Technical Guide

Link Layer Discovery Protocol (LLDP)

Feature Overview and Configuration Guide

Introduction

This guide describes the Link Layer Discovery Protocol (LLDP), LLDP for Media Endpoint Devices (LLDP-MED) and Voice VLAN, and general configuration information for these.

LLDP is a Layer 2 protocol defined by the IEEE Standard 802.1AB-2005. Your switch supports LLDP as specified in this standard, including Annex F and Annex G. LLDP allows network devices to share device-related information to or from directly connected devices on the network.

LLDP is designed to be managed with the Simple Network Management Protocol (SNMP), and SNMP-based Network Management Systems (NMS). LLDP can be configured, and the information it provides can be accessed, using either the command line interface or SNMP.

Products and software version that apply to this guide

This guide applies to AlliedWare Plus products that support LLDP, running version **5.4.4** or later.

To see whether your product supports LLDP, see the following documents:

- The product's Datasheet
- The AlliedWare Plus Datasheet
- The product's Command Reference

These documents are available from the above links on our website at alliedtelesis.com.

Feature support may change in later software versions. For the latest information, see the above documents.

Content

Link Layer Discovery Protocol

LLDP enables Ethernet network devices, such as switches and routers, to transmit and/or receive descriptive information, and to store such information learned about other devices. The data sent and received by LLDP is useful for many reasons:

- devices can discover neighbors—other devices directly connected to it.
- devices can use LLDP to advertise some parts of their Layer 2 configuration to their neighbors.
- some kinds of misconfiguration can be more easily detected and corrected.
- the LLDP-MED extension provides a level of plug & play configuration of peripheral devices.

LLDP is a link level (“one hop”) protocol; LLDP information can only be sent to and received from devices that are directly connected to each other, or connected via a hub or repeater. LLDP packets are not forwarded on to other devices on the network.

The information transmitted in LLDP advertisements flows in one direction only, from one device to its neighbors, and the communication ends there. Transmitted advertisements do not solicit responses, and received advertisements do not trigger acknowledgment.

LLDP operates over physical ports (Layer 2) only. For example, it can be configured on switch ports that belong to static or dynamic aggregated links (channel groups), but not on the aggregated links themselves; and on switch ports that belong to VLANs, but not on the VLANs themselves.

LLDP provides a way for the switch to:

- transmit information about itself to neighbors
- receive device information from neighbors
- store and manage information in an LLDP MIB

Each port can be configured to transmit local information, receive neighbor information, or both.

LLDP defines:

- a set of common advertisements, see"LLDP Advertisements" on page 5
- a protocol for transmitting and receiving advertisements, see "Transmission and Reception" on page 9
- a method for storing the information that is contained within received advertisements, see "Storing LLDP Information" on page 10

Interactions with other features

LLDP has the following interactions with other switch features:

- **Spanning tree**:

  Ports blocked by a spanning tree protocol can still transmit and receive LLDP advertisements.

- **802.1x**:

  Ports blocked by 802.1x port authorization cannot transmit or receive LLDP advertisements. If LLDP has stored information for a neighbor on the port before it was blocked, this information will eventually time out and be discarded.

- **VLAN tagging:**

  LLDP packets are untagged; they do not contain 802.1Q header information with VLAN identifier and priority tagging.

- **Virtual Chassis Stacking (VCStack) resiliency link**:

  When a port is configured as a VCStack resiliency link port, LLDP does not operate on the port; LLDP neither transmits nor receives advertisements, and any LLDP configuration and data stored for the port, including counters, is discarded.

- **Mirror ports**:

  LLDP does not operate on mirror analyzer ports.

LLDP-MED

LLDP for Media Endpoint Devices (LLDP-MED), is an extension of LLDP used between LAN network connectivity devices, such as a switch, and the media endpoint devices connected to it, such as IP phones. LLDP-MED is specified in ANSI/TIA-1057-2006. Of the application types specified in ANSI/TIA-1057-2006, the switch supports Application Type 1: Voice.

LLDP-MED uses the LLDP advertisement, transmission, and storage mechanisms, but transmits, receives, and stores data specifically related to managing the voice endpoint devices. This includes information about network policy, location, hardware configuration, and, for Power over Ethernet-capable devices, power management.

Voice VLAN

Many IP phones (or other IP voice devices) have two interfaces: one to connect to the network and another that allows a computer or similar device to connect to the network via the IP phone. It is often desirable to treat the voice and data traffic separately so that appropriate Quality of Service (QoS) policies can be applied to each. The Voice VLAN feature uses LLDP-MED to convey to the IP phone a set of configuration information (such as VLAN ID and User Priority tagging, and DiffServ Code Point (DSCP))— that the phone can apply to voice traffic.

In response, the IP phone sends voice traffic according to this configuration. The data traffic coming through the IP phone from the PC is sent with the default configuration, typically untagged with normal priority.

LLDP Advertisements

LLDP transmits advertisements as packets called LLDP Data Units (LLDPDUs). An LLDPDU consists of a set of Type-Length-Value elements (TLV), each of which contains a particular type of information about the device or port transmitting it.

Type-Length-Value (TLV)

A single LLDPDU contains multiple TLVs. TLVs are short information elements that communicate data, such as variable length strings, in a standardized format. Each TLV advertises a single type of information, such as its device ID, type, or management addresses. The following table describes fields in a TLV.

Table 1: Fields in a Type Length Value element

FIELD	DESCRIPTION
Type	Identifies the kind of information. It consists of a 7-bit Type code.
Length	Identifies the length of the information. It consists of a 9-bit value that specifies the number of bytes of data in the Value field.
Value	Contains the actual value of the advertised information. This is a variable length data field.

LLDP sends mandatory TLVs in each advertisement; it can also be configured to send one or more optional TLVs, from the following groups:

- Mandatory Base TLVs, included in all LLDP advertisements. See IEEE 802.1AB-2005.
- Optional Base TLVs, which may be included in any LLDP advertisements. See IEEE 802.1AB-2005.
- IEEE 802.1 Organizationally Specific TLVs (802.1 TLVs). See IEEE 802.1AB-2005 Annex F.
- IEEE 802.3 Organizationally Specific TLVs (802.3 TLVs). See IEEE 802.1AB-2005 Annex G.
- LLDP-MED Organizationally Specific TLVs (LLDP-MED TLVs), included in LLDP-MED advertisements. See ANSI/TIA-1057- 2006.

Mandatory and optional TLVs for LLDP and LLDP-MED advertisements are shown in the table following:

Table 2: TLVs in LLDP advertisements

TLV	DESCRIPTION
Mandatory Base TLVs—IEEE 802.1AB-2005	
Chassis ID	Identifies the device's chassis. On this switch, this is the MAC address of the switch or stack.
Port ID	Identifies the port that transmitted the LLDPDU.
Time To Live (TTL)	Indicates the length of time in seconds for which the information received in the LLDPDU remains valid. If the value is greater than zero, the information is stored in the LLDP remote system MIB. If the value is zero, the information previously received is no longer valid, and is removed from the MIB.
End of LLDPDU	Signals that there are no more TLVs in the LLDPDU.

Table 2: TLVs in LLDP advertisements (continued)

TLV	DESCRIPTION
Optional Base TLVs—IEEE 802.1AB-2005	
Port description	A description of the device's port in alpha-numeric format.
System name	The system's assigned name in alpha-numeric format.
System description	A description of the device in alpha-numeric format. This includes information about the device's hardware and operating system.
System capabilities	The device's router and bridge functions, and whether or not these functions are currently enabled.
Management address	The address of the local LLDP agent. This can be used to obtain information related to the local device.
IEEE 802.1 Organizationally Specific TLVs (802.1 TLVs)—IEEE 802.1AB-2005 Annex F	
Port VLAN	VLAN identifier that the local port associates with untagged or priority tagged frames.
Port & Protocol VLANs	Whether Port & Protocol VLAN is supported and enabled on the port, and the list of Port & Protocol VLAN identifiers.
VLAN Names	List of VLAN names that the port is assigned to.
Protocol IDs	List of protocols that are accessible through the port, for instance: ■ 9000 (Loopback) ■ 00 26 42 42 03 00 00 00 (STP) ■ 00 27 42 42 03 00 00 02 (RSTP) ■ 00 69 42 42 03 00 00 03 (MSTP) ■ 888e01 (802.1x) ■ aa aa 03 00 e0 2b 00 bb (EPSR) ■ 88090101 (LACP) ■ 00540000e302 (Loop protection) ■ 0800 (IPv4) ■ 0806 (ARP) ■ 86dd (IPv6)
IEEE 802.3 Organizationally Specific TLVs (802.3 TLVs)—IEEE 802.1AB-2005 Annex G	
MAC/PHY Configuration/ Status	The current values of the following for the port: ■ Speed and duplex mode auto-negotiation support ■ Auto-negotiation status ■ PMD (physical media dependent) auto-negotiation advertised capability ■ Operational MAU type This TLV is always included in LLDP-MED advertisements.
Power Via MDI	The power-via-MDI capabilities. On devices that are LLDP-MED and PoE-capable, we recommend using the Extended Power-via-MDI TLV instead of this TLV.
Link Aggregation	Whether the link is capable of being aggregated, whether it is currently in an aggregation and if in an aggregation, the port of the aggregation.
Maximum Frame Size	The maximum supported 802.3 frame size that the sending device is capable of receiving—larger frames will be dropped.
LLDP-MED Organizationally Specific TLVs (LLDP-MED TLVs)—ANSI/TIA-1057- 2006	
LLDP-MED Capabilities	Indicates an LLDP-MED capable device, and advertises which LLDP-MED TLVs are supported and enabled, and the device type. For this switch, the device type is Network Connectivity Device. An advertisement containing this TLV is an LLDP-MED advertisement.

Table 2: TLVs in LLDP advertisements (continued)

TLV	DESCRIPTION
Network Policy	Network policy information configured on the port for connected media endpoint devices. The switch supports Application Type 1: Voice, including the following network policy for connected voice devices to use for voice data: ■ Voice VLAN ID ■ Voice VLAN User Priority tagging ■ Voice VLAN Diffserv Code Point (DSCP)
Location Identification	Location information configured for the port, in one or more of the following formats: ■ Civic address ■ Coordinate-based LCI ■ Emergency Location Identification Number (ELIN) For more information, see "LLDP-MED: Location Identification TLV" on page 8.
Extended Power-via-MDI	For PoE-capable devices, this TLV includes: ■ Power Type field: Power Sourcing Entity (PSE). ■ Power Source field: current power source, either Primary Power Source or Backup Power Source. ■ Power Priority field: power priority configured on the port. ■ Power Value field: In TLVs transmitted by Power Sourcing Equipment (PSE) such as this switch, this advertises the power that the port can supply over a maximum length cable based on its current configuration (that is, it takes into account power losses over the cable). In TLVs received from Powered Device (PD) neighbors, the power value is the power the neighbor requests.
Inventory Management TLV Set	Includes the following TLVs, based on the current hardware platform and the software version, identical on every port on the switch: ■ Hardware Revision ■ Firmware Revision ■ Software Revision ■ Serial Number ■ Manufacturer Name ■ Model Name ■ Asset ID On Virtual Chassis Stacking devices, the inventory information is based on the current master.

LLDP-MED: Location Identification TLV

Location information can be configured for each port, and advertised to remote devices, which can then transmit this information in calls; the location associated with voice devices is particularly important for emergency call services. All ports may be configured with the location of the switch, or each port may be configured with the location of the remote voice device connected to it.

The location information for a particular port can be configured using one or more of the following three data formats: coordinate-based, Emergency Location Identification Number (ELIN), and civic address. Up to one location of each type can be assigned to a port.

Location configuration information (LCI) in all configured data formats is transmitted in Location Identification TLVs. When LLDP receives a Location Identification TLV, it updates the remote entry in the LLDP-MED MIB with this information.

Co-ordinate LCI

Coordinate-based location data format uses geospatial data, that is, latitude, longitude, and altitude (height or floors), including indications of resolution, with reference to a particular datum: WGS 84, NAD83—North American Vertical Datum of 1988 (NAVD88), or NAD83—Mean Lower Low Water (MLLW). For more information, see RFC 3825, Dynamic Host Configuration Protocol Option for Coordinate-based Location Configuration Information.

ELIN LCI

Emergency Location Identification Number (ELIN) location data format provides a unique number for each location for Emergency Call Services (ECS). In North America, ELINs are typically 10 digits long; ELINs up to 25 digits are supported.

Civic Address LCI

The Civic Address location data format uses common street address format, as described in RFC4776.

Transmission and Reception

Table 3 describes the LLDP transmission and reception processes. Additional LLDP-MED processes are described in "LLDP-MED Operation" on page 10.

Table 3: LLDP transmission and reception processes

WHEN ...	AND ...	THEN ...
LLDP is enabled.	Ports are configured to transmit LLDP advertisements.	Regular LLDP advertisements are sent via these ports at intervals determined by the transmit interval. Each advertisement contains local information (from the Local Systems MIB) for all the mandatory TLVs and the optional TLVs that the port is configured to send.
	Ports are configured to receive LLDP advertisements.	Information received in advertisements via the se ports is stored in the Neighbor table (Remote Systems MIB). This information is retained until it is replaced by a more recent advertisement from the same neighbor or it times out (the TTL elapses).
Local information changes.	The transmission delay time has elapsed since the last advertisement was transmitted.	New advertisements are sent containing the new set of local information.
Neighbor information changes.	Notifications are enabled, and the notification interval has elapsed since the last notification was sent	The SNMP notification (trap) lldpRemTablesChange is sent.
LLDP transmission and reception is disabled on a port.	An LLDP command was used to do this.	It transmits a final 'shutdown' LLDPDU with a Time-To-Live (TTL) TLV that has a value of "0". This tells any remote neighboring devices to remove the information associated with this switch from their remote systems MIB. Then it stops transmitting and receiving advertisements. The neighbor information remains in the Remote Systems MIB until it times out.
	A shutdown command was used on the port.	It makes a best effort to send a 'shutdown' LLDPDU. Then it stops transmitting and receiving advertisements. The neighbor information remains in the Remote Systems MIB until it times out.
	Something else disabled LLDP, such as Virtual Chassis Stacking (VCStack) failover.	It does not send a 'shutdown' LLDPDU. It stops transmitting and receiving advertisements. The neighbor information remains in the Remote Systems MIB until it times out.
	It is enabled again.	LLDP reinitializes and resumes transmitting and receiving advertisements after the reinitialization interval has elapsed.
The Neighbor table has 1600 neighbors.		It discards any further neighbors.
LLDP receives a LLDPDU or TLV with a detectable error.		It discards the incorrect TLV.
LLDP receives a TLV it does not recognize.	It contains no basic format errors.	It stores it for possible later retrieval by network management (in the unrecognized TLV information table lldpRemUnknownTLVTable in the LLDP MIB).

LLDP-MED Operation

When LLDP is enabled, LLDP-MED is enabled by default, however the device will not advertise any LLDP-MED TLVs onto a link until it has first received an LLDPDU containing an LLDP-MED TLV on that link.

Once the device has received a LLDPDU with LLDP-MED TLVs from a newly connected LLDP-MED-capable device, it transmits one LLDP-MED advertisement per second via this port, a configurable number of times. You can configure the LLDP-MED advertisement rate using the command: **lldp fast start-count**.

Aside from these deviations, transmission of LLDPDUs containing LLDP-MED TLVs follows the process as described in Table 3.

If LLDP-MED notifications are enabled for a port, and SNMP traps for LLDP are enabled, LLDP-MED generates a Topology Change Notification (LLDP-MED lldpXMedTopology ChangeDetected) when a new LLDP-MED compliant IP telephony device is connected to a port or removed from a port. This notification includes the following information:

- IP Phone Chassis ID and Chassis ID sub-type (IP address)
- LLDP Endpoint Device Class
- Switch Chassis ID (MAC address) and Port ID where the device is attached

Storing LLDP Information

When an LLDP device receives a valid LLDP advertisement from a neighboring network device, it stores the information in an IEEE-defined Simple Network Management Protocol (SNMP) Management Information Base (MIB).

LLDP stores information in the LLDP MIB defined in Section 12 of the IEEE Standard 802.1AB-2005, its extensions defined in Annex F, Annex G, and ANSI/TIA-1057- 2006, about:

LLDP-EXT-MED-MIB ANSI/TIA-1057- 2006, Section 13.3, LLDP-MED MIB Definition

- Local system information. This is the information that LLDP can transmit in advertisements to its neighbors.
- Remote systems information. This is the data that the device receives in advertisements from its neighbors.
- LLDP configuration. This can be used with SNMP to configure LLDP on the device.
- LLDP statistics. This includes information about LLDP operation on the device, including packet and event counters.

This information can be accessed either via SNMP, or directly using the command line interface.

Local system

Information about your device is called local system information. The LLDP local system MIB maintains this information, which consists of device details, as well as any user-configured information that you have set up for your switch, for example a port description or a management address.

LLDP on this device can store one management address per port, and transmit this in LLDP advertisements. It can store multiple management addresses received from each neighbor.

Remote systems

Information gained from neighboring devices is called remote system information. The LLDP remote systems MIB maintains this information.

The length of time for which neighbor information remains in the LLDP remote systems MIB is determined by the Time-To-Live (TTL) value of received LLDPDUs. When it receives an advertisement from a neighbor, LLDP starts a timer based on the Time To Live (TTL) information in the advertisement.

TTL information in an advertisement is:

TTL=transmit interval x holdtime multiplier. If the TTL elapses, for instance if the neighbor has been removed, LLDP deletes the neighbor's information from the MIB. This ensures that only valid LLDP information is stored.

Whenever a new neighbor is discovered, or an existing neighbor sends an advertisement with new information that differs from the previous advertisement, for example a new or changed TLV, a remote tables change event is activated. If SNMP notifications are enabled, the notification lldpRemTablesChange is sent.

To prevent the remote systems MIB from using large amounts of memory and possibly affecting the operation of your switch, it limits the number of neighbors it stores information for to 1600. If it is storing information from 1600 neighbors, and detects any more neighbors, it is considered to have too many neighbors, and discards advertisements from the rest. There is no per-port limit to the number of neighbors.

SNMP utilities

An SNMP utility can read the Neighbors table MIB (Remote Systems Data in the LLDP MIB) on a device to find out about the LLDP neighbors it is directly connected to on each port. Then it can read the Neighbors table MIB on each of these neighbors to find out about their neighboring LLDP devices, and so on.

Configuring LLDP

You can configure LLDP on the device using either:

- the command line interface
- SNMP

This section includes the following command line interface configuration procedures:

- "Configure LLDP" on page 12— This procedure includes configuration for LLDP between network connectivity devices; it does not include LLDP-MED. If you are configuring LLDP-MED only, use the following procedure instead of this one.
- "Configure LLDP-MED" on page 15—This procedure includes the LLDP configuration required to support LLDP-MED, as well as specific LLDP-MED and Voice VLAN configuration.
- "Configure Authentication for Voice VLAN using a RADIUS Server" on page 19—This procedure includes 802.1X port authentication configuration including dynamic VLAN assignment to be used with LLDP-MED. Use the previous procedure before using this one.

Because LLDP is often used together with SNMP, consider configuring SNMP before you configure LLDP. LLDP transmits large amounts of data about the network. For security reasons, we recommend configuring SNMP for SNMP version 3 only (for read and write access). Remove all SNMPv1 and SNMPv2 configuration.

Configure LLDP

Use the procedure described below to configure LLDP.

Some optional TLVs send information that can be configured by other commands. If LLDP will be configured to send these TLVs, consider whether to configure the corresponding parameters first.

- Port Description
- System Name

Table 4: Configuration procedure for LLDP

Step 1. Enable LLDP		
	`awplus#configure terminal`	Enter Configuration mode.
	`awplus(config)#lldp run`	Enable LLDP.
Step 2. Configure ports for LLDP		
	Configure each port to determine whether and which LLDP messages are transmitted and received. If all the ports running LLDP require the same configuration, configure them all together. Otherwise repeat these commands for each port or group of ports that requires a particular configuration.	
	`awplus(config)# interface <port-list>`	Enter Interface Configuration mode for the switch ports.
	`awplus(config-if)#lldp tlv-select {[<tlv>]...}` `awplus(config-if)#lldp tlv-select all`	By default, the mandatory TLVs are included in LLDP messages. Enable the transmission of one or more optional TLVs through these port as required.
	`awplus(config-if)#exit`	Return to Global Configuration mode.

Table 4: Configuration procedure for LLDP

	`awplus(config)#interface <port-list>`	By default, transmission and reception of LLDP advertisements is enabled on all ports. Enter Interface Configuration mode for any switch ports that should have transmission or reception disabled.
	`awplus(config-if)#no lldp {[transmit] [receive]}`	Disable transmission and/or reception as required.
	`awplus(config-if)#exit`	Return to Global Configuration mode.
	`awplus(config)#exit`	Return to Privileged Exec mode.
Step 3. Check LLDP configuration		

	`awplus#show lldp`
	`awplus#show lldp interface [<port-list>]`
	`awplus#show lldp local-info [base] [dot1] [dot3] [med] [interface <port-list>]`
	`awplus#show running-config lldp`
		Review the LLDP configuration.

Step 4. Monitor LLDP		

	`awplus#show lldp neighbors`
	`awplus#show lldp neighbors detail`
	`awplus#show lldp statistics`
	`awplus#show lldp statistics interface [<port-list>]`
		Monitor LLDP operations and display neighbor information as required.

Step 5. Advanced LLDP configuration		
	The configuration procedure above and the defaults for other settings suit most networks. Use the following commands for fine tuning if necessary. Timer intervals should be long enough not to create unnecessarily high numbers of advertisements when there are topology changes. However, be aware that if the intervals are long, a neighbor's information can continue to be stored after its information has changed, or after it is disconnected.	
	`awplus#configure terminal`	Enter Configuration mode.
	`awplus(config)#interface <port-list>`	Enter Interface Configuration mode for the switch ports.
	`awplus(config-if)#lldp management-address <ipaddr>`	Override the default LLDP management address advertised through this port if required. This must be an IPv4 address that is already configured on the device.
	`awplus(config-if)#lldp notifications`	By default, SNMP notifications are not transmitted. Enable them for these ports if required. (SNMP LLDP traps (notifications) must also be enabled.)
	`awplus(config-if)#exit`	Return to Global Configuration mode.
	`awplus(config)#lldp timer <5-32768>`	The transmit interval determines how often regular LLDP transmits are advertised from each port. The transmit interval must be at least four times the transmission delay. Default: 30 seconds

Table 4: Configuration procedure for LLDP

	`awplus(config)#lldp notification-interval <5-3600>`	The notification interval determines the minimum interval between sending SNMP notifications (traps). Default: 5 seconds
	`awplus(config)#lldp tx-delay <1-8192>`	A series of successive changes over a short period of time can trigger the agent to send a large number of LLDPDUs. To prevent this, there is a transmission delay timer. This establishes a minimum length of time that must elapse between successive LLDP transmissions. The transmission delay cannot be greater than a quarter of the transmit interval. Default: **2** seconds
	`awplus(config)#lldp reinit <1-10>`	Reinitialization delay timer determines the minimum time after disabling LLDP on a port before it can reinitialize. Default: **2** seconds
	`awplus(config)#lldp holdtime-multiplier <2-10>`	The transmit interval is multiplied by the holdtime multiplier to give the Time To Live (TTL) value that is advertised to neighbors. Default: **4** (i.e. by default, the TTL is 4 times the holdtime)
	`awplus(config)#exit`	Return to Privileged Exec mode.
Step 6. Clear data		
	If necessary, you can clear either neighbor information or LLDP statistics for particular ports or all ports.	
	`awplus#clear lldp table [interface <port-list>]`	Clear the information from the table of neighbor information.
	`awplus#clear lldp statistics [interface <port-list>]`	Clear LLDP statistics (packet and event counters).

Configure LLDP-MED

Use the procedure in the table below, to configure LLDP-MED and Voice VLAN for voice devices connected to the switch.

Consider whether you also need to configure:

- Simple Network Management Protocol
- 802.1X port authentication
- RADIUS server
- RADIUS server
- Quality of Service
- Access Control Lists
- Power over Ethernet (PoE), if the switch supports PoE

In most cases, configuring LLDP-MED using SNMP or using the CLI command line interface (CLI) has the same effect. However, the effect of configuring location information using SNMP differs from the CLI. When location information is assigned to a port by SNMP and a matching location is not found on the device, then a new location is automatically created and assigned to the specified port.

If the location is unset by SNMP later, then the location is removed to prevent accumulating SNMP-set location information. However, if the location is being used for other ports, the automatically created location is not removed until no ports use it. Once it is modified or assigned to other ports by CLI commands, the location remains even after no ports use the location.

Table 5: Configuration procedure for Voice VLAN and LLDP-MED

Step 1. Configure a Voice VLAN		
	Create a VLAN for voice data from voice endpoint devices connected to ports on the switch. Specify the network policy for voice data in this voice VLAN. LLDP-MED sends the network policy to voice devices connected to these ports. The voice devices use this network policy to determine the VLAN, priority and DSCP tagging of voice data it transmits.	
	`awplus# configure terminal`	Enter Global Configuration mode.
	`awplus(config)# vlan database`	Enter VLAN Database Configuration mode.
	`awplus(config-vlan)# vlan <vid> [name <vlan-name>] [state {enable|disable}]`	Create a VLAN to be used for the voice data to and from voice devices connected to the switch. By default, the new VLAN is enabled.
	`awplus(config-vlan)# exit`	Return to global configuration mode.
	`awplus(config)# interface <port-list>`	Enter interface configuration mode for the ports to be configured with the same network policy. This may be all the switch ports with voice devices connected to them, or a subset if the network policy will differ between ports.
	`awplus(config-if)# switchport voice vlan [<vid>| dot1p|dynamic|untagged]`	Specify the VLAN tagging to be used for voice data on these ports. Use the **dynamic** option if the VLAN tagging will be allocated dynamically by a RADIUS server. To configure authentication and dynamic VLAN allocation using the local RADIUS server, see the procedure in Table 6 on page 19. Default: **none**.

Table 5: Configuration procedure for Voice VLAN and LLDP-MED

	`awplus(config-if)# switchport voice vlan priority <0-7>`	Specify the priority-tagging that voice endpoint devices should put into their data packets. Default: **5**.
	`awplus(config-if)# switchport voice dscp <0-63>`	Specify the DSCP value that voice endpoint devices should put into their data packets. Default: **0**.
	`awplus(config-if)# exit`	Return to global configuration mode.
Step 2. Enable LLDP		
	`awplus(config)# lldp run`	Enable LLDP on the switch. Default: LLDP is **disabled**.
	`awplus(config)# interface <port-list>`	Enter interface configuration mode for the switch ports LLDP is NOT to run on.
	`awplus(config-if)# no lldp {[transmit] [receive]}`	Disable transmission or reception on these ports as required. Default: **transmit** and **receive** enabled.
	`awplus(config-if)# exit`	Return to global configuration mode.
Step 3. Configure LLDP-MED location information Create civic address, coordinate, and/or ELIN locations, and assign them to switch ports.		
	`awplus(config)# location civic-location identifier <civic-loc-id>`	Specify a civic location ID, and enter configuration mode for this identifier.

	`awplus(config-civic)# country <country>`
	`awplus(config-civic)# city <city>`
	`awplus(config-civic)# primary-road-name <primary-road-name>`
	`awplus(config-civic)# street-suffix <street-suffix>`
	`awplus(config-civic)# house-number <house-number>`
	`awplus(config-civic)# <other-civic-location-parameters …>`
		Specify the civic address location information for the civic address location ID. You must specify a country first, using the upper-case two-letter country code, and then at least one more parameter.
		
		For the full set of parameters you can use to specify civic address location, see the **location civic-location** configuration command in the LLDP chapter of the command reference.

	`awplus(config-civic)# exit`	Return to global configuration mode.
	`awplus(config)# location coord-location identifier <coord-loc-id>`	Specify a coordinate location identifier, and enter configuration mode for this identifier.

	`awplus(config-coord)# latitude <latitude>`
	`awplus(config-coord)# lat-resolution <lat-resolution>`
	`awplus(config-coord)# longitude <longitude>`
	`awplus(config-coord)# long-resolution <long-resolution>`
	`awplus(config-coord)# altitude <altitude> {meters|floor}`
	`awplus(config-coord)# alt-resolution <alt-resolution>`
	`awplus(config-coord)# datum {wgs84|nad83-navd|nad83-mllw}`
		Specify the coordinate location for the coordinate location identifier.

Table 5: Configuration procedure for Voice VLAN and LLDP-MED

	`awplus(config-coord)# exit`	Return to global configuration mode.
	`awplus(config)# location elin-location <elin> identifier <elin-loc-id>`	Specify an ELIN location identifier, and the ELIN for this identifier.
	`awplus(config)# interface <port-list>`	Enter interface configuration mode for one or more switch ports which require the same location information.

	`awplus(config-if)# location civic-location-id <civic-loc-id>`
	`awplus(config-if)# location coord-location-id <coord-loc-id>`
	`awplus(config-if)# location elin-location-id <elin-loc-id>`
		Assign the civic, coordinate, and/or ELIN location identifier to these ports.
		LLDP-MED will send the location information associated with a port to the voice endpoint device attached to it.

	`awplus(config-if)# exit`	Return to global configuration mode.
	`awplus(config)# exit`	Return to Privileged Exec mode.
Step 4. Review the LLDP configuration		
	`awplus# show lldp`	Check general LLDP configuration settings.
	`awplus# show lldp interface [<port-list>]`	Check LLDP configuration for ports.
	`awplus# show lldp local-info [base] [dot1] [dot3] [med] [interface <port-list>]`	Check the information that may be transmitted in LLDP advertisements from ports.

	`awplus# show location {civic-location|coord-location|elin-location}`
	`awplus# show location {civic-location|coord-location|elin-location} identifier {<civic-loc-id>|<coord-loc-id>|<elin-loc-id>}`
	`awplus# show location {civic-location|coord-location|elin-location} interface <port-list>`
		Check the location information.

	`awplus# show running-config lldp`	If you want to display all the LLDP configuration, use this command.
Step 5. Monitor LLDP-MED		

	`awplus# show lldp neighbors [interface <port-list>]`
	`awplus# show lldp neighbors detail [base] [dot1] [dot3] [med] [interface <port-list>]`
	`awplus# show lldp statistics`
	`awplus# show lldp statistics interface [<port-list>]`
		Monitor LLDP operation.

Step 6. Advanced configuration		
	The configuration procedure above and the defaults for other settings suit most networks. Use the following commands for fine tuning if necessary. For information about other advanced configuration for LLDP, including LLDP timers, see Table 4 on page 12.	
	`awplus#configure terminal`	Enter Global Configuration mode.

Table 5: Configuration procedure for Voice VLAN and LLDP-MED

	`awplus(config)# lldp faststart-count <1-10>`	By default, when LLDP-MED detects an LLDP-MED capable device on a port, it sends 3 advertisements at 1s intervals. Change the fast start count if required. Default: fast start count is 3
	`awplus(config)# lldp non-strict-med-tlv-order-check`	By default non-strict order checking for LLDP-MED advertisements is disabled. That is, strict order checking is applied to LLDP-MED advertisements, and LLDP-MED TLVs in non-standard order are discarded. If you require LLDP-MED advertisements with non-standard TLV order to be received and stored, enable non-strict order checking.
	`awplus(config)# interface <port-list>`	Enter interface configuration mode for switch ports which will have the same advanced configuration.
	`awplus(config-if)# lldp management-address <ipaddr>`	Override the default LLDP management address advertised through this port if required. This must be an IPv4 address that is already configured on the device. To see the management address that will be advertised, use the **show lldp local-info** command.
	`awplus(config-if)# lldp med-notifications`	By default, SNMP notifications are not transmitted. Enable LLDP-MED Topology Change Detected notifications for these ports if required. (SNMP LLDP traps (notifications) must also be enabled.) Default: LLDP-MED notifications disabled
	`awplus(config-if)# lldp tlv-select {[<tlv>]...}`	Enable the transmission of one or more optional LLDP TLVs in LLDP-MED advertisements through this port as required. The **mac-phy-config** TLV is transmitted in LLDP-MED advertisements whether or not it is enabled by this command. Default: all mandatory TLVs are enabled.

	`awplus(config-if)# lldp med-tlv-select {[capabilities] [network-policy] [location] [power-management-ext] [inventory-management]}`
	`awplus(config-if)# lldp med-tlv-select all`
	`awplus(config-if)# no lldp med-tlv-select {[capabilities] [network-policy] [location] [power-management-ext] [inventory-management]}`
	`awplus(config-if)# no lldp med-tlv-select all`
		Enable or disable the transmission of optional LLDP-MED TLVs in LLDP-MED advertisements through these ports as required.
		Default: **capabilities**, **network-policy**, **location**, **power-management** are enabled.

	`awplus(config-if)# exit`	Return to global configuration mode.
	`awplus(config)# exit`	Return to privileged exec mode.
Step 7. Clear data		
	If necessary, you can clear either neighbor information or LLDP statistics for particular ports or all ports.	
	`awplus# clear lldp table [interface <port-list>]`	Clear the information from the table of neighbor information.
	`awplus# clear lldp statistics [interface <port-list>]`	Clear LLDP statistics (packet and event counters).

Configure Authentication for Voice VLAN using a RADIUS Server

Use the following procedure with LLDP-MED and Voice VLAN to configure 802.1X port authentication and dynamic VLAN assignment using a RADIUS server.

This procedure assumes that you have already:

- configured Voice VLAN and LLDP-MED using the procedure in Table 5 on page 15
- set **switchport voice vlan** to **dynamic** in the above procedure

Table 6: Configuration procedure for Voice VLAN with RADIUS authentication and dynamic VLAN

Step 1. Configure the IP address of the RADIUS server		
	`awplus#configure terminal`	Enter Global Configuration mode.
	`awplus(config)#radius-server host <server-ip-address> key <key-string>`	Configure the IP address for the RADIUS server. Set the key that Network Access Servers (NAS) will need to use to get access to this RADIUS server. RADIUS server hosts configured using this command are included in the default RADIUS server group.
Step 2. Create VLANs		
	`awplus(config)# vlan database`	Enter VLAN Database Configuration mode.
	`awplus(config-vlan)# vlan <vid-range>`	Create the VLANs.
	`awplus(config-vlan)# exit`	Return to Global Configuration mode.
Step 3. Configure 802.1X port authentication		
	`awplus(config)# aaa authentication dot1x default group radius`	Enable 802.1X port authentication and set it to use the default group of RADIUS servers that contains all RADIUS server hosts configured using the **radius-server host** command.
	`awplus(config)# interface <port-list>`	Enter Interface Configuration mode for the ports that have users (PCs and phones) connected to them.
	`awplus(config-if)# dot1x port-control auto`	Enable 802.1X for port authentication on these ports.
	`awplus(config-if)# auth host-mode multi-supplicant`	Configure the ports to use multi-supplicant mode for authentication, so that the phone and PC can be dynamically allocated to different VLANs.
	`awplus(config-if)# auth dynamic-vlan-creation`	Configure the ports to accept dynamic VLAN allocation. In this procedure, the RADIUS server user groups for the PCs and the Phones will use different VLANs, so that the phone traffic will be in the Voice VLAN, and the PC traffic will be in a different, untagged, VLAN.
	`awplus(config-if)# exit`	Return to Global Configuration mode.
	`awplus(config)# exit`	Return to Privileged Exec mode.

Table 6: Configuration procedure for Voice VLAN with RADIUS authentication and dynamic VLAN

Step 4. Review the authentication configuration		
	`awplus# show vlan {all|brief|dynamic|static|auto|static-ports<1-4094>}`	Check the VLAN configuration.
	`awplus# show dot1x [all]`	Check the 802.1X authentication configuration.

Configure authentication for Voice VLAN using the local RADIUS server

Use the following procedure with LLDP-MED and Voice VLAN to configure 802.1X port authentication and dynamic VLAN assignment using the local RADIUS server on the switch to which the voice endpoint devices are connected.

This procedure configures the local RADIUS server. If your configuration uses one or more remote RADIUS servers instead, set the IP addresses of the remote RADIUS servers using the **radius-server host** command and skip all the steps that configure the local RADIUS server.

Table 7: Configuration procedure for Voice VLAN with RADIUS authentication and dynamic VLAN

Step 1. Configure the IP address of the RADIUS host.		
	`awplus#configure terminal`	Enter Global Configuration mode.
	`awplus(config)#radius-server host 127.0.0.1 key <key-string>`	Configure the IP address for the RADIUS server to be the local loopback interface address, so that RADIUS requests are sent to the local RADIUS server. Set the key that Network Access Servers (NAS) will need to use to get access to this RADIUS server.
Step 2. Enable the local RADIUS server.		
	`awplus(config)# radius-server local`	Enter RADIUS Server Configuration mode.
	`awplus(config-radsrv)# server enable`	Enable the local RADIUS server.
	`awplus(config-radsrv)# nas 127.0.0.1 key <key-string>`	Set the switch as a client device (Network Access Server), to allow it to send authentication requests to the local RADIUS server. Use the same local loopback interface IP address and key as in the **radius-server host** command used in Step 1 above.
Step 3. Configure a local RADIUS user group for connected PCs.		
	`awplus(config-radsrv)# group <user-group-name>`	Create a local RADIUS server user group for PCs connected to the switch, and enter RADIUS Server Group Configuration mode.
	`awplus(config-radsrv-group)# vlan {<vid>|<vlan-name>}`	Set the VLAN ID for the user group. This will assign the untagged VLAN ID to authenticated ports for PCs connected to the switch. To create multiple user groups for PCs with different VLANs, repeat these two steps.
	`awplus(config-radsrv-group)#exit`	Return to RADIUS Server Configuration mode.

Table 7: Configuration procedure for Voice VLAN with RADIUS authentication and dynamic VLAN (continued)

Step 4. Configure a local RADIUS user group for connected phones.		
	`awplus(config-radsrv)# group <user-group-name>`	Create a new local RADIUS server user group for phones connected to the switch, and enter RADIUS Server Group Configuration mode.
	`awplus(config-radsrv-group)# egress-vlan-id <vid> tagged`	Set the Egress-VLAN ID attribute for the user group, and set it to send tagged frames. This will assign the tagged VLAN ID to authenticated ports for phones connected to the switch. To create multiple user groups for phones with different VLANs, repeat these two steps.
	`awplus(config-radsrv-group)# exit`	Return to RADIUS Server Configuration mode.
Step 5. Add users to the local RADIUS server.		
	`awplus(config-radsrv)# user <radius-user-name> password <user-password> group <user-group>`	Add RADIUS user names and passwords to the local RADIUS server for authenticating PCs and phones. Assign the corresponding RADIUS server user groups configured in Step 3 and Step 4.
	`awplus(config-radsrv)# exit`	Return to Global Configuration mode.
Step 6. Create VLANs.		
	`awplus(config)# vlan database`	Enter VLAN Database Configuration mode.
	`awplus(config-vlan)# vlan <vid-range>`	Create the VLANs corresponding to the VLAN IDs that will be allocated to the authenticated ports, as configured in Step 3 and Step 4.
	`awplus(config-vlan)# exit`	Return to Global Configuration mode.
Step 7. Configure 802.1X port authentication.		
	`awplus(config)# aaa authentication dot1x default group radius`	Enable 802.1X port authentication and set it to use the default group of RADIUS servers that contains all RADIUS server hosts configured using the **radius-server host** command. In this procedure, the default group consists of the local RADIUS server.
	`awplus(config)# interface <port-list>`	Enter interface configuration mode for the ports that have users (PCs and phones) connected to them.
	`awplus(config-if)# dot1x port-control auto`	Enable 802.1X for port authentication on these ports.
	`awplus(config-if)# auth host-mode multi-supplicant`	Configure the ports to use multi-supplicant mode for authentication, so that the phone and PC can be dynamically allocated to different VLANs.
	`awplus(config-if)# auth dynamic-vlan-creation`	Configure the ports to accept dynamic VLAN allocation. In this procedure, the RADIUS server user groups for the PCs and the Phones allocate different VLANs.
	`awplus(config-if)# exit`	Return to Global Configuration mode.
	`awplus(config)# exit`	Return to Privileged Exec mode.

Table 7: Configuration procedure for Voice VLAN with RADIUS authentication and dynamic VLAN (continued)

Step 8. Review the authentication configuration.		

	`awplus# show radius local-server group [<user-group-name>]`
	`awplus# show radius local-server nas [<ip-address>]`
	`awplus# show radius local-server user [<user-name>]`
		Check the local RADIUS server configuration.

	`awplus# show vlan {all|brief|dynamic|static|auto|static-ports<1-4094>}`	Check the VLAN configuration.
	`awplus# show dot1x [all]`	Check the 802.1X authentication configuration.

C613-22072-00 REV B

North America Headquarters | 19800 North Creek Parkway | Suite 100 | Bothell | WA 98011 | USA | T: +1 800 424 4284 | F: +1 425 481 3895
Asia-Pacific Headquarters | 11 Tai Seng Link | Singapore | 534182 | T: +65 6383 3832 | F: +65 6383 3830
EMEA & CSA Operations | Incheonweg 7 | 1437 EK Rozenburg | The Netherlands | T: +31 20 7950020 | F: +31 20 7950021

alliedtelesis.com