

802.1X for EX-series Switches Overview

IEEE 802.1X provides network edge security, protecting Ethernet LANs from Denial of Service (DoS) attacks and preventing unauthorized user access.

802.1X works by using an *Authenticator Port Access Entity* (the switch) to block all traffic to and from a supplicant (client) at the port until the supplicant's credentials are presented and matched on the *Authentication server* (a RADIUS server). When authenticated, the switch stops blocking traffic and opens the port to the supplicant.

The supplicant is authenticated in either *single* mode, *single-secure* mode, or *multiple* mode:

- **single**—Authenticates only the first supplicant. All other supplicants who connect later to the port are allowed full access without any further authentication. They effectively “piggyback” on the first supplicant’s authentication.
- **single-secure**—Allows only one supplicant to connect to the port. No other supplicant is allowed to connect until the first supplicant logs out.
- **multiple**—Allows multiple supplicants to connect to the port. Each supplicant will be authenticated individually.

Network access can be further defined using VLANs and firewall filters, which both act as filters to separate and match groups of supplicants to the areas of the LAN they require.

802.1X does not replace other security technologies. 802.1X works together with port security features, such as DHCP snooping, dynamic ARP inspection (DAI), and MAC limiting, to guard against DoS attacks and spoofing.

802.1X features on EX-series switches are:

- **Guest VLAN**—Provides limited access to a LAN, typically just to the Internet, for supplicants that fail 802.1X authentication.
- **Dynamic VLAN**—Enables a supplicant, after authentication, to be a member of a VLAN dynamically.
- **MAC-based authentication**—Provides MAC-based authentication as a bypass mechanism to authenticate non-responsive hosts (such as printers) that are not 802.1X-enabled. MAC-based authentication connects the non-responsive hosts to 802.1X-enabled ports, bypassing 802.1X authentication.
- **Dynamic changes to a user session**—Lets the switch administrator terminate an already authenticated session. This feature is based on support of the RADIUS Disconnect Message defined in RFC 3576.
- **Support for VoIP**—Supports IP telephones. If the phone is 802-1X enabled, it is authenticated like any other supplicant. When it is authenticated, the RADIUS server returns the Voice VLAN ID and other parameters for managing VoIP traffic. If the phone is not 802.1X-enabled, but has another 802.1X-compatible device connected to its data port, that device is authenticated, and then VoIP traffic can flow to and from the phone.



NOTE: Configuring a voice over IP (VoIP) VLAN on private VLAN (PVLAN) interfaces is not supported.

If the IP phone supports Link Layer Discovery Protocol (LLDP) or Link Layer Discovery Protocol Media Endpoint Discovery (LLDP-MED), the RADIUS server can send VoIP parameters to the IP telephone through these protocols. The VoIP parameters ensure that voice traffic gets tagged and prioritized with the correct values at the source itself. If the phone does not support LLDP or LLDP-MED, then the packets will be put in the VoIP VLAN configured on the switch.

- RADIUS accounting—Sends accounting information to the RADIUS accounting server. Accounting information is sent to the server whenever a subscriber logs in or logs out and whenever a subscriber activates or deactivates a subscription. This feature is based on RFC 2866, *RADIUS Accounting*.
- Vendor Specific Attributes (VSAs)—Supports a new set of filtering attributes that are applied on the RADIUS authentication server. These filtering attributes further define a supplicant's access during the 802.1X authentication process. Centrally configuring VSAs on the authentication server does away with the need to configure these same attributes in the form of firewall filters on every switch in the LAN to which the supplicant may connect to the LAN. This feature is based on RLI 4583, *AAA RADIUS BRAS VSA Support*.

Related Topics

- Understanding Static MAC Bypass of Authentication on EX Series Switches
- Understanding 802.1X Authentication on EX Series Switches
- Understanding 802.1X and VoIP on EX Series Switches
- Understanding 802.1X and LLDP and LLDP-MED on EX Series Switches
- Understanding 802.1X and RADIUS Accounting on EX Series Switches
- Understanding Guest VLANs for 802.1X on EX Series Switches
- Understanding 802.1X and VSAs on EX Series Switches
- Understanding Server Fail Fallback and 802.1X Authentication on EX Series Switches
- Understanding MAC RADIUS Authentication on EX Series Switches

Published: 2009-08-25