WHITE PAPER

IEEE 802.1X and Axis' Implementation

AXIS COMMUNICATIONS

Table of contents

1. Introduction

Network security is a very important issue in the IP world. There are different levels of security when it comes to securing information being sent over IP networks. 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. Many Axis network video products support IEEE 802.1X as a security feature. In this white paper we will discuss the background as well as the working principle of IEEE 802.1X. We will also describe how 802.1X in Axis network camera products should be used, and when RADIUS (remote authentication dial-in user service) servers and switches are well configured.

The intended audience of this document is technical personnel and system integrators.

2. General

IEEE 802.1X is an IEEE Standard for port-based Network Access Control ("port" means the same physical connection to the LAN infrastructure). It is part of the IEEE 802.1 group of networking protocols. It 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 by getting to a network jack inside or outside a building. IEEE 802.1X is useful in, for example, network video applications since network cameras are often located in public spaces where a network jack can pose a security risk. In today's enterprise networks, IEEE 802.1X is becoming a basic requirement for anything that is connected to a network.

3. Working principle

There are three basic terms in 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 802.1X is Extensible Authentication Protocol encapsulation over LANs (EAPOL). There are a number of modes of operation, but the most common case would look something like this (see 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 (e.g., the supplicant, for example a network camera 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.

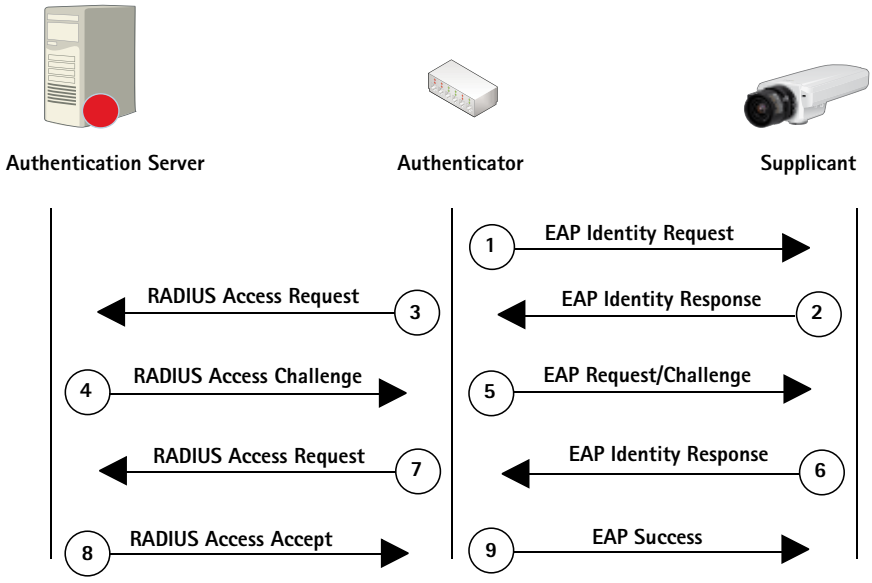

Figure 1.
EAP authentication procedure in IEEE 802.1X

What should be noted is that setting up and configuring 802.1X is a fairly complex procedure, and it is important that RADIUS servers, switches and clients (like Axis cameras) are set up correctly.

4. Axis' implementation of IEEE 802.1X

To gain access to a protected network, the AXIS P1344 Network Camera, for example, must have a CA certificate, a Client certificate, as well as a Client private key. They should be created by the servers and are uploaded via a web interface or ftp. When the camera is connected to the switch, the camera will present its certificate to the network switch. If the certificate is approved, the switch allows the camera 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 802.1X. You may also need to contact your network administrator for information on certificates, user ID's and passwords.

The settings here enable the AXIS P1344 Network Camera to access a network protected by 802.1X/EAPOL (Extensible Authentication Protocol Over Lan).

There are many EAP methods available to gain access to a network. The one used by Axis is EAP-TLS (EAP-Transport Layer Security).

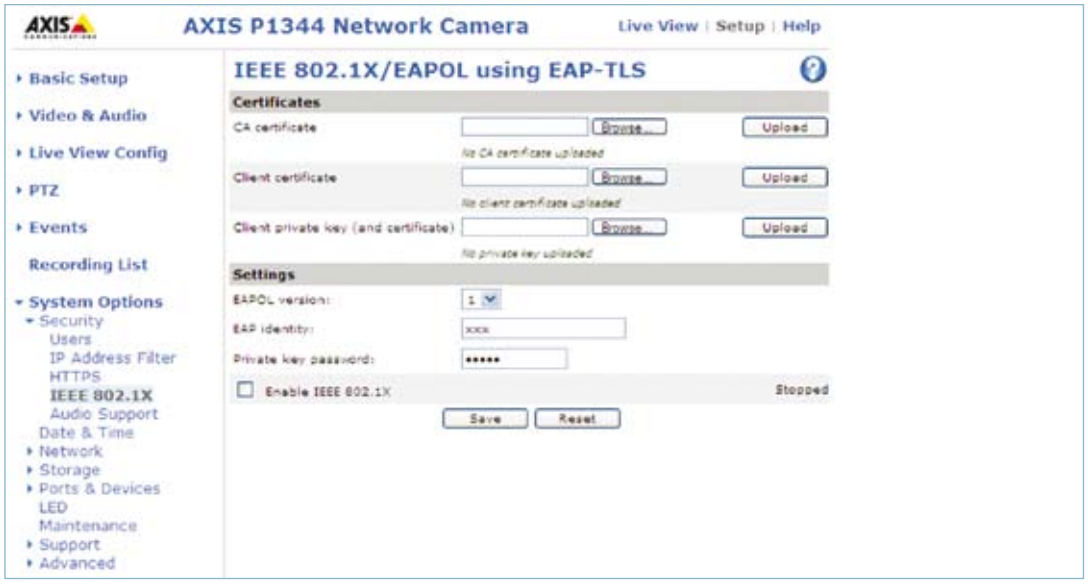

Figure 2.
Web interface with AXIS P1344

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 network cameras 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 P1344 Network Camera needs this certificate to check the server's identity. Provide the path to the certificate directly, or use the browse button to locate it. Then click the Upload button. To remove a CA certificate, click the Remove button.

Client certificate/private key - The AXIS P1344 Network Camera must also authenticate itself using a client certificate and a private key. Provide the path to the certificate in the first field, or use the Browse button to locate it. Then click the Upload button. To remove a client certificate, click the Remove button.

Alternatively, it may be possible to upload the client certificate and key in one combined file, (e.g. a PFX file or PEM file). Provide the path to the file, or use the Browse button to locate it. Click Upload to load the file. To remove a client certificate and key, click the Remove button.

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.

Private key password - Enter the password (maximum 16 characters) for your user identity.

5. Discussion and conclusion

In today's enterprise networks, IEEE 802.1X is more and more required as a gatekeeper. Many Axis network video products support IEEE 802.1X as a security feature. Setting up 802.1X is a fairly complex procedure, and it is important that Radius servers, switches and clients (like Axis cameras) 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.

6. Helpful links

> www.axis.com/products/video/
> www.axis.com/products/video/about_networkvideo/security.htm

www.axis.com

37589/EN/R1/0912

About Axis Communications

Axis is an IT company offering network video solutions for professional installations. The company is the global market leader in network video, driving the ongoing shift from analog to digital video surveillance. Axis products and solutions focus on security surveillance and remote monitoring, and are based on innovative, open technology platforms.

Axis is a Swedish-based company, operating worldwide with offices in more than 20 countries and cooperating with partners in more than 70 countries. Founded in 1984, Axis is listed on the NASDAQ OMX Stockholm under the ticker AXIS. For more information about Axis, please visit our website at www.axis.com

AXIS COMMUNICATIONS