8

Configuring Port-Based Access Control (802.1X)

Contents

Overview 8-3
- Why Use Port-Based Access Control? 8-3
- General Features 8-3

How 802.1X Operates 8-6
- Authenticator Operation 8-6
- Switch-Port Supplicant Operation 8-7

Terminology 8-8

General Operating Rules and Notes 8-10

General Setup Procedure for Port-Based Access Control (802.1X) 8-12
- Do These Steps Before You Configure 802.1X Operation 8-12
- Overview: Configuring 802.1X Authentication on the Switch 8-13

Configuring Switch Ports as 802.1X Authenticators 8-15
- 1. Enable 802.1X Authentication on Selected Ports 8-15
- 3. Configure the 802.1X Authentication Method 8-19
- 4. Enter the RADIUS Host IP Address(es) 8-20
- 5. Enable 802.1X Authentication on the Switch 8-20

802.1X Open VLAN Mode 8-21
- Introduction 8-21
- Use Models for 802.1X Open VLAN Modes 8-22
- Operating Rules for Authorized-Client and Unauthorized-Client VLANs 8-25
- Setting Up and Configuring 802.1X Open VLAN Mode 8-27
- 802.1X Open VLAN Operating Notes 8-31

Option For Authenticator Ports: Configure Port-Security To Allow Only 802.1X Devices 8-32

Configuring Switch Ports To Operate As Supplicants for 802.1X Connections to Other Switches 8-34

Displaying 802.1X Configuration, Statistics, and Counters 8-38

Show Commands for Port-Access Authenticator 8-38

Viewing 802.1X Open VLAN Mode Status 8-40

Show Commands for Port-Access Supplicant 8-43

How RADIUS/802.1X Authentication Affects VLAN Operation 8-44

Messages Related to 802.1X Operation 8-48

Overview

Feature	Default	Menu	CLI	Web
Configuring Switch Ports as 802.1X Authenticators	Disabled	n/a	page 8-15	n/a
Configuring 802.1X Open VLAN Mode	Disabled	n/a	page 8-21	n/a
Configuring Switch Ports to Operate as 802.1X Supplicants	Disabled	n/a	page 8-34	n/a
Displaying 802.1X Configuration, Statistics, and Counters	n/a	n/a	page 8-38	n/a
How 802.1X Affects VLAN Operation	n/a	n/a	page 8-44	n/a
RADIUS Authentication and Accounting	Refer to "RADIUS Authentication and Accounting" on page 5-1			

Why Use Port-Based Access Control?

Local area networks are often deployed in a way that allows unauthorized clients to attach to network devices, or allows unauthorized users to get access to unattended clients on a network. Also, the use of DHCP services and zero configuration make access to networking services easily available. This exposes the network to unauthorized use and malicious attacks. While access to the network should be made easy, uncontrolled and unauthorized access is usually not desirable. 802.1X provides access control along with the ability to control user profiles from a central RADIUS server while allowing users access from multiple points within the network.

General Features

802.1X on the ProCurve switches covered in this manual includes the following:

- Switch operation as both an authenticator (for supplicants having a point-to-point connection to the switch) and as a supplicant for point-to-point connections to other 802.1X-aware switches.
  - Authentication of 802.1X clients using a RADIUS server and either the EAP or CHAP protocol.
  - Provision for enabling clients that do not have 802.1 supplicant software to use the switch as a path for downloading the software and initiating the authentication process (802.1X Open VLAN mode).
  - Supplicant implementation using CHAP authentication and independent username and password configuration on each port.
- Prevention of traffic flow in either direction on unauthorized ports.

- Local authentication of 802.1X clients using the switch's local username and password (as an alternative to RADIUS authentication).
- Temporary on-demand change of a port's VLAN membership status to support a current client's session. (This does not include ports that are members of a trunk.)
- Session accounting with a RADIUS server, including the accounting update interval.
- Use of Show commands to display session counters.
- With port-security enabled for port-access control, limit a port to one 802.1X client session at a given time.

Authenticating Users. Port-Based Access Control (802.1X) provides switch-level security that allows LAN access only to users who enter the authorized RADIUS username and password on 802.1X-capable clients (supplicants). This simplifies security management by allowing you to control access from a master database in a single server (although you can use up to three RADIUS servers to provide backups in case access to the primary server fails). It also means a user can enter the same username and password pair for authentication, regardless of which switch is the access point into the LAN. Note that you can also configure 802.1X for authentication through the switch's local username and password instead of a RADIUS server, but doing so increases the administrative burden, decentralizes username/password administration, and reduces security by limiting authentication to one Operator/Manager password set for all users.

Providing a Path for Downloading 802.1X Supplicant Software. For clients that do not have the necessary 802.1X supplicant software, there is also the option to configure the 802.1X Open VLAN mode. This mode allows you to assign such clients to an isolated VLAN through which you can provide the necessary supplicant software these clients need to begin the authentication process. (Refer to "802.1X Open VLAN Mode" on page 8-21.)

Authenticating One Switch to Another. 802.1X authentication also enables the switch to operate as a supplicant when connected to a port on another switch running 802.1X authentication.

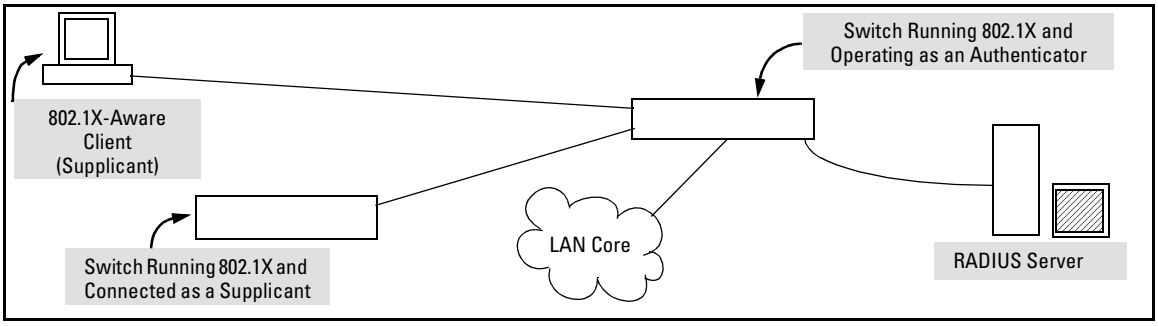

Figure 8-1. Example of an 802.1X Application

Accounting . The switch also provides RADIUS Network accounting for 802.1X access. Refer to "RADIUS Authentication and Accounting" on page 5-1.

How 802.1X Operates

Authenticator Operation

This operation provides security on a direct, point-to-point link between a single client and the switch, where both devices are 802.1X-aware. (If you expect desirable clients that do not have the necessary 802.1X supplicant software, you can provide a path for downloading such software by using the 802.1X Open VLAN mode—refer to "802.1X Open VLAN Mode" on page 8-21.) For example, suppose that you have configured a port on the switch for 802.1X authentication operation. If you then connect an 802.1X-aware client (supplicant) to the port and attempt to log on:

1. When the switch detects the client on the port, it blocks access to the LAN from that port.
2. The switch responds with an identity request.
3. The client responds with a user name that uniquely defines this request for the client.
4. The switch responds in one of the following ways:
   - If 802.1X (port-access) on the switch is configured for RADIUS authentication, the switch then forwards the request to a RADIUS server.
     i. The server responds with an access challenge which the switch forwards to the client.
     ii. The client then provides identifying credentials (such as a user certificate), which the switch forwards to the RADIUS server.
     iii. The RADIUS server then checks the credentials provided by the client.
     iv. If the client is successfully authenticated and authorized to connect to the network, then the server notifies the switch to allow access to the client. Otherwise, access is denied and the port remains blocked.
   - If 802.1X (port-access) on the switch is configured for local authentication, then:
     i. The switch compares the client's credentials with the username and password configured in the switch (Operator or Manager level).
     ii. If the client is successfully authenticated and authorized to connect to the network, then the switch allows access to the client. Otherwise, access is denied and the port remains blocked.

Switch-Port Supplicant Operation

This operation provides security on links between 802.1X-aware switches. For example, suppose that you want to connect two switches, where:

- Switch “A” has port A1 configured for 802.1X supplicant operation.
- You want to connect port A1 on switch “A” to port B5 on switch “B”.

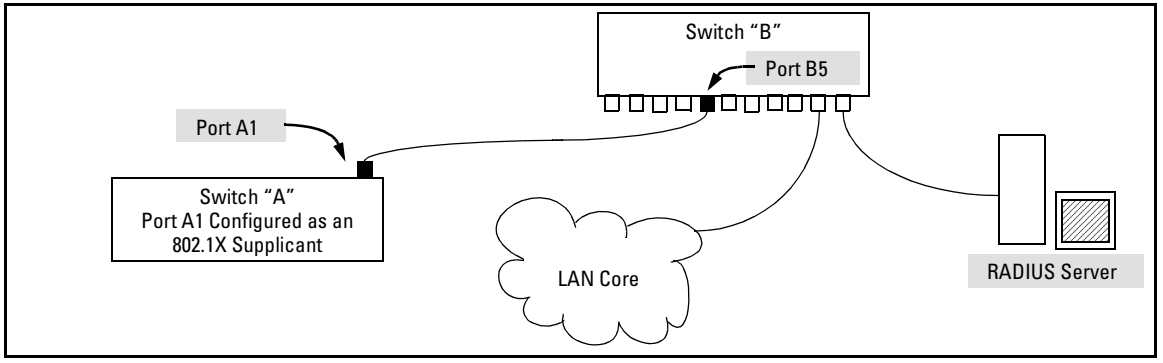

Figure 8-2. Example of Supplicant Operation

1. When port A1 on switch “A” is first connected to a port on switch “B”, or if the ports are already connected and either switch reboots, port A1 begins sending start packets to port B5 on switch “B”.
   - If, after the supplicant port sends the configured number of start packets, it does not receive a response, it assumes that switch “B” is not 802.1X-aware, and transitions to the authenticated state. If switch “B” is operating properly and is not 802.1X-aware, then the link should begin functioning normally, but without 802.1X security.
   - If, after sending one or more start packets, port A1 receives a request packet from port B5, then switch “B” is operating as an 802.1X authenticator. The supplicant port then sends a response/ID packet. Switch “B” forwards this request to a RADIUS server.
2. The RADIUS server then responds with an MD5 access challenge that switch “B” forwards to port A1 on switch “A”.
3. Port A1 replies with an MD5 hash response based on its username and password or other unique credentials. Switch “B” forwards this response to the RADIUS server.
4. The RADIUS server then analyzes the response and sends either a “success” or “failure” packet back through switch “B” to port A1.
   - A “success” response unblocks port B5 to normal traffic from port A1.

- A “failure” response continues the block on port B5 and causes port A1 to wait for the “held-time” period before trying again to achieve authentication through port B5.

Note You can configure a switch port to operate as both a supplicant and an authenticator at the same time.

Terminology

802.1X-Aware: Refers to a device that is running either 802.1X authenticator software or 802.1X client software and is capable of interacting with other devices on the basis of the IEEE 802.1X standard.

Authorized-Client VLAN: Like the Unauthorized-Client VLAN, this is a conventional, static VLAN previously configured on the switch by the System Administrator. The intent in using this VLAN is to provide authenticated clients with network services that are not available on either the port’s statically configured VLAN memberships or any VLAN memberships that may be assigned during the RADIUS authentication process. While an 802.1X port is a member of this VLAN, the port is untagged. When the client connection terminates, the port drops its membership in this VLAN.

Authentication Server: The entity providing an authentication service to the switch when the switch is configured to operate as an authenticator. In the case of an ProCurve switch running 802.1X, this is a RADIUS server (unless local authentication is used, in which case the switch performs this function using its own username and password for authenticating a supplicant).

Authenticator: In ProCurve switch applications, a device such as a switch that requires a supplicant to provide the proper credentials (username and password) before being allowed access to the network.

CHAP (MD5): Challenge Handshake Authentication Protocol.

Client: In this application, an end-node device such as a management station, workstation, or mobile PC linked to the switch through a point-to-point LAN link.

EAP (Extensible Authentication Protocol)**:** EAP enables network access that supports multiple authentication methods.

EAPOL: Extensible Authentication Protocol Over LAN, as defined in the 802.1X standard.

Friendly Client: A client that does not pose a security risk if given access to the switch and your network.

MD5: An algorithm for calculating a unique digital signature over a stream of bytes. It is used by CHAP to perform authentication without revealing the shared secret (password).

PVID (Port VID): This is the VLAN ID for the untagged VLAN to which an 802.1X port belongs.

Static VLAN: A VLAN that has been configured as "permanent" on the switch by using the CLI **vlan < *vid* >** command or the Menu interface.

Supplicant: The entity that must provide the proper credentials to the switch before receiving access to the network. This is usually an end-user workstation, but it can be a switch, router, or another device seeking network services.

Tagged VLAN Membership: This type of VLAN membership allows a port to be a member of multiple VLANs simultaneously. If a client connected to the port has an operating system that supports 802.1q VLAN tagging, then the client can access VLANs for which the port is a tagged member. If the client does not support VLAN tagging, then it can access only a VLAN for which the port is an untagged member. (A port can be an untagged member of only one VLAN at a time.) 802.1X Open VLAN mode does not affect a port's tagged VLAN access unless the port is statically configured as a member of a VLAN that is also configured as the Unauthorized-Client or Authorized-Client VLAN. See also "**Untagged VLAN Membership**".

Unauthorized-Client VLAN: A conventional, static VLAN previously configured on the switch by the System Administrator. It is used to provide access to a client prior to authentication. It should be set up to allow an unauthenticated client to access only the initialization services necessary to establish an authenticated connection, plus any other desirable services whose use by an unauthenticated client poses no security threat to your network. (Note that an unauthenticated client has access to all network resources that have membership in the VLAN you designate as the Unauthorized-Client VLAN.) A port configured to use a given Unauthorized-Client VLAN does not have to be statically configured as a

member of that VLAN as long as at least one other port on the switch is statically configured as a tagged or untagged member of the same Unauthorized-Client VLAN.

Untagged VLAN Membership: A port can be an untagged member of only one VLAN. (In the factory-default configuration, all ports on the switch are untagged members of the default VLAN.) An untagged VLAN membership is *required* for a client that does not support 802.1q VLAN tagging. A port can simultaneously have one untagged VLAN membership and multiple tagged VLAN memberships. Depending on how you configure 802.1X Open VLAN mode for a port, a statically configured, untagged VLAN membership may become unavailable while there is a client session on the port. See also "**Tagged VLAN Membership**".

General Operating Rules and Notes

- When a port on the switch is configured as either an authenticator or supplicant and is connected to another device, rebooting the switch causes a re-authentication of the link.
- When a port on the switch is configured as an authenticator, it will block access to a client that either does not provide the proper authentication credentials or is not 802.1X-aware. (You can use the optional 802.1X Open VLAN mode to open a path for downloading 802.1X supplicant software to a client, which enables the client to initiate the authentication procedure. Refer to "802.1X Open VLAN Mode" on page 8-21.)
- If a port on switch "A" is configured as an 802.1X supplicant and is connected to a port on another switch, "B", that is not 802.1X-aware, access to switch "B" will occur without 802.1X security protection.
- You can configure a port as both an 802.1X authenticator *and* an 802.1X supplicant.
- If a port on switch "A" is configured as both an 802.1X authenticator *and* supplicant and is connected to a port on another switch, "B", that is not 802.1X-aware, access to switch "B" will occur without 802.1X security protection, but switch "B" will not be allowed access to switch "A". This means that traffic on this link between the two switches will flow from "A" to "B", but not the reverse.

- If a client already has access to a switch port when you configure the port for 802.1X authenticator operation, the port will block the client from further network access until it can be authenticated.
- On a port configured for 802.1X with RADIUS authentication, if the RADIUS server specifies a VLAN for the supplicant and the port is a trunk member, the port will be blocked. If the port is later removed from the trunk, the port will try to authenticate the supplicant. If authentication is successful, the port becomes unblocked. Similarly, if the supplicant is authenticated and later the port becomes a trunk member, the port will be blocked. If the port is then removed from the trunk, it tries to re-authenticate the supplicant. If successful, the port becomes unblocked.
- To help maintain security, 802.1X and LACP cannot both be enabled on the same port. If you try to configure 802.1X on a port already configured for LACP (or the reverse) you will see a message similar to the following:

  Error configuring port *X*: LACP and 802.1X cannot be run together.

Note on 802.1X and LACP

To help maintain security, the switch does not allow 802.1X and LACP to both be enabled at the same time on the same port. Refer to “802.1X Operating Messages” on page 8-48

General Setup Procedure for Port-Based Access Control (802.1X)

Do These Steps Before You Configure 802.1X Operation

1. Configure a local username and password on the switch for both the Operator (login) and Manager (enable) access levels. (While this may or may not be required for your 802.1X configuration, ProCurve recommends that you use a local username and password pair at least until your other security measures are in place.)
2. Determine which ports on the switch you want to operate as authenticators and/or supplicants, and disable LACP on these ports. (See the "Note on 802.1X and LACP" on page 8-11.)
3. Determine whether to use the optional 802.1X Open VLAN mode for clients that are not 802.1X-aware; that is, for clients that are not running 802.1X supplicant software. (This will require you to provide downloadable software that the client can use to enable an authentication session.) For more on this topic, refer to "802.1X Open VLAN Mode" on page 8-21.
4. For each port you want to operate as a supplicant, determine a username and password pair. You can either use the same pair for each port or use unique pairs for individual ports or subgroups of ports. (This can also be the same local username/password pair that you assign to the switch.)
5. Unless you are using only the switch's local username and password for 802.1X authentication, configure at least one RADIUS server to authenticate access requests coming through the ports on the switch from external supplicants (including switch ports operating as 802.1X supplicants). You can use up to three RADIUS servers for authentication; one primary and two backups. Refer to the documentation provided with your RADIUS application.

Overview: Configuring 802.1X Authentication on the Switch

This section outlines the steps for configuring 802.1X on the switch. For detailed information on each step, refer to "RADIUS Authentication and Accounting" on page 5-1 or "Configuring Switch Ports To Operate As Supplicants for 802.1X Connections to Other Switches" on page 8-34.

1. Enable 802.1X authentication on the individual ports you want to serve as authenticators. On the ports you will use as authenticators, either accept the default 802.1X settings or change them, as necessary. Note that, by default, the port-control parameter is set to **auto** for all ports on the switch. This requires a client to support 802.1X authentication and to provide valid credentials to get network access. Refer to page 8-15.
2. If you want to provide a path for clients without 802.1X supplicant software to download the software so that they can initiate an authentication session, enable the 802.1X Open VLAN mode on the ports you want to support this feature. Refer to page 8-21.
3. Configure the 802.1X authentication type. Options include:
   - Local Operator username and password (the default). This option allows a client to use the switch's local username and password as valid 802.1X credentials for network access.
   - EAP RADIUS: This option requires your RADIUS server application to support EAP authentication for 802.1X.
   - CHAP (MD5) RADIUS: This option requires your RADIUS server application to support CHAP (MD5) authentication.

   See page 8-19.
4. If you select either **eap-radius** or **chap-radius** for step 3, use the **radius host** command to configure up to three RADIUS server IP address(es) on the switch. See page 8-20.
5. Enable 802.1X authentication on the switch. See page 8-15.
6. Test both the authorized and unauthorized access to your system to ensure that the 802.1X authentication works properly on the ports you have configured for port-access.

Note

If you want to implement the optional port security feature (step 7) on the switch, you should first ensure that the ports you have configured as 802.1X authenticators operate as expected.

7. If you are using Port Security on the switch, configure the switch to allow only 802.1X access on ports configured for 802.1X operation, and (if desired) the action to take if an unauthorized device attempts access through an 802.1X port. See page 8-32.
8. If you want a port on the switch to operate as a supplicant in a connection with a port operating as an 802.1X authenticator on another device, then configure the supplicant operation. (Refer to "Configuring Switch Ports To Operate As Supplicants for 802.1X Connections to Other Switches" on page 8-34.)

Configuring Switch Ports as 802.1X Authenticators

802.1X Authentication Commands	Page
[no] aaa port-access authenticator < [ethernet] < *port-list* >	8-15
[control | quiet-period | tx-period | supplicant-timeout | server-timeout | max-requests | reauth-period | auth-vid | unauth-vid | initialize | reauthenticate | clear-statistics]	8-15
aaa authentication port-access	8-19
< local | eap-radius | chap-radius >	
[no] aaa port-access authenticator active	8-15
[no] port-security [ethernet] < *port-list* > learn-mode port-access	8-32
802.1X Open VLAN Mode Commands	8-21
802.1X Supplicant Commands	8-34
802.1X-Related Show Commands	8-38
RADIUS server configuration	8-20

1. Enable 802.1X Authentication on Selected Ports

This task configures the individual ports you want to operate as 802.1X authenticators for point-to-point links to 802.1X-aware clients or switches. (Actual 802.1X operation does not commence until you perform step 5 on page 8-13 to activate 802.1X authentication on the switch.)

Note

When you enable 802.1X authentication on a port, the switch automatically disables LACP on that port. However, if the port is already operating in an LACP trunk, you must remove the port from the trunk before you can configure it for 802.1X authentication.

Syntax: aaa port-access authenticator < *port-list* >

Enables specified ports to operate as 802.1X authenticators with current per- port authenticator configuration. To activate configured 802.1X operation, you must enable 802.1X authentication. Refer to "5. Enable 802.1X Authentication on the switch" on page 8-13.

[control < authorized | auto | unauthorized >]

Controls authentication mode on the specified port:

authorized: *Also termed* Force Authorized. *Grants access to any device connected to the port. In this case, the device does not have to provide 802.1X credentials or support 802.1X authentication. (However, you can still configure console, Telnet, or SSH security on the port.)*

auto *(the default): The device connected to the port must support 802.1X authentication and provide valid credentials in order to get network access. (You have the option of using the Open VLAN mode to provide a path for clients without 802.1X supplicant software to download this software and begin the authentication process. Refer to "802.1X Open VLAN Mode" on page 8-21.)*

unauthorized: *Also termed* Force Unauthorized. *Do not grant access to the network, regardless of whether the device provides the correct credentials and has 802.1X support. In this state, the port blocks access to any connected device.*

[quiet-period < 0 - 65535 >]

Sets the period during which the port does not try to acquire a supplicant. The period begins after the last attempt authorized by the **max-requests** *parameter fails (next page). (Default: 60 seconds)*

[tx-period < 0 - 65535 >]

Sets the period the port waits to retransmit the next EAPOL PDU during an authentication session. (Default: 30 seconds)

[supplicant-timeout < 1 - 300 >]

Sets the period of time the switch waits for a supplicant response to an EAP re quest. If the supplicant does not respond within the configured time frame, the session times out. (Default: 30 seconds)

aaa port-access authenticator < *port-list* > ***(Syntax Continued)***

[server-timeout < 1 - 300 >]

Sets the period of time the switch waits for a server response to an authentication request. If there is no response within the configured time frame, the switch assumes that the authentication attempt has timed out. Depending on the current **max-requests** *setting, the switch will either send a new request to the server or end the authentication session. (Default: 30 seconds)*

[max-requests < 1 - 10 >]

Sets the number of authentication attempts that must time-out before authentication fails and the authentication session ends. If you are using the Local authentication option, or are using RADIUS authentication with only one host server, the switch will not start another session until a client tries a new access attempt. If you are using RADIUS authentication with two or three host servers, the switch will open a session with each server, in turn, until authentication occurs or there are no more servers to try. During the **quiet-period** *(previous page), if any, you cannot reconfigure this parameter. (Default: 2)*

[reauth-period < 1 - 9999999 >]

Sets the period of time after which clients connected must be re-authenticated. When the timeout is set to 0 the reauthentication is disabled (Default: 0 second)

[unauth-vid < *vlan-id* >]

Configures an existing static VLAN to be the Unauthorized-Client VLAN. This enables you to provide a path for clients without supplicant software to download the software and begin an authentication session. Refer to "802.1X Open VLAN Mode" on page 8-21.

[auth-vid < *vid* >

Configures an existing, static VLAN to be the Authorized-Client VLAN. Refer to "802.1X Open VLAN Mode" on page 8-21.

aaa port-access authenticator < *port-list* > ***(Syntax Continued)***

[initialize]

On the specified ports, blocks inbound and outbound traffic and restarts the 802.1X authentication process. This happens only on ports configured with ***control auto*** *and actively operating as 802.1X authenticators.*
Note: *If a specified port is configured with* ***control authorized*** *and* ***port-security****, and the port has learned an authorized address, the port will remove this address and learn a new one from the first packet it receives.*

[reauthenticate]

Forces reauthentication (unless the authenticator is in 'HELD' state).

[clear-statistics]

Clears authenticator statistics counters.

3. Configure the 802.1X Authentication Method

This task specifies how the switch will authenticate the credentials provided by a supplicant connected to a switch port configured as an 802.1X authenticator.

Syntax: aaa authentication port-access < local | eap-radius | chap-radius >

Determines the type of RADIUS authentication to use.

local *Use the switch's local username and password for supplicant authentication.*

eap-radius *Use EAP-RADIUS authentication. (Refer to the documentation for your RADIUS server.)*

chap-radius *Use CHAP-RADIUS (MD-5) authentication. (Refer to the documentation for your RADIUS server application.)*

For example, to enable the switch to perform 802.1X authentication using one or more EAP-capable RADIUS servers:

```
ProCurve(config)# aaa authentication port-access eap-radius
ProCurve(config)# show auth

 Status and Counters - Authentication Information

  Login Attempts : 3

             | Login      Login      Enable     Enable
  Access Task | Primary    Secondary  Primary    Secondary
  ----------- + ---------- ---------- ---------- ----------
  Console     | Local      None       Local      None
  Telnet      | Local      None       Local      None
  Port-Access | EapRadius
  SSH         | Local      None       Local      None
```

Configuration command for EAP-RADIUS authentication.

802.1X (Port-Access) configured for EAP-RADIUS authentication.

Figure 8-3. Example of 802.1X (Port-Access) Authentication

4. Enter the RADIUS Host IP Address(es)

If you selected either **eap-radius** or **chap-radius** for the authentication method, configure the switch to use 1 to 3 RADIUS servers for authentication. The following syntax shows the basic commands. For coverage of all commands related to RADIUS server configuration, refer to "RADIUS Authentication and Accounting" on page 5-1.

Syntax: radius host < *ip-address* >

Adds a server to the RADIUS configuration.

[key < *server-specific key-string* >]

Optional. Specifies an encryption key for use during authentication (or accounting) sessions with the specified server. This key must match the key used on the RADIUS server. Use this option only if the specified server requires a different key than configured for the global encryption key.

radius-server key < *global key-string* >

Specifies the global encryption key the switch uses for sessions with servers for which the switch does not have a server-specific key. This key is optional if all RADIUS server addresses configured in the switch include a server- specific encryption key.

5. Enable 802.1X Authentication on the Switch

After configuring 802.1X authentication as described in the preceding four sections, activate it with this command:

Syntax: aaa port-access authenticator active

Activates 802.1X port-access on ports you have configured as authenticators.

802.1X Open VLAN Mode

802.1X Authentication Commands	page 8-15
802.1X Supplicant Commands	page 8-35
802.1X Open VLAN Mode Commands	
[no] aaa port-access authenticator [e] < *port-list* >	page 8-30
[auth-vid < *vlan-id* >]	
[unauth-vid < *vlan-id* >]	
802.1X-Related Show Commands	page 8-38
RADIUS server configuration	pages 8-20

This section describes how to use the 802.1X Open VLAN mode to configure unauthorized-client and authorized-client VLANs on ports configured as 802.1X authenticators.

Introduction

Configuring the 802.1X Open VLAN mode on a port changes how the port responds when it detects a new client. In earlier releases, a “friendly” client computer not running 802.1X supplicant software could not be authenticated on a port protected by 802.1X access security. As a result, the port would become blocked and the client could not access the network. This prevented the client from:

- Acquiring IP addressing from a DHCP server
- Downloading the 802.1X supplicant software necessary for an authentication session

The 802.1X Open VLAN mode solves this problem by temporarily suspending the port’s static, tagged and untagged VLAN memberships and placing the port in a designated *Unauthorized-Client VLAN*. In this state the client can proceed with initialization services, such as acquiring IP addressing and 802.1X software, and starting the authentication process. Following client authentication, the port drops its temporary (untagged) membership in the Unauthorized-Client VLAN and joins (or rejoins) *one* of the following as an *untagged* member:

1. **1st Priority:** The port joins a VLAN to which it has been assigned by a RADIUS server during authentication.
2. **2nd Priority:** If RADIUS authentication does not include assigning the port to a VLAN, then the switch assigns the port to the VLAN entered in the port's 802.1X configuration as an *Authorized-Client* VLAN, if configured.
3. **3rd Priority:** If the port does not have an Authorized-Client VLAN configured, but does have a static, untagged VLAN membership in its configuration, then the switch assigns the port to this VLAN.

If the port is not configured for any of the above, then it must be a tagged member of at least one static VLAN. If the client is capable of operating with that tagged VLAN, then it receives access to the VLAN. Otherwise, the connection fails.

Note

After client authentication, the port resumes membership in any tagged VLANs for which it is configured. If the port belongs to a tagged VLAN used for 1 or 2 above, then it operates as an untagged member of that VLAN while the client is connected. When the client disconnects, the port reverts to tagged membership in the VLAN.

Use Models for 802.1X Open VLAN Modes

You can apply the 802.1X Open VLAN mode in more than one way. Depending on your use, you will need to create one or two static VLANs on the switch for *exclusive* use by per-port 802.1X Open VLAN mode authentication:

- **Unauthorized-Client VLAN:** Configure this VLAN when unauthenticated, friendly clients will need access to some services before being authenticated.
- **Authorized-Client VLAN:** Configure this VLAN for authenticated clients when the port is not statically configured as an untagged member of a VLAN you want clients to use, or when the port is statically configured as an untagged member of a VLAN you do not want clients to use. (A port can be configured as untagged on only one VLAN. When an Authorized-Client VLAN is configured, it will always be untagged and will block the port from using a statically configured, untagged membership in another VLAN.) Note that after client authentication, the port returns to membership in any tagged VLANs for which you have configured it. See the "Note", above.

Table 8-1. 802.1X Open VLAN Mode Options

802.1X Per-Port Configuration	Port Response
No Open VLAN mode:	The port automatically blocks a client that cannot initiate an authentication session.
Open VLAN mode with **both** of the following configured:	
Unauthorized-Client VLAN	• When the port detects a client, it automatically becomes an untagged member of this VLAN. If you previously configured the port as a static, tagged member of the VLAN, membership temporarily changes to untagged while the client remains unauthenticated. • If the port already has a statically configured, untagged membership in another VLAN, then the port temporarily closes access to this other VLAN while in the Unauthorized-Client VLAN. • To limit security risks, the network services and access available on the Unauthorized-Client VLAN should include only what a client needs to enable an authentication session. If the port is statically configured as a tagged member of any other VLANs, access to these VLANs is blocked while the port is a member of the Unauthorized-Client VLAN.
Authorized-Client VLAN	• After the client is authenticated, the port drops membership in the Unauthorized-Client VLAN and becomes an untagged member of this VLAN. **Note:** if RADIUS authentication assigns a VLAN, the port temporarily becomes a member of the RADIUS-assigned VLAN — instead of the Authorized-Client VLAN—while the client is connected. • If the port is statically configured as a tagged member of a VLAN, and this VLAN is used as the Authorized-Client VLAN, then the port temporarily becomes an untagged member of this VLAN when the client becomes authenticated. When the client disconnects, the port returns to tagged membership in this VLAN. • If the port is statically configured as a tagged member of a VLAN that is not used by 802.1X Open VLAN mode, the port returns to tagged membership in this VLAN upon successful authentication. This happens even if the RADIUS server assigns the port to another, authorized VLAN. If the port is already configured as a tagged member of a VLAN that RADIUS assigns as an authorized VLAN, then the port becomes an untagged member of that VLAN for the duration of the client connection. After the client disconnects, the port returns to tagged membership in that VLAN.

802.1X Per-Port Configuration	Port Response
Open VLAN Mode with **Only** an **Unauthorized-Client VLAN** Configured:	
	• When the port detects a client, it automatically becomes an untagged member of this VLAN. To limit security risks, the network services and access available on this VLAN should include only what a client needs to enable an authentication session. If the port is statically configured as an untagged member of another VLAN, the switch temporarily removes the port from membership in this other VLAN while membership in the Unauthorized-Client VLAN exists. • After the client is authenticated, and if the port is statically configured as an untagged member of another VLAN, the port's access to this other VLAN is restored. **Note:** If RADIUS authentication assigns a VLAN to the port, this assignment overrides any statically configured, untagged VLAN membership on the port (while the client is connected). • If the port is statically configured as a tagged member of a VLAN that is not used by 802.1X Open VLAN mode, the port returns to tagged membership in this VLAN upon successful client authentication. This happens even if the RADIUS server assigns the port to another, authorized VLAN. Note that if the port is already configured as a tagged member of a VLAN that RADIUS assigns as an authorized VLAN, then the port becomes an untagged member of that VLAN for the duration of the client connection. After the client disconnects, the port returns to tagged membership in that VLAN.
Open VLAN Mode with **Only** an **Authorized-Client VLAN** Configured:	
	• Port automatically blocks a client that cannot initiate an authentication session. • If the client successfully completes an authentication session, the port becomes an untagged member of this VLAN. **Note:** if RADIUS authentication assigns a VLAN, the port temporarily becomes an untagged member of the RADIUS-assigned VLAN —instead of the Authorized-Client VLAN—while the client is connected. • If the port is statically configured as a tagged member of any other VLAN, the port returns to tagged membership in this VLAN upon successful client authentication. This happens even if the RADIUS server assigns the port to another, authorized VLAN. If the port is already configured as a tagged member of a VLAN that RADIUS assigns as an authorized VLAN, then the port becomes an untagged member of that VLAN for the duration of the client connection. After the client disconnects, the port returns to tagged membership in that VLAN.

Operating Rules for Authorized-Client and Unauthorized-Client VLANs

Condition	Rule
Static VLANs used as *Authorized-Client* or *Unauthorized-Client* VLANs	These must be configured on the switch before you configure an 802.1X authenticator port to use them. (Use the **vlan < *vlan-id* >** command or the VLAN Menu screen in the Menu interface.)
VLAN Assignment Received from a RADIUS Server	If the RADIUS server specifies a VLAN for an authenticated supplicant connected to an 802.1X authenticator port, this VLAN assignment overrides any Authorized-Client VLAN assignment configured on the authenticator port. This is because both VLANs are untagged, and the switch allows only one untagged VLAN membership per-port. For example, suppose you configured port A4 to place authenticated supplicants in VLAN 20. If a RADIUS server authenticates supplicant "A" and assigns this supplicant to VLAN 50, then the port can access VLAN 50 as an untagged member while the client session is running. When the client disconnects from the port, then the port drops these assignments and uses the untagged VLAN memberships for which it is statically configured. (After client authentication, the port resumes any tagged VLAN memberships for which it is already configured. For details, refer to the Note on page 8-22.)
Temporary VLAN Membership During a Client Session	• Port membership in a VLAN assigned to operate as the Unauthorized-Client VLAN is temporary, and ends when the client receives authentication or the client disconnects from the port, whichever is first. • Port membership in a VLAN assigned to operate as the Authorized-Client VLAN is also temporary, and ends when the client disconnects from the port.If a VLAN assignment from a RADIUS server is used instead, the same rule applies.
Effect of Unauthorized-Client VLAN session on untagged port VLAN membership	• When an unauthenticated client connects to a port that is already configured with a static, untagged VLAN, the switch temporarily moves the port to the Unauthorized-Client VLAN (also untagged). (While the Unauthorized-Client VLAN is in use, the port does not access the static, untagged VLAN.) • When the client either becomes authenticated or disconnects, the port leaves the Unauthorized-Client VLAN and reacquires its untagged membership in the statically configured VLAN.

Condition	Rule
Effect of Authorized-Client VLAN session on untagged port VLAN membership.	• When a client becomes authenticated on a port that is already configured with a static, untagged VLAN, the switch temporarily moves the port to the Authorized-Client VLAN (also untagged). While the Authorized-Client VLAN is in use, the port does not have access to the statically configured, untagged VLAN. • When the authenticated client disconnects, the switch removes the port from the Authorized-Client VLAN and moves it back to the untagged membership in the statically configured VLAN. (After client authentication, the port resumes any tagged VLAN memberships for which it is already configured. For details, refer to the Note on page 8-22.)
Multiple Authenticator Ports Using the Same Unauthorized-Client and Authorized-Client VLANs	You can use the same static VLAN as the Unauthorized-Client VLAN for all 802.1X authenticator ports configured on the switch. Similarly, you can use the same static VLAN as the Authorized-Client VLAN for all 802.1X authenticator ports configured on the switch. ***Caution:*** *Do not use the same static VLAN for both the unauthorized and the Authorized-Client VLAN. Using one VLAN for both creates a security risk by defeating the isolation of unauthenticated clients.*
Effect of Failed Client Authentication Attempt	When there is an Unauthorized-Client VLAN configured on an 802.1X authenticator port, an unauthorized client connected to the port has access only to the network resources belonging to the Unauthorized-Client VLAN. This access continues until the client disconnects from the port. (If there is no Unauthorized-Client VLAN configured on the authenticator port, the port simply blocks access for any unauthorized client that cannot be authenticated.)
IP Addressing for a Client Connected to a Port Configured for 802.x Open VLAN Mode	A client can either acquire an IP address from a DHCP server or have a preconfigured, manual IP address before connecting to the switch.
802.1X Supplicant Software for a Client Connected to a Port Configured for 802.1X Open VLAN Mode	A friendly client, without 802.1X supplicant software, connecting to an authenticator port must be able to download this software from the Unauthorized-Client VLAN before authentication can begin.

Note: If you use the same VLAN as the Unauthorized-Client VLAN for all authenticator ports, unauthenticated clients on different ports can communicate with each other. However, in this case, you can improve security between authenticator ports by using the switch's Source-Port filter feature. For example, if you are using ports B1 and B2 as authenticator ports on the same Unauthorized-Client VLAN, you can configure a Source-Port filter on B1 to drop all packets from B2 and the reverse.

Setting Up and Configuring 802.1X Open VLAN Mode

Preparation. This section assumes use of both the Unauthorized-Client and Authorized-Client VLANs. Refer to Table 8-1 on page 8-23 for other options.

Before you configure the 802.1X Open VLAN mode on a port:

- Statically configure an "Unauthorized-Client VLAN" in the switch. The only ports that should belong to this VLAN are ports offering services and access you want available to unauthenticated clients. (802.1X authenticator ports do not have to be members of this VLAN.)

Caution

Do not allow any port memberships or network services on this VLAN that would pose a security risk if exposed to an unauthorized client.

- Statically configure an Authorized-Client VLAN in the switch. The only ports that should belong to this VLAN are ports offering services and access you want available to authenticated clients. 802.1X authenticator ports do not have to be members of this VLAN.

  Note that if an 802.1X authenticator port is an untagged member of another VLAN, the port's access to that other VLAN will be temporarily removed while an authenticated client is connected to the port. For example, if:

  i. Port A5 is an untagged member of VLAN 1 (the default VLAN).
  ii. You configure port A5 as an 802.1X authenticator port.
  iii. You configure port A5 to use an Authorized-Client VLAN.

  Then, if a client connects to port A5 and is authenticated, port A5 becomes an untagged member of the Authorized-Client VLAN and is temporarily suspended from membership in the default VLAN.

- If you expect friendly clients to connect without having 802.1X supplicant software running, provide a server on the Unauthorized-Client VLAN for downloading 802.1X supplicant software to the client, and a procedure by which the client initiates the download.

- A client must either have a valid IP address configured before connecting to the switch, or download one through the Unauthorized-Client VLAN from a DHCP server. In the latter case, you will need to provide DHCP services on the Unauthorized-Client VLAN.

- Ensure that the switch is connected to a RADIUS server configured to support authentication requests from clients using ports configured as 802.1X authenticators. (The RADIUS server should not be on the Unauthorized-Client VLAN.)

  Note that as an alternative, you can configure the switch to use local password authentication instead of RADIUS authentication. However, this is less desirable because it means that all clients use the same passwords and have the same access privileges. Also, you must use 802.1X supplicant software that supports the use of local switch passwords.

Caution

Ensure that you do not introduce a security risk by allowing Unauthorized-Client VLAN access to network services or resources that could be compromised by an unauthorized client.

Configuring General 802.1X Operation: These steps enable 802.1X authentication, and must be done before configuring 802.1X VLAN operation.

1. Enable 802.1X authentication on the individual ports you want to serve as authenticators. (The switch automatically disables LACP on the ports on which you enable 802.1X.) On the ports you will use as authenticators with VLAN operation, ensure that the (default) port-control parameter is set to **auto**. (Refer to "1. Enable 802.1X Authentication on Selected Ports" on page 8-15.) This setting requires a client to support 802.1X authentication (with 802.1X supplicant operation) and to provide valid credentials to get network access.

   Syntax: aaa port-access authenticator e < *port-list* > control auto

   Activates 802.1X port-access on ports you have configured as authenticators.

2. Configure the 802.1X authentication type. Options include:

   Syntax: aaa authentication port-access < local | eap-radius | chap-radius >

   Determines the type of RADIUS authentication to use.

   local: *Use the switch's local username and password for supplicant authentication (the default).*

   eap-radius*Use EAP-RADIUS authentication. (Refer to the documentation for your RADIUS server.*

   chap-radius*Use CHAP-RADIUS (MD5) authentication. (Refer to the documentation for your RADIUS server software.)*

3. If you selected either **eap-radius** or **chap-radius** for step 2, use the **radius host** command to configure up to three RADIUS server IP address(es) on the switch.

Syntax: radius host < *ip-address* >

Adds a server to the RADIUS configuration.

[key < *server-specific key-string* >]

Optional. Specifies an encryption key for use with the specified server. This key must match the key used on the RADIUS server. Use this option only if the specified server requires a different key than configured for the global encryption key.

radius-server key < *global key-string* >

Specifies the global encryption key the switch uses for sessions with servers for which the switch does not have a server-specific key. This key is optional if all RADIUS server addresses configured in the switch include a server- specific encryption key.

4. Activate authentication on the switch.

Syntax: aaa port-access authenticator active

Activates 802.1X port-access on ports you have configured as authenticators.

5. Test both the authorized and unauthorized access to your system to ensure that the 802.1X authentication works properly on the ports you have configured for port-access.

Note

If you want to implement the optional port security feature on the switch, you should first ensure that the ports you have configured as 802.1X authenticators operate as expected. Then refer to "Option For Authenticator Ports: Configure Port-Security To Allow Only 802.1X Devices" on page 8-32.

After you complete steps 1 and 2, the configured ports are enabled for 802.1X authentication (without VLAN operation), and you are ready to configure VLAN Operation.

Configuring 802.1X Open VLAN Mode. Use these commands to actually configure Open VLAN mode. For a listing of the steps needed to prepare the switch for using Open VLAN mode, refer to "Preparation" on page 8-27.

Syntax: aaa port-access authenticator [e] < *port-list* >

[auth-vid < *vlan-id* >]

Configures an existing, static VLAN to be the Authorized-Client VLAN.

[< unauth-vid < *vlan-id* >]

Configures an existing, static VLAN to be the Unauthorized-Client VLAN.

For example, suppose you want to configure 802.1X port-access with Open VLAN mode on ports A10 - A20 and:

- These two static VLANs already exist on the switch:
  - Unauthorized, VID = 80
  - Authorized, VID = 81
- Your RADIUS server has an IP address of 10.28.127.101. The server uses **rad4all** as a server-specific key string. The server is connected to a port on the Default VLAN.
- The switch's default VLAN is already configured with an IP address of 10.28.127.100 and a network mask of 255.255.255.0

```
ProCurve(config)# aaa authentication port-access eap-radius
```

Configures the switch for 802.1X authentication using an EAP-RADIUS server.

```
ProCurve(config)# aaa port-access authenticator a10-a20
```

Configures ports A10 - A20 as 802.1 authenticator ports.

```
ProCurve(config)# radius host 10.28.127.101 key rad4all
```

Configures the switch to look for a RADIUS server with an IP address of 10.28.127.101 and an encryption key of rad4all.

```
ProCurve(config)# aaa port-access authenticator e a10-a20 unauth-vid 80
```

Configures ports A10 - A20 to use VLAN 80 as the Unauthorized-Client VLAN.

```
ProCurve(config)# aaa port-access authenticator e a10-a20 auth-vid 81
```

Configures ports A10 - A20 to use VLAN 81 as the Authorized-Client VLAN.

```
ProCurve(config)# aaa port-access authenticator active
```

Activates 802.1X port-access on ports you have configured as authenticators.

Inspecting 802.1X Open VLAN Mode Operation. For information and an example on viewing current Open VLAN mode operation, refer to "Viewing 802.1X Open VLAN Mode Status" on page 8-40.

802.1X Open VLAN Operating Notes

- Although you can configure Open VLAN mode to use the same VLAN for both the Unauthorized-Client VLAN and the Authorized-Client VLAN, this is *not* recommended. Using the same VLAN for both purposes allows unauthenticated clients access to a VLAN intended only for authenticated clients, which poses a security breach.
- While an Unauthorized-Client VLAN is in use on a port, the switch temporarily removes the port from any other statically configured VLAN for which that port is configured as a member. Note that the Menu interface will still display the port's statically configured VLAN(s).
- A VLAN used as the Unauthorized-Client VLAN should not allow access to resources that must be protected from unauthenticated clients.
- If a port is configured as a tagged member of VLAN "X" that is not used as an Unauthorized-Client, Authorized-Client, or RADIUS-assigned VLAN, then the port returns to tagged membership in VLAN "X" upon successful client authentication. This happens even if the RADIUS server assigns the port to another, authorized VLAN "Y". Note that if RADIUS assigns VLAN "X" as an authorized VLAN, then the port becomes an untagged member of VLAN "X" for the duration of the client connection. After the client disconnects, the port returns to tagged membership in VLAN "X". (If there is no Authorized-Client or RADIUS-assigned VLAN, then an authenticated client without tagged VLAN capability can access only a statically configured, untagged VLAN on that port.)
- When a client's authentication attempt on an Unauthorized-Client VLAN fails, the port remains a member of the Unauthorized-Client VLAN until the client disconnects from the port.
- During an authentication session on a port in 802.1X Open VLAN mode, if RADIUS specifies membership in an untagged VLAN, this assignment overrides port membership in the Authorized-Client VLAN. If there is no Authorized-Client VLAN configured, then the RADIUS assignment overrides any untagged VLAN for which the port is statically configured.

- If an authenticated client loses authentication during a session in 802.1X Open VLAN mode, the port VLAN membership reverts back to the Unauthorized-Client VLAN. If there is no Unauthorized-Client VLAN configured, then the client loses access to the port until it can reauthenticate itself.

Option For Authenticator Ports: Configure Port-Security To Allow Only 802.1X Devices

If you use port-security on authenticator ports, you can configure it to learn only the MAC address of the first 802.1X-aware device detected on the port. Then, only traffic from this specific device is allowed on the port. When this device logs off, another 802.1X-aware device can be authenticated on the port.

Syntax: port-security [ethernet] < *port-list* >

learn-mode port-access

Configures port-security on the specified port(s) to allow only the first 802.1X-aware device the port detects.

action < none | send-alarm | send-disable >

Configures the port's response (in addition to blocking unauthorized traffic) to detecting an intruder.

Note

Port-Security operates with 802.1X authentication as described above only if the selected ports are configured as 802.1X; that is with the **control** mode in the port-access authenticator command set to **auto**. For example, to configure port A10 for 802.1X authenticator operation and display the result:

```
ProCurve(config)# aaa port-access authenticator e A10
control auto
ProCurve(config)# show port-access authenticator e A10
config
```

Note on Blocking a Non-802.1X Device

If the port's 802.1X authenticator **control** mode is configured to **authorized** (as shown below, instead of **auto**), then the first source MAC address from any device, whether 802.1X-aware or not, becomes the only authorized device on the port.

aaa port-access authenticator < *port-list* > control authorized

With 802.1X authentication disabled on a port or set to **authorized** (Force Authorize), the port may learn a MAC address that you don't want authorized. If this occurs, you can block access by the unauthorized, non-802.1X device by using one of the following options:

- If 802.1X authentication is disabled on the port, use these command syntaxes to enable it and allow only an 802.1X-aware device:

  aaa port-access authenticator e < *port-list* >

  Enables 802.1X authentication on the port.

  aaa port-access authenticator e < *port-list* > control auto

  Forces the port to accept only a device that supports 802.1X and supplies valid credentials.

- If 802.1X authentication is enabled on the port, but set to **authorized** (Force Authorized), use this command syntax to allow only an 802.1X-aware
  device:

  aaa port-access authenticator e < *port-list* > control auto

  Forces the port to accept only a device that supports 802.1X and supplies valid credentials.

Configuring Switch Ports To Operate As Supplicants for 802.1X Connections to Other Switches

802.1X Authentication Commands	page 8-15
802.1X Supplicant Commands	
[no] aaa port-access < supplicant < [ethernet] < *port-list* >	page 8-35
[auth-timeout | held-period | start-period | max-start | initialize | identity | secret | clear-statistics]	page 8-36
802.1X-Related Show Commands	page 8-38
RADIUS server configuration	pages 8-20

You can configure a switch port to operate as a supplicant in a connection to a port on another 802.1X-aware switch to provide security on links between 802.1X-aware switches. (Note that a port can operate as both an authenticator and a supplicant.)

For example, suppose that you want to connect two switches, where:

- Switch “A” has port A1 configured for 802.1X supplicant operation
- You want to connect port A1 on switch “A” to port B5 on switch “B”.

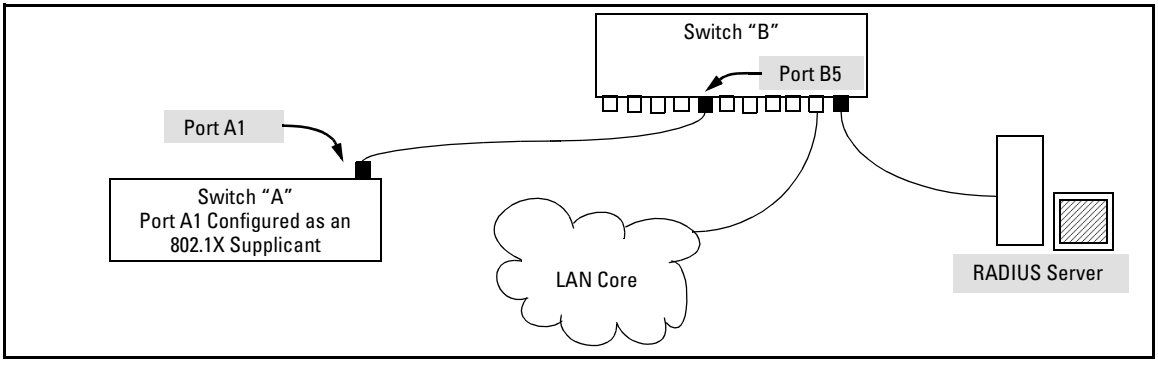

Figure 8-4. Example of Supplicant Operation

1. When port A1 on switch "A" is first connected to a port on switch "B", or if the ports are already connected and either switch reboots, port A1 begins sending start packets to port B5 on switch "B".
   - If, after the supplicant port sends the configured number of start request packets, it does not receive a response, it assumes that switch "B" is not 802.1X-aware, and transitions to the authenticated state. If switch "B" is operating properly and is not 802.1X-aware, then the link should begin functioning normally, but without 802.1X security.
   - If, after sending one or more start request packets, port A1 receives a request packet from port B5, then switch "B" is operating as an 802.1X authenticator. The supplicant port then sends a response/ID packet. If switch "B" is configured for RADIUS authentication, it forwards this request to a RADIUS server. If switch "B" is configured for Local 802.1X authentication (page 8-19), the authenticator compares the switch "A" response to its local username and password.
2. The RADIUS server then responds with an access challenge that switch "B" forwards to port A1 on switch "A".
3. Port A1 replies with a hash response based on its unique credentials. Switch "B" forwards this response to the RADIUS server.
4. The RADIUS server then analyzes the response and sends either a "success" or "failure" packet back through switch "B" to port A1.
   - A "success" response unblocks port B5 to normal traffic from port A1.
   - A "failure" response continues the block on port B5 and causes port A1 to wait for the "held-time" period before trying again to achieve authentication through port B5.

Note

You can configure a switch port to operate as both a supplicant and an authenticator at the same time.

Enabling a Switch Port To Operate as a Supplicant. You can configure one or more switch ports to operate as supplicants for point-to-point links to 802.1X-aware ports on other switches. *You must configure a port as a supplicant before you can configure any supplicant-related parameters.*

Syntax: [no] aaa port-access supplicant [ethernet] < *port-list* >

*Configures a port to operate as a supplicant using either the default supplicant parameters or any previously configured supplicant parameters, whichever is the most recent. The "***no***" form of the command disables supplicant operation on the specified ports.*

Configuring a Supplicant Switch Port. Note that you must enable supplicant operation on a port before you can change the supplicant configuration. This means you must execute the supplicant command once without any other parameters, then execute it again with a supplicant parameter you want to configure. If the intended authenticator port uses RADIUS authentication, then use the **identity** and **secret** options to configure the RADIUS-expected username and password on the supplicant port. If the intended authenticator port uses Local 802.1X authentication, then use the **identity** and **secret** options to configure the authenticator switch's local username and password on the supplicant port.

Syntax: aaa port-access supplicant [ethernet] < *port-list* >

To enable supplicant operation on the designated ports, execute this command without any other parameters. After doing this, you can use the command again with the following parameters to configure supplicant operation. (Use one instance of the command for each parameter you want to configure The **no** *form disables supplicant operation on the designated port(s).*

[identity < *username* >]

Sets the username and password to pass to the authenticator port when a challenge-request packet is received from the authenticator port in response to an authentication request. If the intended authenticator port is configured for RADIUS authentication, then ***< username >*** *and* ***< password >*** *must be the username and password expected by the RADIUS server. If the intended authenticator port is configured for Local authentication, then* ***< username >*** *and* ***< password >*** *must be the username and password configured on the Authenticator switch. (Defaults: Null)*

[secret]

Enter secret: < *password* >
Repeat secret: < *password* >

Sets the secret password to be used by the port supplicant when an MD5 authentication request is received from an authenticator. The switch prompts you to enter the secret password after the command is invoked.

aaa port-access supplicant [ethernet] < *port-list* > ***(Syntax Continued)***

[auth-timeout < 1 - 300 >]

Sets the period of time the port waits to receive a challenge from the authenticator. If the request times out, the port sends another authentication request, up to the number of attempts specified by the **max-start** *parameter. (Default: 30 seconds).*

[max-start < 1 - 10 >]

Defines the maximum number of times the supplicant port requests authentication. See step 1 on page 8-35 for a description of how the port reacts to the authenticator response. (Default: 3).

[held-period < 0 - 65535 >]

Sets the time period the supplicant port waits after an active 802.1X session fails before trying to re- acquire the authenticator port. (Default: 60 seconds)

[start-period < 1 - 300 >]

Sets the time period between Start packet retransmissions. That is, after a supplicant sends a start packet, it waits during the **start-period** *for a response. If no response comes during the* **start- period**, *the supplicant sends a new start packet. The max-start setting (above) specifies how many start attempts are allowed in the session. (Default: 30 seconds)*

aaa port-access supplicant [ethernet] < *port-list* >

[initialize]

On the specified ports, blocks inbound and outbound traffic and restarts the 802.1X authentication process. Affects only ports configured as 802.1X supplicants.

[clear-statistics]

Clears and restarts the 802.1X supplicant statistics counters.

Displaying 802.1X Configuration, Statistics, and Counters

802.1X Authentication Commands	page 8-15
802.1X Supplicant Commands	page 8-34
802.1X Open VLAN Mode Commands	page 8-21
802.1X-Related Show Commands	
show port-access authenticator	below
show port-access supplicant	page 8-43
Details of 802.1X Mode Status Listings	page 8-40
RADIUS server configuration	pages 8-20

Show Commands for Port-Access Authenticator

Syntax: show port-access authenticator [[e] < *port-list* >]
[config | statistics | session-counters]

- *Without* [< *port-list* > [config | statistics | session-counters]], *displays whether port-access authenticator is active (***Yes** *or* **No***) and the status of all ports configured for 802.1X authentication. The Authenticator Backend State in this data refers to the switch's interaction with the authentication server.*
- *With* < *port-list* > *only, same as above, but limits port status to only the specified port. Does not display data for a specified port that is not enabled as an authenticator.*
- *With* [< *port-list* > [config | statistics | session-counters]], *displays the* [config | statistics | session-counters] *data for the specified port(s). Does not display data for a specified port that is not enabled as an authenticator.*
- *With* [config | statistics | session-counters] *only, displays the* [config | statistics | session-counters] *data for all ports enabled as authenticators.*

For descriptions of [config | statistics | session-counters] *refer to the next section of this table.*

show port-access authenticator ***(Syntax Continued)***

config [[e] < *port-list* >]

Shows:

- *Whether port-access authenticator is active*
- *The 802.1X configuration of the ports configured as 802.1X authenticators*

If you do not specify < port-list >*, the command lists all ports configured as 802.1X port-access authenticators. Does not display data for a specified port that is not enabled as an authenticator.*

statistics [[e] < *port-list* >]

Shows:

- *Whether port-access authenticator is active*
- *The statistics of the ports configured as 802.1X authenticators, including the supplicant's MAC address, as determined by the content of the last EAPOL frame received on the port.*

Does not display data for a specified port that is not enabled as an authenticator.

session-counters [[e] < *port-list* >]

Shows:

- *Whether port-access authenticator is active*
- *The session status on the specified ports configured as 802.1X authenticators*

Also, for each port, the "User" column lists the user name the supplicant included in its response packet. (For the switch, this is the **identity** *setting included in the* **supplicant** *command—page 8-36.) Does not display data for a specified port that is not enabled as an authenticator.*

Viewing 802.1X Open VLAN Mode Status

You can examine the switch's current VLAN status by using the **show port-access authenticator** and **show vlan** < *vlan-id* > commands as illustrated in this section. Figure 8-5 shows an example of **show port-access authenticator** output, and table 8-1 describes the data that this command displays. Figure 8-6 shows related VLAN data that can help you to see how the switch is using statically configured VLANs to support 802.1X operation.

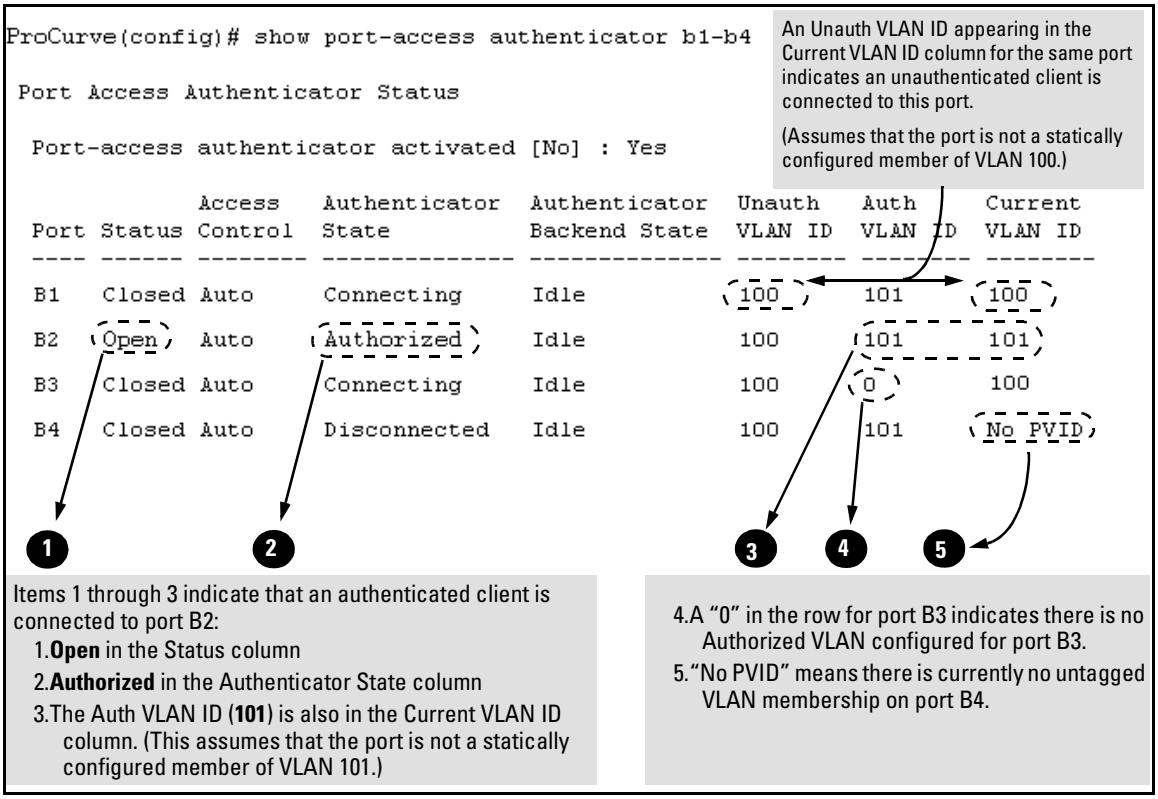

Figure 8-5. Example Showing Ports Configured for Open VLAN Mode

Thus, in the **show port-access authenticator** output:

- When the **Auth VLAN ID** is configured and matches the **Current VLAN ID** in the above command output, an authenticated client is connected to the port. (This assumes the port is not a statically configured member of the VLAN you are using for Auth VLAN.)

- When the **Unauth VLAN ID** is configured and matches the **Current VLAN ID** in the above command output, an unauthenticated client is connected to the port. (This assumes the port is not a statically configured member of the VLAN you are using for Unauth VLAN.)

Note that because a temporary Open VLAN port assignment to either an authorized or unauthorized VLAN is an untagged VLAN membership, these assignments temporarily replace any other untagged VLAN membership that is statically configured on the port. For example, if port A12 is statically configured as an untagged member of VLAN 1, but is configured to use VLAN 25 as an authorized VLAN, then the port's membership in VLAN 1 will be temporarily suspended whenever an authenticated 802.1X client is attached to the port.

Table 8-2. Open VLAN Mode Status

Status Indicator	Meaning
Port	Lists the ports configured as 802.1X port-access authenticators.
Status	**Closed:** Either no client is connected or the connected client has not received authorization through 802.1X authentication. **Open:** An authorized 802.1X supplicant is connected to the port.
Access Control This state is controlled by the following port-access command syntax: **ProCurve(config)# aaa port-access authenticator** < *port-list* > **control** < authorized | auto | unauthorized >	**Auto:** Configures the port to allow network access to any connected device that supports 802.1X authentication and provides valid 802.1X credentials. (This is the default authenticator setting.) **FA:** Configures the port for "Force Authorized", which allows access to any device connected to the port, regardless of whether it meets 802.1X criteria. (You can still configure console, Telnet, or SSH security on the port.) **FU:** Configures the port for "Force Unauthorized", which blocks access to any device connected to the port, regardless of whether the device meets 802.1X criteria.
Authenticator State	**Connecting:** A client is connected to the port, but has not received 802.1X authentication. **Force Unauth:** Indicates the "Force Unauthorized" state. Blocks access to the network, regardless of whether the client supports 802.1X authentication or provides 802.1X credentials. **Force Auth:** Indicates the "Force Authorized" state. Grants access to any device connected to the port. The device does not have to support 802.1X authentication or provide 802.1X credentials. **Authorized:** The device connected to the port supports 802.1X authentication, has provided 802.1X credentials, and has received access to the network. This is the default state for access control. **Disconnected:** No client is connected to the port.
Authenticator Backend State	**Idle:** The switch is not currently interacting with the RADIUS authentication server. Other states (**Request**, **Response**, **Success**, **Fail**, **Timeout**, and **Initialize**) may appear temporarily to indicate interaction with a RADIUS server. However, these interactions occur quickly and are replaced by **Idle** when completed.

Status Indicator	Meaning
Unauthorized VLAN ID	**< *vlan-id* >:** Lists the VID of the static VLAN configured as the unauthorized VLAN for the indicated port. **0:** No unauthorized VLAN has been configured for the indicated port.
Authorized VLAN ID	< vlan-id >: Lists the VID of the static VLAN configured as the authorized VLAN for the indicated port. 0: No authorized VLAN has been configured for the indicated port.
Current VLAN ID	**< *vlan-id* >:** Lists the VID of the static, untagged VLAN to which the port currently belongs. **No PVID:** The port is not an untagged member of any VLAN.

Syntax: show vlan < *vlan-id* >

Displays the port status for the selected VLAN, including an indication of which port memberships have been temporarily overridden by Open VLAN mode.

```
ProCurve(config)# show vlan 1
Status and Counters - VLAN Information - Ports - VLAN 1

 802.1Q VLAN ID : 1
 Name           : DEFAULT_VLAN
 Status         : Static

 Port Information Mode     Unknown VLAN Status
 ---------------- -------- ------------ ----------
 A1               Untagged Learn        Up
 A2               Untagged Learn        Up
 A3               Untagged Learn        Up
 A4               Untagged Learn        Up
 B2               Untagged Learn        Up
 B4               Tagged   Learn        Up
 B5               Untagged Learn        Down
  .                   .      .          .
  .                   .      .          .
  .                   .      .          .
 B23              Untagged Learn        Up
 B24              Untagged Learn        Up

 Overridden Port VLAN configuration

 Port Mode
 ---- ------------
 B1   Untagged
 B3   Untagged
```

Note that ports B1 and B3 are not in the upper listing, but are included under "Overridden Port VLAN configuration". This shows that static, untagged VLAN memberships on ports B1 and B3 have been overridden by temporary assignment to the authorized or unauthorized VLAN. Using the **show port-access authenticator < *port-list* >** command shown in figure 8-5 provides details.

Figure 8-6. Example of Showing a VLAN with Ports Configured for Open VLAN Mode

Show Commands for Port-Access Supplicant

Syntax: show port-access supplicant [[e] < *port-list* >] [statistics]

show port-access supplicant [[e] < *port-list* >]

Shows the port-access supplicant configuration (excluding the ***secret*** *parameter) for all ports or* < *port-list* > *ports configured on the switch as supplicants. The Supplicant State can include the following:*
Connecting - *Starting authentication.*
Authenticated - *Authentication completed (regardless of whether the attempt was successful).*
Acquired - *The port received a request for identification from an authenticator.*
Authenticating - *Authentication is in progress.*
Held - *Authenticator sent notice of failure. The supplicant port is waiting for the authenticator's held-period (page 8-36).*

For descriptions of the supplicant parameters, refer to "Configuring a Supplicant Switch Port" on page 8-36.

show port-access supplicant [[e] < *port-list* >] statistics

Shows the port-access statistics and source MAC address(es) for all ports or < *port-list* > *ports configured on the switch as supplicants. See the "Note on Supplicant Statistics", below.*

Note on Supplicant Statistics. For each port configured as a supplicant, **show port-access supplicant statistics [e] < *port-list* >]** displays the source MAC address and statistics for transactions with the authenticator device most recently detected on the port. If the link between the supplicant port and the authenticator device fails, the supplicant port continues to show data received from the connection to the most recent authenticator device until one of the following occurs:

- The supplicant port detects a different authenticator device.
- You use the **aaa port-access supplicant [e] < *port-list* > clear-statistics** command to clear the statistics for the supplicant port.
- The switch reboots.

Thus, if the supplicant's link to the authenticator fails, the supplicant retains the transaction statistics it most recently received until one of the above events occurs. Also, if you move a link with an authenticator from one

supplicant port to another without clearing the statistics data from the first port, the authenticator's MAC address will appear in the supplicant statistics for both ports.

How RADIUS/802.1X Authentication Affects VLAN Operation

Static VLAN Requirement. RADIUS authentication for an 802.1X client on a given port can include a (static) VLAN requirement. (Refer to the documentation provided with your RADIUS application.) The static VLAN to which a RADIUS server assigns a client must already exist on the switch. If it does not exist or is a dynamic VLAN (created by GVRP), authentication fails. Also, for the session to proceed, the port must be an untagged member of the required VLAN. If it is not, the switch temporarily reassigns the port as described below.

If the Port Used by the Client Is Not Configured as an Untagged Member of the Required Static VLAN: When a client is authenticated on port "N", if port "N" is not already configured as an untagged member of the static VLAN specified by the RADIUS server, then the switch temporarily assigns port "N" as an untagged member of the required VLAN (for the duration of the 802.1X session). *At the same time, if port "N" is already configured as an untagged member of another VLAN, port "N" loses access to that other VLAN for the duration of the session.* (This is because a port can be an untagged member of only one VLAN at a time.)

For example, suppose that a RADIUS-authenticated, 802.1X-aware client on port A2 requires access to VLAN 22, but VLAN 22 is configured for no access on port A2, and VLAN 33 is configured as untagged on port A2:

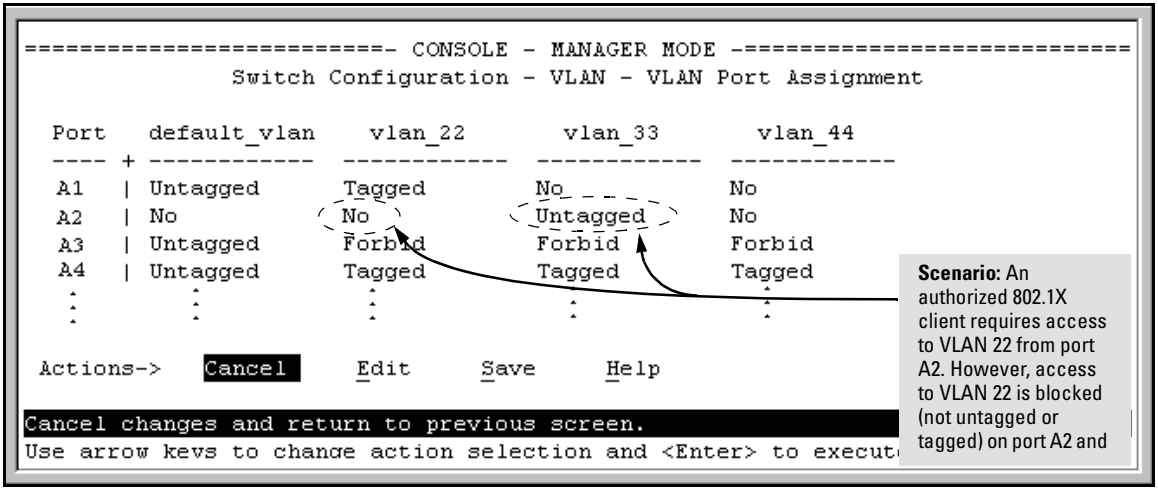

Figure 8-7. Example of an Active VLAN Configuration

In figure 8-7, if RADIUS authorizes an 802.1X client on port 2 with the requirement that the client use VLAN 22, then:

- VLAN 22 becomes available as Untagged on port A2 for the duration of the session.
- VLAN 33 becomes unavailable to port A2 for the duration of the session (because there can be only one untagged VLAN on any port).

You can use the **show vlan < *vlan-id* >** command to view this temporary change to the active configuration, as shown below:

- You can see the temporary VLAN assignment by using the **show vlan < *vlan-id* >** command with the **< *vlan-id* >** of the static VLAN that the authenticated client is using.

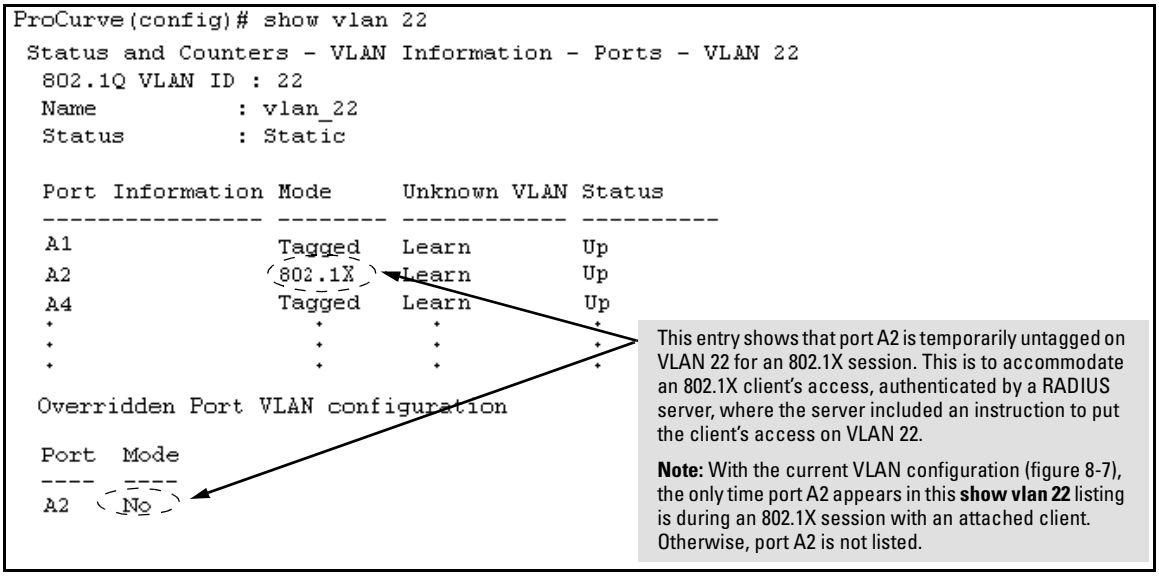

Figure 8-8. The Active Configuration for VLAN 22 Temporarily Changes for the 802.1X Session

- With the preceding in mind, since (static) VLAN 33 is configured as untagged on port A2 (see figure 8-7), and since a port can be untagged on only one VLAN, port A2 loses access to VLAN 33 for the duration of the 802.1X session involving VLAN 22. You can verify the temporary loss of access to VLAN 33 with the **show vlan 33** command.

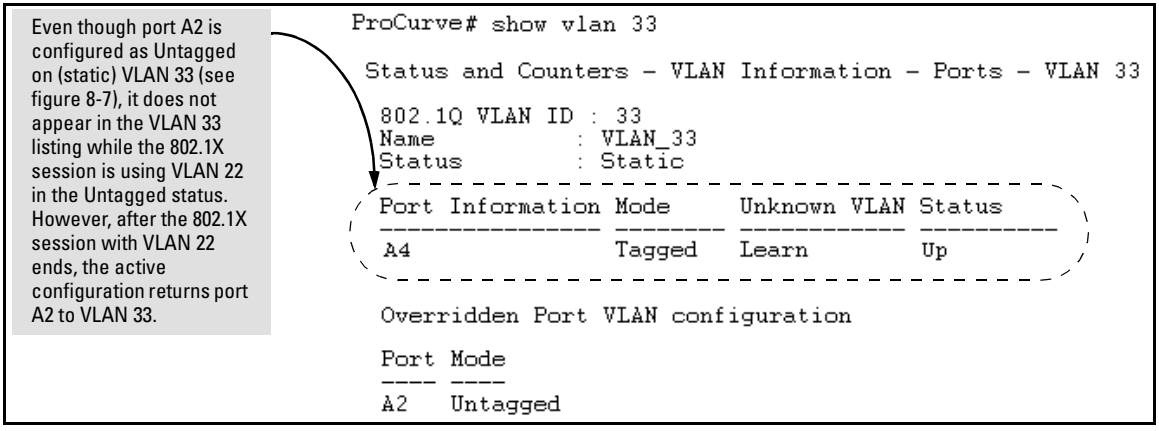

Figure 8-9. The Active Configuration for VLAN 33 Temporarily Drops Port 22 for the 802.1X Session

When the 802.1X client's session on port A2 ends, the port discards the temporary untagged VLAN membership. At this time the static VLAN actually configured as untagged on the port again becomes available. Thus, when the RADIUS-authenticated 802.1X session on port A2 ends, VLAN 22 access on port A2 also ends, and the untagged VLAN 33 access on port A2 is restored.

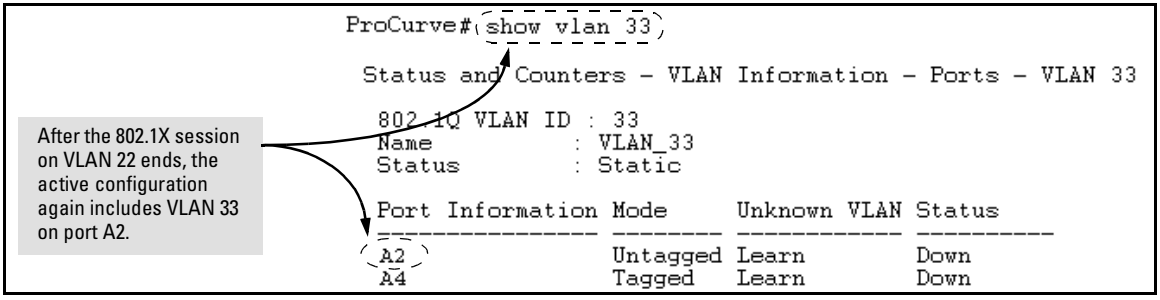

Figure 8-10. The Active Configuration for VLAN 33 Restores Port A2 After the 802.1X Session Ends

Notes

Any port VLAN-ID changes you make on 802.1X-aware ports during an 802.1X-authenticated session do not take effect until the session ends.

With GVRP enabled, a temporary, untagged static VLAN assignment created on a port by 802.1X authentication is advertised as an existing VLAN. If this temporary VLAN assignment causes the switch to disable a configured (untagged) static VLAN assignment on the port, then the disabled VLAN assignment is not advertised. When the 802.1X session ends, the switch:

- Eliminates and ceases to advertise the temporary VLAN assignment.
- Re-activates and resumes advertising the temporarily disabled VLAN assignment.

Messages Related to 802.1X Operation

Table 8-3. 802.1X Operating Messages

Message	Meaning
`Port < port-list > is not an authenticator.`	The ports in the port list have not been enabled as 802.1X authenticators. Use this command to enable the ports as authenticators: `ProCurve(config)# aaa port-access authenticator e 10`
`Port < port-list > is not a supplicant.`	Occurs when there is an attempt to change the supplicant configuration on a port that is not currently enabled as a supplicant. Enable the port as a supplicant and then make the desired supplicant configuration changes. Refer to "Enabling a Switch Port To Operate as a Supplicant" on page 8-35.
`No server(s) responding.`	This message can appear if you configured the switch for EAP-RADIUS or CHAP-RADIUS authentication, but the switch does not receive a response from a RADIUS server. Ensure that the switch is configured to access at least one RADIUS server. (Use **show radius**.) If you also see the message `Can't reach RADIUS server < x.x.x.x >`, try the suggestions listed for that message (page 5-31).
`LACP has been disabled on 802.1X port(s).`	To maintain security, LACP is not allowed on ports configured for 802.1X authenticator operation. If you configure port security on a port on which LACP (active or passive) is configured, the switch removes the LACP configuration, displays a notice that LACP is disabled on the port(s), and enables 802.1X on that port.
`Error configuring port < port-number >: LACP and 802.1X cannot be run together.`	Also, the switch will not allow you to configure LACP on a port on which port access (802.1X) is enabled.