White paper

IEEE 802.1X in Axis products

March 2020

Table of contents

1. Summary

IEEE 802.1X is a standard for port-based network access control. It is increasingly required as a gatekeeper in today's enterprise networks, and Axis network video products support IEEE 802.1X as a security feature. Configuring IEEE 802.1X is a fairly complex procedure, and it is important that RADIUS servers, switches, and clients (like Axis devices) are set up correctly. However, when RADIUS servers and switches are well configured for 802.1X, it is quite straightforward to configure and integrate Axis network products into the 802.1X system.

2. Introduction

There are different levels of security for a network's infrastructure and the devices connected to it. The first level is authentication and authorization. The user or device identifies itself to the network and the remote end by a username and password, which are then verified before the device is allowed into the system. Added security can be achieved by encrypting the data to prevent others from using or reading the data. Common methods are HTTPS (also known as SSL/ TLS), VPN, and WEP or WPA in wireless networks.

IEEE 802.1X is an authentication and authorization technique. Axis network video products support IEEE 802.1X as a security feature.

This white paper presents the background of IEEE 802.1X, as well as its working principle. It also describes how IEEE 802.1X should be used in Axis devices, and how the RADIUS (remote authentication dial-in user service) servers and switches need to be configured. The intended audience of this document is technical personnel and system integrators.

3. Background

IEEE 802.1X is an IEEE standard for port-based network access control ("port" means the physical connection to the LAN infrastructure). It is part of the IEEE 802.1 group of networking protocols and provides an authentication mechanism for devices to connect to a LAN, either establishing a connection or preventing the connection if authentication fails.

IEEE 802.1X prevents what is called "port hi-jacking", that is, when an unauthorized computer gets access to a network through a network jack inside or outside a building. IEEE 802.1X is useful in network video applications since their devices are often located in public spaces where a network jack can pose a security risk. In modern enterprise networks, IEEE 802.1X is becoming a basic requirement for anything that is connected to a network.

4. Working principle

There are three basic terms in IEEE 802.1X. The user or client that wants to be authenticated is called a supplicant. The actual server doing the authentication, typically a RADIUS server, is called the authentication server. And the device in between, such as a switch, is called the authenticator.

The protocol used in IEEE 802.1X is EAPOL (Extensible authentication protocol encapsulation over LANs). There are several modes of operation, but the most common case is described here and in Figure 1.

1. The authenticator sends an "EAP-Request/Identity" packet to the supplicant as soon as it detects that the network link is active (this could be because the supplicant, for example a specific Axis device in a network video system, is connected to the switch).
2. The supplicant sends an "EAP-Response/Identity" packet to the authenticator.
3. The "EAP-Response/Identity" packet is then passed on to the authentication (RADIUS) server by the authenticator.
4. The authentication server sends back a challenge to the authenticator, such as with a token password system.
5. The authenticator unpacks this from IP and repackages it into EAPOL and sends it to the supplicant. Different authentication methods will vary this message and the total number of messages. EAP supports client-only authentication and strong mutual authentication.
6. The supplicant responds to the challenge by the authenticator.
7. The authenticator passes the response to the challenge onto the authentication server.
8. If the supplicant provides proper identity, the authentication server responds with a success message to the authenticator.
9. The success message is then passed onto the supplicant by the authenticator. The authenticator now allows access of the supplicant to the LAN, possibly restricted based on attributes that came back from the authentication server. For example, the authenticator might switch the supplicant to a particular virtual LAN or install a set of firewall rules.

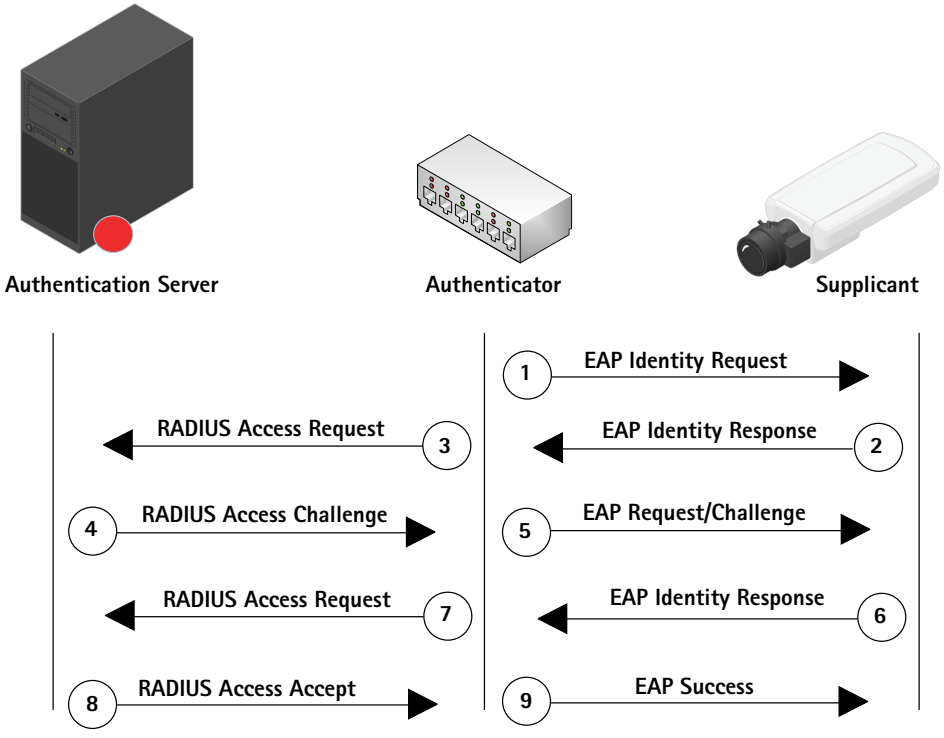

Figure 1. EAP authentication procedure in IEEE 802.1X

It should be noted that setting up and configuring IEEE 802.1X is a fairly complex procedure, and it is important that RADIUS servers, switches, and clients (such as Axis devices) are set up correctly.

5. IEEE 802.1X in Axis products

To gain access to a protected network, the Axis device must have a CA certificate, a client certificate, and a client private key. They should be created by the servers and are uploaded via a web interface. When the Axis device is connected to the network switch, the device will present its certificate to the switch. If the certificate is approved, the switch allows the device access on a preconfigured port.

As pointed out previously, in order to use port-based authentication, the network must be equipped with a RADIUS server and a network switch with support for IEEE 802.1X. You may also need to contact your network administrator for information on certificates, user IDs and passwords depending on the type of RADIUS server that is used.

The settings here enable the Axis device to access a network protected by IEEE 802.1X/EAPOL (Extensible authentication protocol over LAN).

There are many EAP methods available to gain access to a network. The protocol used by Axis is EAP-TLS (EAP-Transport Layer Security) for wired and wireless IEEE 802.1X network authentication as well as EAP-PEAP/MSCHAPv2 for wireless IEEE 802.1 network authentication.

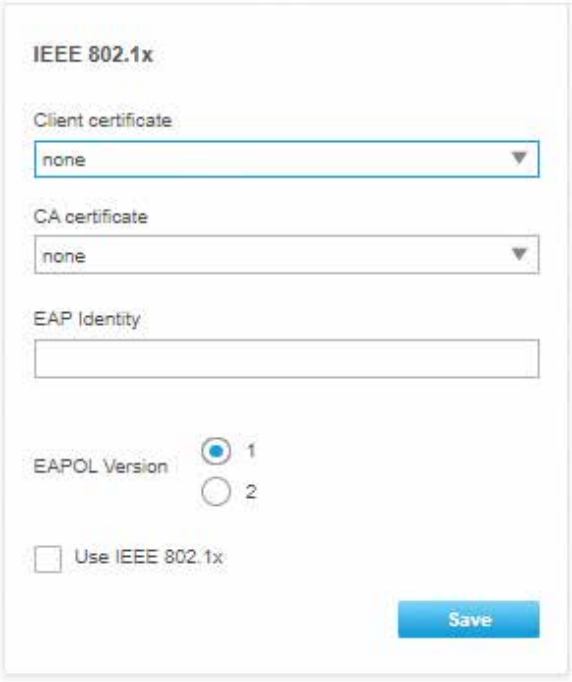

Figure 2. Excerpt of the web interface of AXIS M1065-LW with wired IEEE 802.1X settings (System tab --> Security).

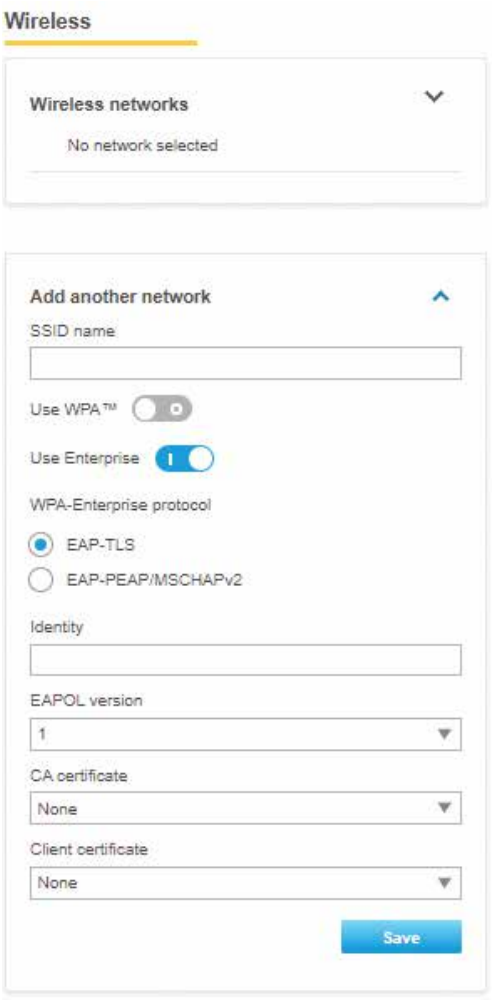

Figure 3. Excerpt of the web interface of AXIS M1065-LW with wireless IEEE 802.1X settings (System tab --> Wireless).

The client and the RADIUS server authenticate each other using digital certificates provided by a PKI (Public key infrastructure) signed by a certification authority. Note that to ensure successful certificate validation, time synchronization should be performed on all clients and servers prior to configuration. Further configuration of Axis devices should be performed on a safe network to avoid MITM (man in the middle) attacks.

Terms used in the web interface are described as follows:

CA certificate - This certificate is created by the certification authority for the purpose of validating itself, so the Axis device needs this certificate to check the server's identity. Select the correct certificate that was uploaded previously in the security tab under CA certificates.

Client certificate - The Axis device must also authenticate itself using a client certificate. Select the correct certificate that was uploaded previously in the security tab under client certificates.

EAPOL version - Select the EAPOL version (1 or 2) used in your network switch.

EAP identity - Enter the user identity associated with your certificate. A maximum of 16 characters can be used.

EN/R1/2003

About Axis Communications

Axis enables a smarter and safer world by creating network solutions that provide insights for improving security and new ways of doing business. As the industry leader in network video, Axis offers products and services for video surveillance and analytics, access control, and audio systems. Axis has more than 3,500 dedicated employees in over 50 countries and collaborates with partners worldwide to deliver customer solutions. Axis was founded in 1984 and has its headquarters in Lund, Sweden.

For more information about Axis, please visit our website www.axis.com.