

Understanding Guest VLANs for 802.1X on EX-series Switches

Guest VLANs, in conjunction with 802.1X authentication, provide secure access to the LAN for corporate guests and for supplicants who fail the 802.1X authentication process.

When a corporate visitor attempts to authenticate on the LAN, and authentication fails, the visitor is moved to a guest VLAN. A guest VLAN typically provides access only to the Internet.

A guest VLAN can also provide limited access to the LAN in cases when authentication fails for supplicants that are not visitors. When authentication fails, the switch receives an Access-Reject message for the client, and checks if a guest VLAN is configured on that port. If so, it moves that user alone to the guest VLAN. If the Access-reject message contains optional VLAN information, then the user is moved to the VLAN specified by the RADIUS server and not to the locally configured guest-VLAN.

Authentication can fail for many reasons:

- The supplicant machine does not have supplicant software on it (for example, the supplicant is a non-responsive host, such as a printer).
- The supplicant provided invalid credentials—a username or password that were not authenticated by the authentication server.

For non-responsive hosts, the guest VLAN could allow limited access to a server from which the non-responsive host can download the supplicant software and attempt authentication again.

Related Topics

- Example: Setting Up 802.1X in Conference Rooms to Provide Internet Access to Corporate Visitors on an EX-series Switch
- Understanding Dynamic VLANs for 802.1X on EX-series Switches

