



## LLDP-MED and Cisco Discovery Protocol

### DEVICE DISCOVERY PROTOCOLS

Device discovery protocols enable directly connected devices to discover information about each other. They advertise information about the device over every interface, allowing any device in the network to “know” everything it is connected to. Examples of applications that use the information conveyed by discovery protocols include:

- Network topology—A network management system (NMS) can accurately represent a map of the network topology.
- Inventory—A management system can query a switch to learn about all the devices connected to that switch.
- Emergency services—Location of a phone can be determined by the switch port to which it is connected.
- VLAN configuration—The switch can tell the phone which VLAN to use for voice.
- Power negotiation—The phone and the switch can negotiate the power that the phone can consume.

Cisco Systems® introduced the Cisco® Discovery Protocol in 1994 to provide a mechanism for the management system to automatically learn about devices connected to the network. Cisco Discovery Protocol runs on Cisco devices (routers, switches, phones, etc.) and is also licensed to run on some network devices from other vendors. Using Cisco Discovery Protocol, network devices periodically advertise their own information to a multicast address on the network, making it available to any device or application that wishes to listen and collect it. Because Cisco Discovery Protocol runs over Ethernet, ATM, and Frame Relay links, it is independent of network protocol (for example, TCP/IP, Internetwork Packet Exchange [IPX], AppleTalk, etc.). With this capability in the network, Cisco customers can introduce a new network management application that can discover and display an accurate topology of all the Cisco devices active on the network. Because automatic device discovery is so helpful for network administration, many vendors in the data networking industry have subsequently implemented their own discovery protocols to manage their devices.

Some of the well-known vendor-proprietary network discovery protocols are listed in Table 1.

**Table 1.** Network Discovery Protocols

Vendor	Acronym	Name
Cisco Systems	–	Cisco Discovery Protocol
Enterasys	CDP	Cabletron Discovery Protocol
Extreme	EDP	Extreme Discovery Protocol
Foundry	FDP	Foundry Discovery Protocol
Nortel	NDP	Nortel Discovery Protocol

Over time, enhancements have been made to discovery protocols to provide greater capabilities. Applications (such as voice) have become dependent on these capabilities to operate properly, leading to interoperability problems between vendors. Therefore, to allow interworking between vendor equipment, it has become necessary to have a single, standardized discovery protocol. Cisco has been working with other leaders in the Internet and IEEE community to develop a new, standardized discovery protocol, 802.1AB (Station and Media Access Control Connectivity Discovery, or Link Layer Discovery Protocol [LLDP]). LLDP, which defines basic discovery capabilities, was enhanced to specifically address the voice application; this extension to LLDP is called LLDP-MED or LLDP for Media Endpoint Devices. It should be noted that either LLDP or LLDP-MED—but not both—can be used at any given time on an interface between two

devices. That is, LLDP-MED defines how a switch port transitions from LLDP to LLDP-MED if it detects an LLDP-MED-capable endpoint.

This paper compares LLDP-MED and the Cisco Discovery Protocol specifically as they relate to phones and switches. It also identifies some outstanding concerns that affect both development and deployment of multiple discovery protocols.

Cisco plans to initially support LLDP and LLDP-MED on both IP phones and LAN switches to provide multi-vendor interoperability. Because Cisco Discovery Protocol is widely deployed and provides some additional capabilities beyond LLDP-MED, Cisco will continue to fully support Cisco Discovery Protocol along with LLDP and LLDP-MED.

## HISTORY

### Cisco Discovery Protocol

Invented at Cisco by Keith McCloghrie and Dino Farinacci, Cisco Discovery Protocol was initially introduced on Cisco products in 1994. This protocol now operates on tens of millions of Cisco devices throughout the world. It initially supported a limited set of attributes that were used mainly for device discovery. These attributes are based on type, length, and value descriptions, referred to as TLVs. The TLVs initially supported include the following:

- Device ID
- Network layer address
- Capabilities (such as router, switch, bridge, etc.)
- Software version
- Platform (for example, the Cisco Catalyst<sup>®</sup> 6500)
- Interface
- Port ID

In 1996 Cisco expanded the Cisco Discovery Protocol to include support for On-Demand Routing (ODR), which simplifies configuration for stub routers. This attribute follows:

- Network prefix

In 1997 Cisco expanded the Cisco Discovery Protocol from Version 1 to Version 2 and included the following TLVs:

- Protocol–Hello—Allows other protocols to piggyback their Hello packets onto Cisco Discovery Protocol
- VLAN Trunking Protocol (VTP) management domain—Names the management domain
- Native VLAN—Indicates the number of the native VLAN
- Full or half duplex—Indicates if the interface is operating in half or full duplex

In 1999 Cisco added attributes to support voice over IP (VoIP). These TLVs included the following:

- Appliance VLAN—Indicates the voice VLAN
- Trigger—Offers ability to cause the remote end to immediately send a Cisco Discovery Protocol packet
- Power—Adds capability to negotiate power
- Extended trust and class of service (CoS)—Offers ability to specify whether the PC port of the phone is trusted and if not, what to mark the Layer 2 packet CoS bits coming in from the PC port

In 2000 Cisco added TLVs as follows:

- Sysname—Indicates fully qualified domain name (FQDN) of the device per RFC 1907
- sysObjectID—Gives object identifier (OID) per RFC 1907
- Management address—Indicates IP addresses for which the device accepts Simple Network Management Protocol (SNMP) messages
- Physical location—Gives a string representing the physical location of the devices

In 2001 Cisco added support for the following TLV:

- External port ID—Identifies the physical fiber

Finally, in 2003 Cisco added the following attributes to the protocol:

- Power requested—Specifies how much power is being requested
- Power available—Specifies how much power is available
- Port unidirectional mode—Specifies that traffic on this port is one way only

## LLDP-MED

LLDP got its start in an IETF Working Group (PTOPOMIB), which focused on a common framework or model to describe physical topology. This group published an informational MIB, RFC 2922, in September 2000. Cisco then worked with the IEEE to create 802.1AB, which was published in May 2005. This protocol provides standards-based discovery for vendor interoperability.

It was recognized that additional capabilities were needed specific to VoIP, and this work was assumed by the Telecommunications Industry Association (TIA) TR-41.4 subcommittee. This committee developed LLDP-MED, which defines extensions to LLDP. LLDP-MED is specified to operate only between endpoint devices such as IP phones and network connectivity devices such as switches.

## COMPARISON OF LLDP-MED AND CISCO DISCOVERY PROTOCOL

LLDP-MED and Cisco Discovery Protocol are closely related protocols. They are similar in many ways, including operation and the information they carry.

The following sections discuss the capabilities of these protocols and how they differ in their implementation. A detailed comparison of these protocols is provided in the appendix.

Note that the following comparison is limited to the scope of operation between switches and endpoints. The Cisco Discovery Protocol has many capabilities that are not compared to LLDP-MED because these capabilities are outside the scope of the switch-to-phone interface specified by LLDP-MED (refer to Table 4 in the appendix for further details).

### Capabilities Discovery

Capabilities discovery allows endpoints to determine the type of capabilities the connected device supports. It can be used to indicate whether the connected device is a phone, a switch, a repeater, etc.

These basic capabilities discoveries are supported by both Cisco Discovery Protocol and LLDP-MED. In addition to basic discovery capabilities, LLDP-MED includes an additional function to specify what capabilities the device currently has enabled. For example, Cisco Discovery Protocol states that a device is a phone, whereas LLDP-MED can state that the device is a phone with a PC port that is enabled or disabled.

## LAN Speed and Duplex Discovery

This capability is important because it allows for the discovery of any speed or duplex mismatches that may occur between the devices. For example, the switch could send a trap if it detects a mismatch between the endpoint and the switch.

LLDP-MED supports both LAN speed and duplex discovery. Cisco Discovery Protocol supports duplex discovery only, but this limited support is not seen as a problem because if there is a speed mismatch, LLDP-MED and Cisco Discovery Protocol cannot be exchanged and thus cannot be used to detect the mismatch.

## Network Policy Discovery

This capability is one of the most important because it provides a mechanism for a switch to notify a phone the VLAN number that it should use. The phone can plug into any switch, obtain its VLAN number, and then start communications with the call control.

Network policy discovery solves the major problem today with third-party phones working with Cisco switches as well as Cisco phones working with third-party switches. For both of these cases, an inter-working problem makes deployment problematic.

### Third-Party Phones with Cisco Switches

Some third-party phones receive their VLAN information through Dynamic Host Configuration Protocol (DHCP), meaning that these phones must first boot up, get an IP address on the native VLAN, get voice VLAN information from the DHCP server, and then boot up again using the voice VLAN. In other cases the phones must be individually configured to assign their VLAN address.

### Cisco Phones with Third-Party Switches

In this case, Cisco phones must be individually provisioned (through the phone interface) with their voice VLAN information.

Both LLDP-MED and Cisco Discovery Protocol support this capability. LLDP-MED provides finer control of the network policy by allowing separate control for signaling and bearer applications. However, from a practical point of view, the critical capability is the VLAN configuration, and it is supported by both Cisco Discovery Protocol and LLDP-MED.

## Location Identification Discovery

This capability is important because it normally provides location information from the switch to the phone. (If the phone is configured with location information or can determine its location, then it may send this information to the switch. However, the real value is getting this information from the switch to the phone for phones that cannot determine their own location.) Location identification discovery allows the phone to be aware of its location—information that can be used for location-based applications on the phone. More importantly, this capability can be used to provide location information when making emergency calls.

Both Cisco Discovery Protocol and LLDP-MED support the transportation of location information. However, LLDP-MED has more supported data formats than Cisco Discovery Protocol.

## Power Discovery

Power discovery allows switches and phones to convey power information—an especially important capability when Power over Ethernet (PoE) is used because with PoE the switch provides power to the phones.

LLDP-MED provides information related to how the device is powered (from the line, from a backup source, from external power source, etc.), power priority (how important is it that this device has power?), and how much power the device needs.

Cisco Discovery Protocol includes separate TLVs for power requested and power available, allowing the switch and the phone to negotiate the power used. Some Cisco IP phones can operate at multiple power settings, lowering their consumption when less power is available.

This distinction between Cisco Discovery Protocol and LLDP-MED is important because Cisco Discovery Protocol provides two-way power negotiation between the IP phone and switch, a capability not supported in LLDP-MED. It should be noted that power negotiation capabilities are being addressed by the IEEE 802.3at, but not as part of LLDP-MED.

### **Inventory Discovery**

Inventory discovery provides a means to effectively manage company assets related to endpoints such as phones. For example, LLDP-MED and Cisco Discovery Protocol allow an IP phone to inform the switch about attributes of the IP phone such as model number, serial number, software revision, etc. This capability is important because many IP phones do not support an SNMP interface such that a management system can directly access this information from the phone. Additionally, providing this information on the switch for all IP phones that are connected to the switch simplifies the management application because it can obtain the information about all the IP phones by centrally querying the switches involved.

Both Cisco Discovery Protocol and LLDP-MED support inventory-discovery capabilities.

### **Trust Extension**

Cisco Discovery Protocol provides an additional capability not found in LLDP-MED that allows the switch to extend trust to the phone. In this case, the phone is now trusted to mark the packets received on the PC port accordingly. This feature can be used to off-load the switch because now it does not need to police the information being received from the phone.

## **INDUSTRY CHALLENGES IN IMPLEMENTING LLDP-MED**

The most important benefit with LLDP-MED is that it is an open standard. This protocol enables Cisco products to work better with third-party products. However, deploying LLDP-MED does present challenges.

Although LLDP-MED is an open standard supported by Cisco, use of Cisco Discovery Protocol must be supported along with LLDP and LLDP-MED (other vendors are expected to have similar concerns with their proprietary protocols). LLDP-MED will not be available at the same time on all equipment, and may never be implemented on older devices. Network administrators will not upgrade all their equipment simultaneously. Therefore, Cisco must support the use of both protocols simultaneously in the network.

A given LAN switch might have devices with any of the following sets of capabilities attached to it:

- Devices that support only LLDP-MED (example: a third-party phone)
- Devices that support only Cisco Discovery Protocol (example: an older Cisco switch or older Cisco phone)
- Devices that support only LLDP (example: a third-party router)
- Devices that support both LLDP and Cisco Discovery Protocol (example: a Cisco router)
- Devices that support both LLDP-MED and Cisco Discovery Protocol (example: A Cisco phone)
- Devices that support LLDP, LLDP-MED, and Cisco Discovery Protocol (example: a Cisco switch)

Figure 1 depicts scenarios of how these protocols can be used and where (if any) challenges lie, as follows:

1. An endpoint connected to a Cisco phone—A PC connected to a Cisco phone can support Cisco Discovery Protocol; that is, some applications that can run on a PC (example Cisco VT Advantage) do support this protocol. The phone uses the protocol to support these applications.

One of the challenges in this area is that LLDP-MED does not adequately specify how the PC port on the phone fits into the overall LLDP-MED architecture. A problem now exists when LLDP is used with a 2-port phone, because this protocol has not yet been standardized for this scenario. IEEE Standard 802.1ah-2005, Provider Bridges, states that LLDP is passed transparently through a provider bridge, invalidating the assumption made by LLDP and LLDP-MED implementations insofar as a provider bridge allows

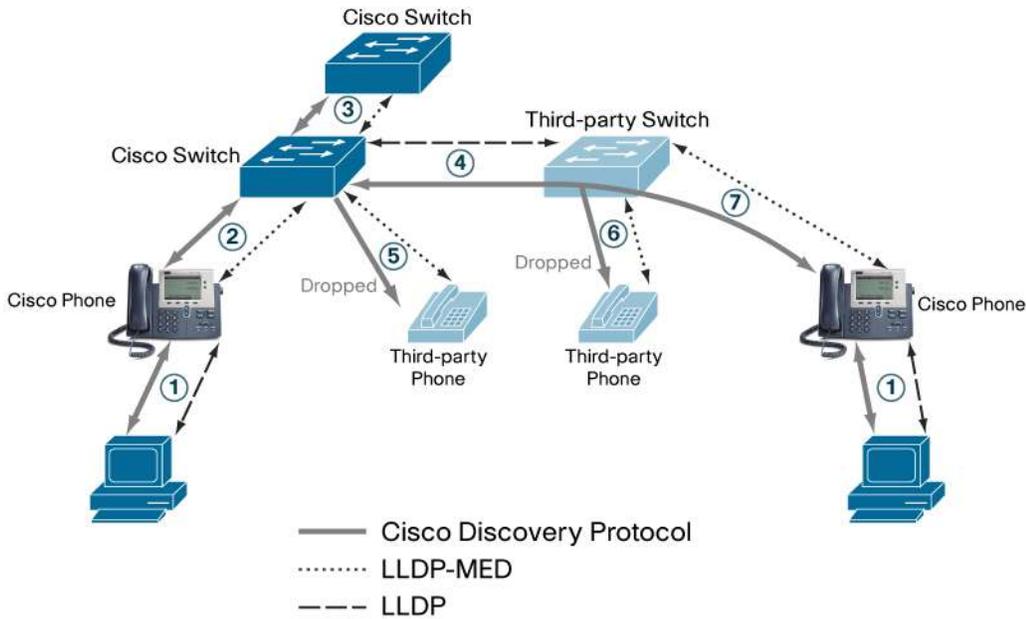
devices that are not physically adjacent to trade LLDP packets as neighbors. The 802.1ah standard suggests that LLDP could be run using two different destination MAC addresses, one that passes through provider bridges (the current address) and one that does not. In addition, the new IEEE 802 project P802.1aj, Two Port MAC Relay, can pass LLDP packets transparently.

Thus, it is uncertain how LLDP will be handled in a telephone; specifically, it is uncertain how many destination MAC addresses a phone or a PC needs to know about. Until this situation is resolved in IEEE 802.1, Cisco takes a conservative position, and does not pass LLDP through the phone.

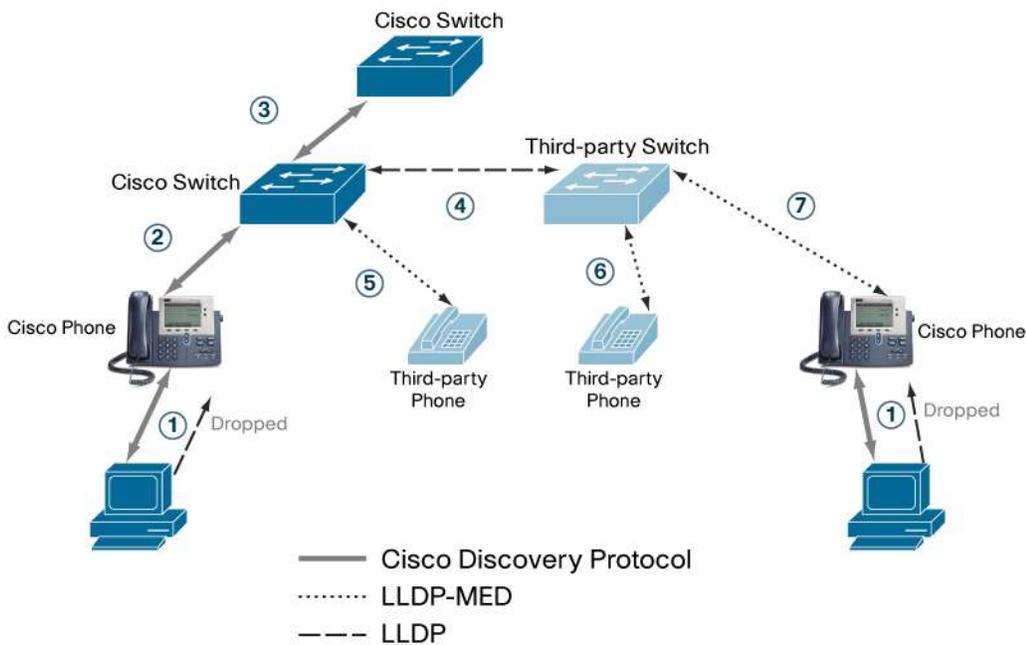
2. A Cisco phone connected to a Cisco switch—Both the Cisco switch and the Cisco phone must support these protocols. The challenge is to determine which protocol takes priority and whether prioritization should be done on a TLV-by-TLV basis.
3. A Cisco switch connected to another Cisco switch—Both LLDP and Cisco Discovery Protocol must be supported in this case. Again the challenge is to determine how these protocols interact.
4. A Cisco switch connected to a third-party switch—In this case the Cisco switch generates the Cisco Discovery Protocol messages and LLDP messages. On most third-party switches the Cisco Discovery Protocol messages are ignored and flooded out the other interfaces, meaning devices connected to the third-party switch receive Cisco Discovery Protocol messages from the Cisco switch. Cisco phones on that switch receive these Cisco Discovery Protocol messages and send Cisco Discovery Protocol messages as if they were directly connected to the Cisco switch. Therefore, when Cisco switches are connected to third-party switches (and the third-party switches support LLDP-MED), Cisco Discovery Protocol should be turned off on ports connecting to the third-party switches.
5. A third-party phone connected to a Cisco switch—The switch generates both Cisco Discovery Protocol and LLDP-MED messages. The phone drops the Cisco Discovery Protocol messages.
6. A third-party phone connected to a third-party switch—In this case of course only LLDP-MED is expected.
7. A Cisco phone connected to a third-party switch —In this case the phone generates both LLDP-MED and Cisco Discovery Protocol messages. The switch uses LLDP-MED messages but usually ignores the Cisco Discovery Protocol messages and floods them out other interfaces. As stated in example 4, if a Cisco switch is connected to the third-party switch, then Cisco Discovery Protocol should be disabled on the Cisco switch trunk interface.

Although Figure 1 does depict Cisco Discovery Protocol and LLDP or LLDP-MED running simultaneously on Cisco devices, control must be provided so that any of these protocols can be disabled. Figure 2 depicts a scenario where protocols are configured such that Cisco Discovery Protocol is used between Cisco equipment and LLDP or LLDP-MED is used between Cisco and third-party equipment.

**Figure 1.** Cisco Discovery Protocol and LLDP-MED Scenarios



**Figure 2.** Cisco Discovery Protocol and LLDP-MED Protocol Tuning



## CONCLUSION

Cisco currently supports a pre-standards-based discovery protocol that provides similar capabilities to the currently released standards-based LLDP-MED. Cisco Discovery Protocol will continue to be fully supported and may be enhanced in the future to address future



capabilities that are not currently supported in LLDP-MED. Additionally, Cisco plans to fully support LLDP-MED on its phones and switches. While some challenges remain, Cisco is actively involved in the standards process to address these challenges and is working internally to ensure that both LLDP-MED and Cisco Discovery Protocol can coexist.

With support for both protocols operating simultaneously, Cisco customers can evolve their networks to an open standard, which enables better interoperability with third-party products while maintaining full compatibility with older devices that only support Cisco Discovery Protocol. It is planned that both protocols are enabled by default on Cisco products to provide the simplest approach from an operational point of view. However, customers can fully control which protocol is running on which devices.

## APPENDIX—PROTOCOL COMPARISON

Table 2 describes some of the details of the two protocols from an operational and capabilities point of view.

**Table 2.** Cisco Discovery Protocol Versus LLDP-MED Protocol Operation Comparison

Protocol Operation	LLDP	Cisco Discovery Protocol
Use of multicast address	Yes 01-80-C2-00-00-0E	Yes 0100.0ccc.cccc c000.0800.0000 for 802.5
Ethertype	LLDP has a dedicated ethertype: 88-CC.	Cisco Discovery Protocol uses IEEE 802.2 and 802.3 encapsulation only.
Subnetwork Access Protocol (SNAP) value	AA-AA-03-00-00-00-88-CC	AA-AA-03-00-00-0C-20-00
Token Ring support	Yes	Yes
Fiber Distributed Data Interface (FDDI) support	Yes	Yes
Ethernet support	Yes	Yes
ATM support	No (not formalized)	Yes
Frame Relay support	No (not formalized)	Yes
Checksum support	No	Yes
Fast Start support	Yes For network connectivity devices such as switches, LLDP fast start occurs only after an LLDP-MED frame has been received and the receiving device does not have any valid data from that device yet. For endpoints such as phones, fast start also occurs at link initialization. For both cases, the default is 1 per second for 3 seconds. LLDP allows configuration of these parameters.	Yes Cisco Discovery Protocol Fast Start occurs when the link first comes up, in which case Cisco Discovery Protocol sends protocol frames at a rate of 1 per second for 3 seconds. These parameters are fixed in Cisco Discovery Protocol.
Protocol uses	LLDP-MED is used only between network devices (such as switches) and endpoint devices (such as phones). For network-to-network connections, LLDP is used.	Network-endpoint Network-network There is no difference in protocol operation, although of course different device types may transmit different TLVs.
MIB support	LLDP-EXT-MED-MIB This MIB includes the following: <ul style="list-style-type: none"> <li>• Topology change notification</li> <li>• LLDP-MED configuration</li> <li>• Local device information</li> <li>• Remote device information</li> </ul>	CISCO-CDP-MIB
Topology change notification—Sends a notification if a device is added or removed	Yes	No
Standard 802.1x interaction	The switch does not accept or send LLDP-MED packets until after authentication occurs.	The switch does not accept or send Cisco Discovery Protocol packets until after authentication occurs. Note <sup>1</sup> that the switch can be configured to bypass authentication if Cisco Discovery Protocol is received.
Advertising frequency (time between protocol frames)	Default 30 seconds (configurable)	Default 60 seconds (configurable)

<sup>1</sup> Refer to [http://www.cisco.com/en/US/products/hw/switches/ps5528/products\\_configuration\\_guide\\_chapter09186a00801e85c4.html](http://www.cisco.com/en/US/products/hw/switches/ps5528/products_configuration_guide_chapter09186a00801e85c4.html) and [http://www.cisco.com/en/US/products/sw/voicesw/ps556/products\\_security\\_notice09186a008048e0d6.html](http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_security_notice09186a008048e0d6.html) for further information.

Transmit frame on local MIB change—If one of the settings in the local MIB changes, then LLDP-MED immediately transmits a message. This is useful because it reduces the time needed for synchronization. For example, if a VLAN is administratively changed, LLDP-MED transmits this change immediately to phones, whereas Cisco Discovery Protocol may take up to a minute.	Yes	No
Cisco device action on receiving an LLDP-MED or Cisco Discovery Protocol frame	Accept, depending on products, the timeframe, and configuration; LLDP-MED is not planned for introduction on all existing endpoint products, and the rollout schedule may vary from product to product	Accept (all Cisco equipment supports Cisco Discovery Protocol); note, of course, that if Cisco Discovery Protocol is disabled then these are dropped
Third-party device action on receiving an LLDP-MED or Cisco Discovery Protocol	Accept, depending on their support for LLDP-MED and configuration	Most switches ignore the Cisco Discovery Protocol messages but forward them.
Discovers Cisco devices	Yes	Yes
Discovers third-party devices	Yes	No
Support for TLV selection in transmission—Provides the ability to specify which TLVs are to be included in the outgoing frames	TLV selection is supported for optional TLVs.	TLVs are grouped into three groups, minimum, standard, and maximum. Global settings and port settings can define which group to use. Configuration of which TLVs are in the standard and maximum groups is supported.

### TLV-Level Comparison

Type, length, and value descriptions (TLVs) describe the individual pieces of information that the protocols transfer. Both LLDP-MED and Cisco Discovery Protocol use TLVs to describe the individual pieces of information.

Table 3 describes these TLVs and compares the functions with regard to the two protocols.

**Table 3.** Cisco Discovery Protocol Versus LLDP-MED TLV Comparison

TLV Function	LLDP-MED TLV	Cisco Discovery Protocol TLV
Device identifier—A TLV that uniquely identifies the device sending the discovery protocol messages	<i>LLDP Chassis ID TLV</i> The device identifier is constrained to MAC address (for a network connectivity device) or network address (for an endpoint device). Note that LLDP also allows for MAC address, but LLDP-MED constrains this use, as discussed previously. Phones use MAC address for this constraint	<i>Device ID TLV</i> This TLV allows for MAC address or serial number. <i>Address TLV</i> This TLV utilizes the network layer addresses associated with the interface to which Cisco Discovery Protocol packets are sent.
Port identifier—Used to identify the port that is sending the discovery protocol message	<i>LLDP Port ID TLV</i> The port identifier is the MAC address of the port issuing the LLDP-MED message. Note that LLDP also allows ifName, but LLDP-MED constrains this use to the MAC address. Phones use the ifName.	<i>Port-ID TLV</i> The port identifier is the name of the interface; it is the same as ifName from MIB RFC 2863.
Time to live—Specifies how long the receiving device should maintain the received information in its MIB	<i>LLDP Time-To-Live TLV</i> 0 <= TTL < 65535 seconds	Time to live is not a specific TLV but is included as part of the header information. 0 <= TTL <= 255 seconds; default is 180 seconds
System capabilities—Determines the capabilities of the device such as phone, switch, or router	<i>LLDP System Capabilities TLV</i> LLDP carries both a value to indicate which capabilities are supported by the device and which capabilities are actually enabled for the device. Note: An example is a phone that has a PC port that is disabled. In this case the system capabilities indicate both phone and bridge, whereas the enabled capabilities indicate phone only.	<i>Capabilities TLV</i> This TLV indicates only primary functions such as the phone and does not indicate that the phone also has PC port.
Physical layer information—Defines information related to the link speed and its half- or full-duplex setting	<i>IEEE802.3 MAC/PHY Configuration/Status TLV</i> This TLV contains the duplex and speed capabilities of the port as well as their current settings. It also indicates if they are autonegotiated or configured.	<i>Full/Half Duplex TLV</i> This TLV indicates the full- or half-duplex setting of the link only.

List of TLVs supported and device class capability—Indicates the TLVs that are supported by the sending device and the class of device	<i>LLDP-MED Capabilities TLV</i> This TLV identifies the LLDP-MED TLVs that the sending device supports and also if this is an endpoint or network connectivity device. If it is an endpoint device, it specifies the LLDP-MED class of the endpoint.	None
VLAN configuration information	<i>LLDP-MED Network Policy TLV</i> This TLV specifies the VLAN ID, the 802.1 priority, and the differentiated-services-code-point (DSCP) value. It also allows for tagged and untagged VLANs.  This TLV can send this policy for each application supported, allowing separate definitions for voice signaling, video, voice bearer, etc.	<i>Appliance VLAN-ID TLV</i> This TLV specifies the VLAN ID and also allows for tagged and untagged VLANs.  It does not allow for specification of 802.1 priority or DSCP values, and it does not differentiate between applications.
Power management support Note: There are some significant differences between these two protocols.	<i>Extended Power Via-MDI TLV</i> LLDP-MED provides information related to how the device is powered (from the line, from a backup source, from an external power source, etc.), power priority (how important is it that this device has power?), and also how much power the device needs.	<i>Power Consumption TLV</i> <i>Power Requested TLV</i> <i>Power Available TLV</i> Cisco Discovery Protocol supports power negotiation and allows the switch and the phone to agree on power. LLDP does not really allow for negotiation.
Inventory management support	<i>Inventory Management TLV</i> This TLV offers the following: <ul style="list-style-type: none"> <li>• Hardware revision</li> <li>• Firmware revision</li> <li>• Software revision</li> <li>• Serial number</li> <li>• Manufacturer name</li> <li>• Model name</li> <li>• Asset ID</li> </ul>	<i>sysName TLV</i> <i>sysObject TLV</i> <i>Platform TLV</i> <i>Version TLV</i>  Note that the Device ID TLV (first one in this table) may contain the serial number.
Extended trust support—Allows the switch to instruct the phone that it should or should not trust the device attached to its PC port; if not trusted, then the protocol can use the CoS to set the 802.1p user priority bits.	No	<i>Extended Trust TLV</i> <i>COS for Untrusted Ports TLV</i>
Capability to allow a device to request another device to send it an updated discovery protocol message.	LLDP-MED does not have a specific attribute for this capability. However, this capability can be indirectly accomplished by first sending a LLDP-MED message with a TTL of 0, followed by another message with a normal TTL.	<i>Trigger TLV</i> When this TLV is received, it causes the receiver to immediately send a Cisco Discovery Protocol message to the sender.
Native VLAN support—Indicates the native VLAN	No	<i>Native VLAN TLV</i>

Although the TLVs listed in Table 4 are Cisco Discovery Protocol-only TLVs, their use is outside the scope of a network connectivity device and endpoint device and thus are compared to LLDP TLVs. That is, these TLVs are generally used between switches or routers and not between switches and endpoints.

**Table 4.** LLDP Versus Cisco Discovery Protocol TLV Comparison

Function Description	LLDP TLV	Cisco Discovery Protocol TLV
IP network prefix support—Used to send the network prefix and used for ODR	No	<i>IP Network Prefix TLV</i>
Hello piggybacking—Can be used to piggy back hello messages from other protocols	No	<i>Protocol Hello TLV</i>
Maximum-transmission-unit (MTU) support— Specifies the size of the MTU	No	<i>MTU TLV</i>
External port support—Used to identify the card terminating the fiber in the case of wavelength-division multiplexing (WDM)	No	<i>External Port-ID TLV</i>
VTP management support	No	<i>VTP Management Domain TLV</i>
Port unidirectional mode—Used in fiber, where the connection may be unidirectional	No	<i>Port UniDirectional Mode TLV</i>
Management address	<i>Management Address TLV</i>	<i>Management-AddressTLV</i>
Allows for organizational unique TLVs	Yes	<i>No</i>

## DISCLAIMER

The specifications and information regarding the products in this document are subject to change without notice. All statements, information and recommendations in this document are believed to be accurate but are presented without warranty of any kind, express or implied. Users must take full responsibility for their application of any products.

The software license and limited warranty for the accompanying product are set forth in the information packet that shipped with the product and are incorporated herein by this reference. If you are unable to locate the software license or limited warranty, contact your Cisco representative for a copy.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

Notwithstanding any other warranty herein, all document files and software of these suppliers are provided "as is" with all faults. Cisco and the above-named suppliers disclaim all warranties, expressed or implied, including, without limitation, those of merchantability, fitness for a particular purpose and noninfringement or arising from a course of dealing, usage, or trade practice.

In no event shall Cisco or its suppliers be liable for any indirect, special, consequential, or incidental damages, including, without limitation, lost profits or loss or damage to data arising out of the use or inability to use this document, even if Cisco or its suppliers have been advised of the possibility of such damage.



**Corporate Headquarters**  
Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
www.cisco.com  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 526-4100

**European Headquarters**  
Cisco Systems International BV  
Haarlerbergpark  
Haarlerbergweg 13-19  
1101 CH Amsterdam  
The Netherlands  
www-europe.cisco.com  
Tel: 31 0 20 357 1000  
Fax: 31 0 20 357 1100

**Americas Headquarters**  
Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
www.cisco.com  
Tel: 408 526-7660  
Fax: 408 527-0883

**Asia Pacific Headquarters**  
Cisco Systems, Inc.  
168 Robinson Road  
#28-01 Capital Tower  
Singapore 068912  
www.cisco.com  
Tel: +65 6317 7777  
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the **Cisco.com Website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus • Czech Republic  
Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel • Italy  
Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal  
Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden  
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Copyright © 2006 Cisco Systems, Inc. All rights reserved. CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, Packet, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website 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. (0601R)

Printed in USA

C11-351374-00 06/06