Understanding 802.1X Authentication on EX-series Switches

EX-series switches use 802.1X authentication to implement access control in an enterprise network. Supplicants (hosts) are authenticated at the initial connection to your LAN. By authenticating supplicants before they receive an IP address from a DHCP server, unauthorized supplicants are prevented from gaining access to your LAN.

The 802.1X standard is based on EAP (Extensible Authentication Protocol), a universal authentication framework. EAP is not an authentication mechanism by itself. Instead, EAP provides some common functions and a negotiation method to determine the authentication mechanism (EAP method) used between the supplicant and the authentication server. EAP methods include IETF standards and proprietary standards.

EAP methods supported on EX-series switches are:

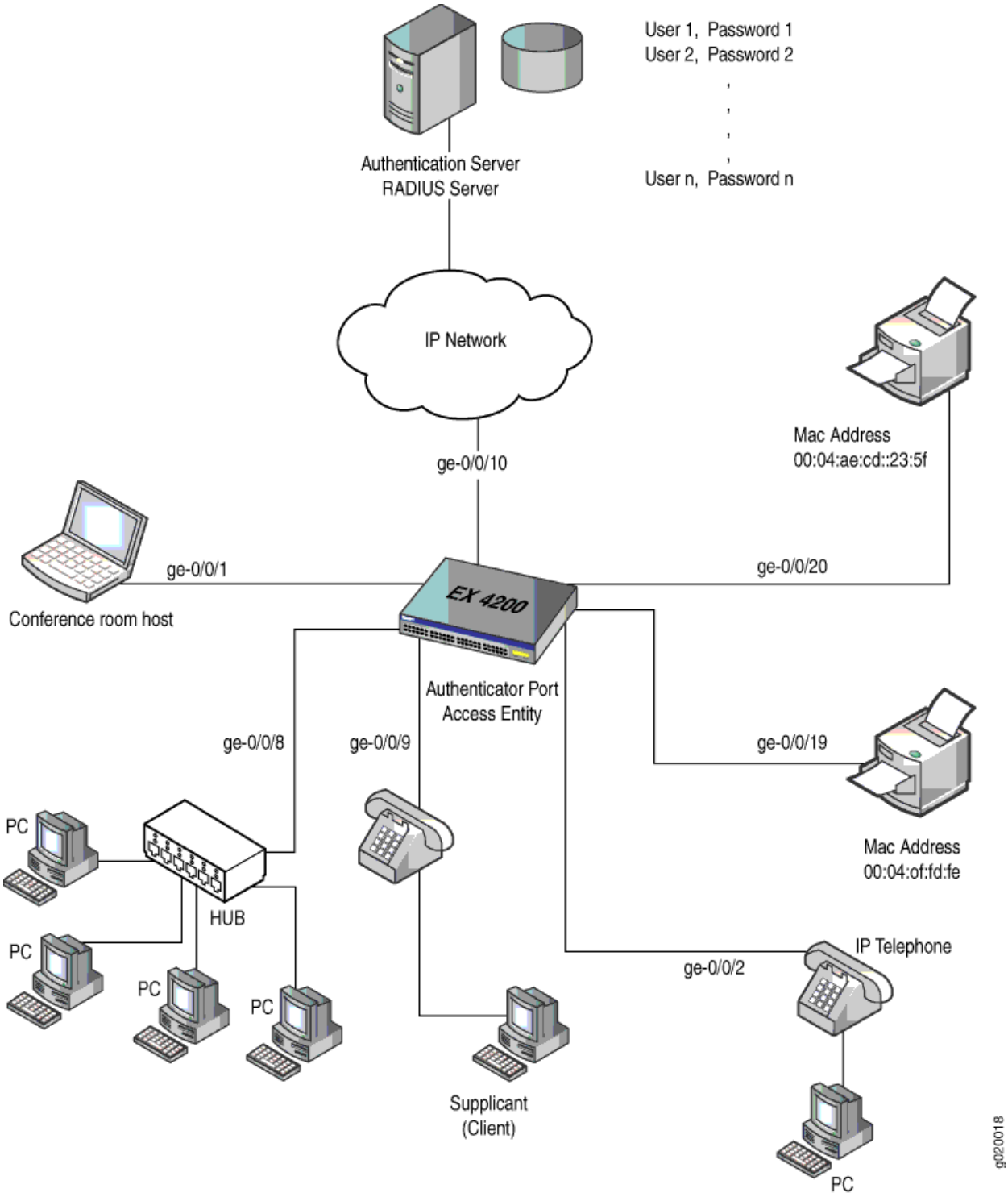
- EAP-MD5
- EAP-TLS
- EAP-TTLS
- EAP-PEAP

A LAN network configured for 802.1X authentication contains three basic components:

- *Supplicant*—The IEEE term for a host that requests to join the network. The host can be responsive or nonresponsive. A responsive host is one on which 802.1X is enabled and provides authentication credentials; specifically, a username and password for EAP MD5, or a username and client certificates for EAP-TLS, EAP-TTLS, and EAP-PEAP. A nonresponsive host is one on which 802.1X is not enabled, but can be authenticated using a MAC-based authentication method.
- *Authenticator Port Access Entity*—The IEEE term for the authenticator. The EX-series switch is the authenticator and it controls access by blocking all traffic to and from supplicants until they are authenticated.
- *Authentication server*— The authentication server contains the backend database that makes authentication decisions. It contains credential information for each supplicant that can connect to the network. The authenticator forwards credentials supplied by the supplicant to the authentication server. If the credentials forwarded by the authenticator match the credentials in the authentication server database, access is granted. If the credentials forwarded do not match, access is denied. The EX-series switches support RADIUS authentication servers.

Figure 1 on page 2 illustrates the basic deployment topology for 802.1X on an EX-series switch:

Figure 1: Example 802.1X Topology

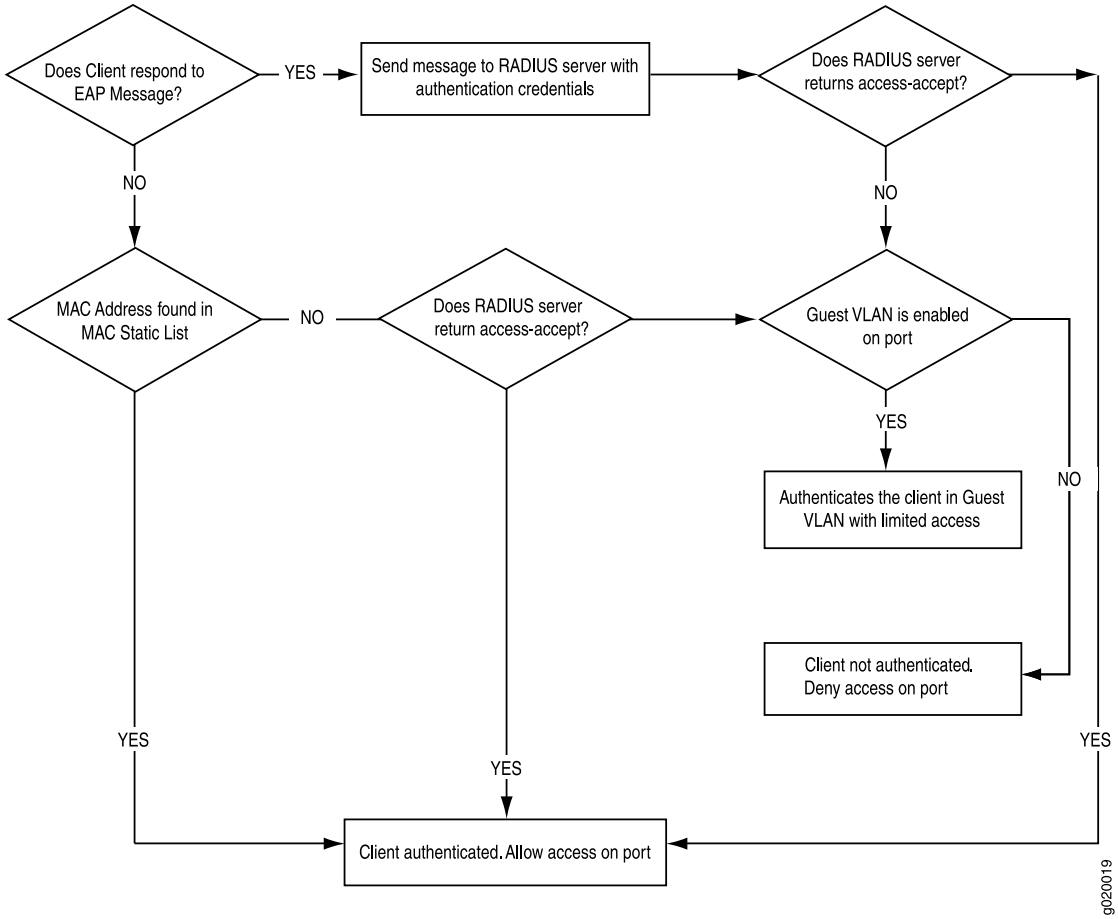


The communication protocol between the supplicant and the EX-series switch is Extensible Authentication Protocol Over LAN (EAPOL). EAPOL is a version of EAP designed to work with Ethernet networks. The communication protocol between the authentication server and the switch is RADIUS.

The authentication process requires multiple message exchanges between the supplicant and the authentication server. The switch that is in between the supplicant and the authentication server is the authenticator. It acts as an intermediary, converting EAPOL messages to RADIUS messages and vice versa.

Figure 2 on page 3 illustrates the authentication process:

Figure 2: Authentication Process



The basic authentication process works like this:

1. Authentication is initiated by the client or the switch. The client initiates authentication by sending an EAPOL-start message, or the switch initiates authentication when it receives the first data packet from the client.
2. When the switch port (authenticator) detects a new supplicant connecting to the LAN network, the port on the authenticator is enabled and set to the initialized

state. In this state, only 802.1X traffic is allowed. Other traffic, such as DHCP and HTTP, is blocked at the data link layer.

3. The authenticator sends a RADIUS access request message to the RADIUS server to allow the supplicant access to the LAN.
4. The authentication server accepts or rejects the access request. If it accepts the request, the authentication server sends a RADIUS access challenge. If the challenge is met by the supplicant, the authenticator sets the port to the authorized state and normal traffic is then accepted to pass through the port. If the authentication server rejects the RADIUS access request, the authenticator sets the port to the unauthorized state, blocking all traffic.
5. When the supplicant disconnects from the network, the supplicant sends an EAP-logoff message to the authenticator. The authenticator then sets the port to the unauthorized state, once again blocking all non-EAP traffic.

The 802.1X authentication feature on an EX-series switch is based upon the IEEE 802.1D standard *Port-Based Network Access Control*.

Related Topics

- 802.1X for EX-series Switches Overview
- Example: Setting Up 802.1X for Single Supplicant or Multiple Supplicant Configurations on an EX-series Switch
- Configuring 802.1X Authentication (CLI Procedure)