Configuring Server Fail Fallback (CLI Procedure)

Server fail fallback allows you to specify how 802.1X supplicants connected to the switch are supported if the RADIUS authentication server becomes unavailable or sends an Extensible Authentication Protocol Over LAN (EAPOL) Access-Reject message.

802.1X user authentication works by using an *authenticator port access entity* (the EX Series switch) to block all traffic to and from a supplicant (client) at the interface until the supplicant's credentials are presented and matched on the *authentication server* (a RADIUS server). When the supplicant has been authenticated, the switch stops blocking and opens the interface to the supplicant.

When you set up 802.1X authentication on the switch, you specify a primary authentication server and one or more backup authentication servers. If the primary authentication server cannot be reached by the switch and the secondary authentication servers are also unreachable, a RADIUS server timeout occurs. Since the authentication server grants or denies access to the supplicants awaiting authentication, the switch does not receive access instructions for supplicants attempting access to the LAN and normal 802.1X authentication cannot be completed. Server fail fallback allows you to configure authentication alternatives that permit the switch to take appropriate actions towards supplicants awaiting authentication or reauthentication.

To configure basic server fail fallback options using the CLI:

- Configure an interface to allow traffic to flow from a supplicant to the LAN if a RADIUS server timeout occurs (as if the supplicant had been successfully authenticated by a RADIUS server):

```
[edit protocols dot1x authenticator]
user@switch# set interface ge-0/0/1 server-fail permit
```

- Configure an interface to prevent traffic flow from a supplicant to the LAN (as if the supplicant had failed authentication and had been rejected by the RADIUS server):

```
[edit protocols dot1x authenticator]
user@switch# set interface ge-0/0/1 server-fail deny
```

- Configure an interface to move a supplicant to a specified VLAN if a RADIUS server timeout occurs (in this case, the VLAN name is vlan1):

```
[edit protocols dot1x authenticator]
user@switch# set interface ge-0/0/1 server-fail vlan-name vlan1
```

- Configure an interface to recognize already connected supplicants as reauthenticated if there is a RADIUS timeout during reauthentication (new users will be denied access):

```
[edit protocols dot1x authenticator]
user@switch# set interface ge-0/0/1 server-fail use-cache
```

- Configure an interface that receives an EAPOL Access-Reject message from the authentication server to move supplicants attempting LAN access on the interface to a specified VLAN already configured on the switch (in this case, the VLAN name is vlan-sf):

```
[edit protocols dot1x authenticator]
user@switch# set interface ge-0/0/1 server-reject-vlan vlan-sf
```

Related Topics

- Example: Configuring 802.1X Authentication Options When the RADIUS Server is Unavailable to an EX Series Switch
- Configuring 802.1X Authentication (J-Web Procedure)
- Configuring 802.1X Interface Settings (CLI Procedure)
- Monitoring 802.1X Authentication
- Understanding Server Fail Fallback and 802.1X Authentication on EX Series Switches

Published: 2009-07-21