Verifying 802.1X Authentication

Purpose Verify that supplicants are being authenticated on an interface on an EX Series switch with the interface configured for 802.1X authentication, and display the method of authentication being used.

Action Display detailed information about an interface configured for 802.1X (here, the interface is ge-0/0/16):

```
user@switch> show dot1x interface ge-0/0/16.0 detail
ge-0/0/16.0
  Role: Authenticator
  Administrative state: Auto
  Supplicant mode: Single
  Number of retries: 3
  Quiet period: 60 seconds
  Transmit period: 30 seconds
  Mac Radius: Enabled
  Mac Radius Strict: Disabled
  Reauthentication: Enabled Reauthentication interval: 40 seconds
  Supplicant timeout: 30 seconds
  Server timeout: 30 seconds
  Maximum EAPOL requests: 1
  Guest VLAN member: <not configured>
  Number of connected supplicants: 1
    Supplicant: user5, 00:30:48:8C:66:BD
      Operational state: Authenticated
      Authentication method: Radius
      Authenticated VLAN: v200
     Reauthentication due in 17 seconds
```

Meaning The sample output from the show dot1x interface detail command shows that the Number of connected supplicants is 1. The supplicant that was authenticated and is now connected to the LAN is known as user5 on the RADIUS server and has the MAC address 00:30:48:8C:66:BD. The supplicant was authenticated by means of the 802.1X authentication method called Radius authentication. When the Radius authentication method is used, the supplicant is configured on the RADIUS server, the RADIUS server communicates this to the switch, and the switch opens LAN access on the interface to which the supplicant is connected. The sample output also shows that the supplicant is connected to VLAN v200.

Other 802.1X authentication methods supported on EX Series switches in addition to the RADIUS method are:

- Guest VLAN—A nonresponsive host is granted Guest-VLAN access.
- MAC Radius—A nonresponsive host is authenticated based on its MAC address. The MAC address is configured as permitted on the RADIUS server, the RADIUS server lets the switch know that the MAC address is a permitted address, and the switch opens LAN access to the nonresponsive host on the interface to which it is connected.
- Server-fail deny—If the RADIUS servers time out, all supplicants are denied access to the LAN, preventing traffic from flowing from the supplicant through the interface. This is the default.

- Server-fail permit—When the RADIUS server is unavailable, a supplicant is still permitted access to the LAN as if the supplicant had been successfully authenticated by the RADIUS server.
- Server-fail use-cache—If the RADIUS servers time out during reauthentication, previously authenticated supplicants are granted access, but new supplicants are denied LAN access.
- Server-fail VLAN—A supplicant is configured to be moved to a specified VLAN if the RADIUS server is unavailable to reauthenticate the supplicant. (The VLAN must already exist on the switch.)

Related Topics

- Configuring 802.1X Interface Settings (CLI Procedure)
- Configuring 802.1X Authentication (J-Web Procedure)
- Configuring MAC RADIUS Authentication (CLI Procedure)
- Configuring Server Fail Fallback (CLI Procedure)

Published: 2009-07-21