802.1X Authentication,

Link Layer Discovery Protocol (LLDP),

and Avaya IP Telephones

Abstract

The purpose of this document is to discuss 802.1X Authentication and Link Layer Discovery Protocol (LLDP) in Avaya IP Telephones. As of H.323 Release 2.6 for 46xx, H.323 Release 1.0 for 96xx, SIP Release 2.0 for 96xx, and H.323 Release 1.0 for 16xx Avaya IP Telephones, an 802.1X Supplicant is supported. Pass-through of 802.1X messages to support authentication of a PC attached to the phone is also supported. As of H.323 Release 2.6 for 46xx, H.323 Release 1.2 for 96xx, and SIP Release 2.0 for 96xx Avaya IP Telephones, support for LLDP has been added as well. This document outlines the features and their functionality and use.

Table of Contents

Definitions

Acronym	Definition
ANSI	American National Standards Institute
CNA	Converged Network Analyzer
DHCP	Dynamic Host Configuration Protocol
EAP	Extensible Authentication Protocol
EAPoL	Extensible Authentication Protocol over LAN
HTTP	Hyper-Text Transfer Protocol
IEEE	Institute of Electrical and Electronics Engineers
LAN	Local Area Network
LLDP	Link Layer Discovery Protocol
LLDP MED	Link Layer Discovery Protocol for Media Endpoint Devices
MAC	Media Access Control
MIB	Management Information Base
OID	Object Identifier
PoE	Power over Ethernet
QoS	Quality of Service
SNMP	Simple Network Management Protocol
TFTP	Trivial File Transfer Protocol
TIA	Telecommunications Industry Association
TLS	Transport Layer Security
TLV	Type-Length-Value
VLAN	Virtual Local Area Network

1 Introduction

Through the support of 802.1X and Link Layer Discovery Protocol, Avaya IP telephones and PCs connected to the telephone's data port can be authenticated separately, receive different port profiles for QoS and security policies, and communicate over different VLANs. This is accomplished with security features on both the phones and on the Ethernet switches that help guarantee standards-based, enterprise-class secure network access control. In addition, Avaya's support for LLDP provides the ability to consolidate information such as device-type, software version and serial number for inventory management. This same capability also provides a structured workflow for problem diagnosis and root-cause analysis in case of user-reported communication issues. When an IT administrator sees discovery protocol packets, they indicate that the phone is operational, the cable is intact and Layer 2 traffic is functioning. Together these features provide for a complete, interoperable, secure, and simple to deploy solution.

2 802.1X Port-Based Network Access Control

802.1X is an IEEE standard for port-based Network Access Control. It provides authentication to devices attached to an Ethernet switch port, allowing access from that port if authentication succeeds, or preventing access from that port if authentication fails. 802.1X is supported on most Ethernet switches to authenticate attached devices equipped with Supplicant software. Upon detection of a new device (Supplicant), the port on the Ethernet switch (the Authenticator) will be set to the Unauthorized state. In this state, only 802.1X traffic will be allowed; other traffic, such as DHCP and HTTP, will be blocked at the data link layer. The Authenticator will send an EAP-Request/Identity message to the Supplicant, and the Supplicant will respond with an EAP-Response/Identity message that the Authenticator will forward to the Authentication Server. The Authentication Server then requests authentication credentials from the Supplicant; if it is successful, the Authentication Server instructs the Authenticator to set the port to the Authorized state and allow normal traffic. When the Supplicant logs off or disconnects from the port, the Authenticator will return the port to the Unauthorized state, once again blocking all non-EAP traffic.

The 802.1X standard assumes that only a single device is connected to each 802.1X-enabled Ethernet switch port (this is sometimes called Single Supplicant operation). Otherwise, if one device is authenticated and the port is set to the Authorized state, other devices would be able to access the network without being authenticated. However, inexpensive Ethernet hubs and switches are readily available, so it is difficult to prevent multiple devices from being connected. Therefore, most 802.1X-capable switches either block any frame that does not have the same MAC-layer Source Address that was used in the authentication message exchange, or they forward such frames only to a specific VLAN. Some Ethernet switches also go beyond the standard and have the ability to independently authenticate multiple devices on the same port (this is sometimes called Multi Supplicant operation). However, MAC addresses can be spoofed, so none of these approaches is completely foolproof.

2.1 802.1X Pass Through (PC Authentication)

Beginning with 46xx H.323 Release 2.3, 96xx H.323 Release 1.0, 96xx SIP Release 1.0, and 16xx H.323 Release 1.0, the Ethernet switches built into Avaya IP telephones support forwarding of messages that have the 802.1X reserved multicast group address as the MAC-layer Destination Address. This allows a laptop or workstation connected to the secondary Ethernet port on Avaya telephones to authenticate with an Ethernet switch on the network.

Beginning with 46xx H.323 Release 2.6, 96xx H.323 Release 1.0, 96xx SIP Release 2.0, and 16xx H.323 Release 1.0, the telephone can provide additional security by sending an EAPOL-Logoff message to the Ethernet switch when the device connected to the telephone disconnects from the Ethernet port. This functionality, also known as proxy logoff, prevents another device from using the port without first authenticating via 802.1X.

2.2 802.1X Supplicant Operation (Telephone Authentication)

Beginning with 46xx H.323 Release 2.6, 96xx H.323 Release 1.0, 96xx SIP Release 2.0, and 16xx H.323 Release 1.0, an 802.1X Supplicant is supported in the telephones. Depending on a parameter setting, the telephone can support authentication from Ethernet switches that send either unicast or multicast 802.1X (EAPoL) messages. Multicast addressing is typically used by Authenticators that only support Single Supplicant operation, while unicast addressing is used by Authenticators that support Multi Supplicant operation. Beginning with 46xx H.323 Release 2.9, 96xx H.323 Release 2.0, and 96xx SIP Release 2.0, the 802.1X Supplicant in the telephone can be completely disabled for compatibility with some vendors' Authenticators that support Multi Supplicant operation when authentication of the telephone is not desired. Beginning with 46xx H.323 Release 2.9 and 96xx H.323 Release 2.0, the Supplicant in the telephone is disabled by default.

The H.323 IP telephone Supplicants currently support the EAP-MD5 Challenge authentication method, while the 96xx SIP Supplicant also supports the EAP-TLS authentication method.

3 Link Layer Discovery Protocol (LLDP)

LLDP is a standard layer 2 discovery protocol (IEEE Std 802.1AB-2005) that allows networked devices to advertise their identity and capabilities to other devices to which they are directly connected, and is positioned to replace proprietary discovery protocols that are supported by some vendors. LLDP allows network elements to exchange Ethernet speed and duplex settings, for example, to help identify potential mismatches. It also allows an Ethernet switch to aggregate information from all endpoints directly connected to its ports into a single SNMP MIB for easier network management.

LLDP supports the advertisement of capabilities through the asynchronous exchange of Type-Length-Value (TLV) elements, each of which contains a specific piece of information. LLDP was also designed to be extensible, so that additional TLVs could be added in the future, either by the IEEE, or by other standards or industry organizations, or even by individual vendors or groups of vendors that wish to advertise information in proprietary TLVs.

3.1 LLDP on Avaya IP Telephones

Beginning with 46xx H.323 Release 2.6, 96xx H.323 Release 1.2, and 96xx SIP Release 2.0, the telephone is able to transmit LLDP frames out its Ethernet line interface. The telephone can also process selected LLDP frames received on its Ethernet line interface. LLDP frames are not transmitted to, received from, or forwarded to or from the telephone's secondary Ethernet interface. No configuration of the telephone is required to enable LLDP operation. However, to prevent unnecessary frames from being transmitted to a network switch that does not support LLDP, the telephone will not transmit any LLDP information until it first receives an LLDP frame from the network.

Avaya IP telephones support the transmission of the following TLV elements specified in the IEEE LLDP standard:

- **Chassis ID**: contains the IP address of the telephone
- **Port ID**: contains the MAC address of the telephone
- **Time-To-Live**: contains the number of seconds that the recipient should consider the LLDP information to be valid
- **System Name**: contains the same Host Name that the telephone transmits in DHCP option 12
- **System Capabilities**: contains an indication of whether or not the telephone is registered with a call server, whether it has a secondary Ethernet interface, and whether that interface is enabled
- **Management Address**: contains the object identifier (OID) of the telephone's SNMP MIB-II sysObjectID
- **MAC/PHY Configuration/Status**: contains the speed and duplex capabilities that are advertised when autonegotiation is enabled and the current operational speed and duplex settings of the Ethernet line interface
- **End-of-LLDPDU**: indicates the end of an LLDP data unit

In addition, since the network Ethernet switch is in the best position to know which VLAN IDs are supported on each port, LLDP can be used as an alternative to DHCP or manual programming to provide VLAN information to IP telephones.

Avaya IP telephones will take the following actions if the indicated TLV element is received:

- **Port VLAN ID**: sets the value of the PHY2VLAN parameter (the VLAN ID used for frames forwarded to and from the secondary Ethernet interface), which can be used to support VLAN separation from the voice VLAN
- **VLAN Name**: can be used to set the value of L2QVLAN (the VLAN ID of the voice VLAN) if the VLAN name in the TLV begins with "voice" (case insensitive)

3.2 LLDP for Media Endpoint Devices (LLDP MED)

LLDP for Media Endpoint Devices (ANSI/TIA-1057) is an extension to LLDP standardized by the American National Standards Institute and the Telecommunications Industry Association. LLDP MED TLVs are transmitted in addition to LLDP TLVs, they do not replace or supersede them.

Avaya IP telephones support the transmission of the following TLV elements specified in the LLDP MED standard:

- **LLDP-MED Capabilities**: –identifies the types of LLDP MED capabilities supported by the telephone
- **Network Policy**: indicates whether layer 2 frames are being tagged, and if so, contains the voice VLAN ID and the layer 2 user priority (QoS) value, as well as the layer 3 DSCP (Differentiated Services Code Point QoS) value
- **Inventory – Hardware Revision**: contains the full model identifier for the telephone as specified by the parameter MODEL
- **Inventory – Firmware Revision**: contains the name of the boot code image as set in the parameter BOOTNAME
- **Inventory – Software Revision**: contains the file name of the main software image as set in the parameter APPNAME
- **Inventory – Serial Number**: contains the serial number of the telephone
- **Inventory – Manufacturer Name**: contains the name Avaya
- **Inventory – Model Name**: contains a shortened version of the model identifier for the telephone as specified by the parameter MODEL with the final "Dxxx" characters removed.

Beginning with 46xx H.323 Release 2.9, 96xx H.323 Release 3.0, and 96xx SIP Release 2.0, the following actions will be taken if the indicated TLV element is received:

- **Network Policy**: controls whether layer 2 frames transmitted by the telephone are tagged, and if so, contains the voice VLAN ID and the layer 2 user priority QoS value, as well as the layer 3 DSCP (Differentiated Services Code Point) QoS value

3.3 Avaya Proprietary LLDP TLVs

In addition to the standard TLVs listed above, Avaya IP telephones also support the transmission of the following Avaya proprietary TLV elements:

- **PoE Conservation Level Support**: indicates typical and maximum power consumption values for the telephone, as well as any lower-power conservation modes that are supported, such as turning off display backlights
- **Call Server IP Address**: contains the IP address of the call server with which the telephone is registered
- **IP Phone Addresses**: contains the telephone's IP address, its subnet mask, and the IP address of the router
- **CNA Server IP Address**: contains the IP address of the Converged Network Analyzer with which the telephone is registered
- **File Server IP Address**: contains the IP address of the file server used by the telephone
- **802.1Q Framing**: indicates whether the telephone is tagging layer 2 frames

In addition, Avaya IP telephones will take the following actions if the following Avaya proprietary TLV elements are received:

- **Call Server IP Address**: sets the value of the MCIPADD (for H.323) or SIPPROXYSRVR (for SIP) parameter if and only if the current value of the parameter is null (i.e., it will not replace a previously configured value)
- **File Server IP Address**: sets the value of the TLSSRVR, HTTPSRVR and TFTPSRVR parameters if and only if their current values are null (i.e., it will not replace previously configured values)
- **802.1Q Framing**: sets the value of the L2Q parameter, but does not immediately change whether frames are being tagged
- **PoE Conservation Level Request**: enables or disables a power conservation mode.

4 Additional References

- *4600 Series IP Telephone LAN Administrator Guide*
- *Avaya one-X™ Deskphone Edition for 9600 Series IP Telephones Administrator Guide*
- *Avaya one-X™ Deskphone Edition for 9600 Series SIP IP Telephones Administrator Guide*
- *Avaya one-X™ Deskphone Value Edition 1600 Series IP Telephones Administrator Guide*
- http://www.ieee802.org/1/pages/802.1x-2004.html
- http://www.ieee802.org/1/pages/802.1ab.html
- http://www.tiaonline.org/standards/