capability  Hello-protocol  Ip-prefix  Trust
Applied on:
Et0/0

Device# show cdp interface ethernet0/0

Ethernet0/0 is up, line protocol is up
  Encapsulation ARPA
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
  Tlv-list applied : group1

Device# show cdp interface ethernet0/1

Ethernet0/1 is up, line protocol is up
  Encapsulation ARPA
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
  Tlv-list applied : group2

Device# show cdp interface

Ethernet0/0 is up, line protocol is up
  Encapsulation ARPA
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
  Tlv-list applied : group1
Ethernet0/1 is up, line protocol is up
  Encapsulation ARPA
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
  Tlv-list applied : group2
```

```
.
.
.
```

Example: Applying TLV List Configurations Globally

The following example shows how to globally apply a Cisco Discovery Protocol type, length, value (TLV) list:

```
Device> enable
Device# configure terminal
Device(config)# cdp filter-tlv-list group1
03:28:44: %CDP-6-TLV_LIST_GLOBALLY: Tlv-list group1 applied globally on all
interfaces.
Device(config)# end
Device# show cdp interface

Ethernet0/0 is up, line protocol is up
  Encapsulation ARPA
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
  Tlv-list applied : group1
Ethernet0/1 is up, line protocol is up
  Encapsulation ARPA
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
  Tlv-list applied : group2
.
.
.
```

Note The **show cdp interface** command displays Cisco Discovery Protocol TLV lists on all interfaces.

Additional References for Secure Cisco Discovery Protocol

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
Cisco Discovery Protocol commands	Cisco IOS Cisco Discovery Protocol Command Reference
SNMP configuration tasks	*Configuring SNMP Support*
On-Demand Routing configuration tasks	*Configuring On-Demand Routing*

Standards and RFCs

Standard/RFC	Title
IEEE 802.1Q	*802.1Q—Virtual LANs*

MIBs

MIB	MIBs Link
CISCO-CDP MIB	To locate and download MIBs for selected platforms, Cisco software 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 and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Secure Cisco Discovery Protocol

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 Secure Cisco Discovery Protocol

Feature Name	Releases	Feature Information
Secure Cisco Discovery Protocol	15.4(1)T	The Secure Cisco Discovery Protocol feature allows you to select what information is sent in Cisco Discovery Protocol packets and block sensitive information. The following commands were introduced or modified: **cdp filter-tlv-list**, **cdp tlv-list**, **show cdp interface**, **show cdp tlv-list**.