13

Configuring Port-Based and User-Based Access Control (802.1X)

Contents

Overview

Feature	Default	Menu	CLI	Web
Configuring Switch Ports as 802.1X Authenticators	Disabled	n/a	page 13-18	n/a
Configuring 802.1X Open VLAN Mode	Disabled	n/a	page 13-29	n/a
Configuring Switch Ports to Operate as 802.1X Supplicants	Disabled	n/a	page 13-47	n/a
Displaying 802.1X Configuration, Statistics, and Counters	n/a	n/a	page 13-51	n/a
How 802.1X Affects VLAN Operation	n/a	n/a	page 13-66	n/a
RADIUS Authentication and Accounting	Refer to chapter 6, "RADIUS Authentication and Accounting"			

Why Use Port-Based or User-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 simplifies security management by providing access control along with the ability to control user profiles from up to three RADIUS servers while allowing a given user to use the same entering valid user credentials for access from multiple points within the network.

General Features

802.1X on the switches covered in this guide 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 access 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).
  - User-Based access control option with support for up to 32 authenticated clients per-port.

  - Port-Based access control option allowing authentication by a single client to open the port. This option does not force a client limit and, on a port opened by an authenticated client, allows unlimited client access without requiring further authentication.
  - Supplicant implementation using CHAP authentication and independent user credentials on each port.
- The local operator password configured with the **password** command for management access to the switch is no longer accepted as an 802.1X authenticator credential. The **password port-access** command configures the local operator username and password used as 802.1X authentication credentials for access to the switch. The values configured can be stored in a configuration file using the **include-credentials** command. For information about the **password port-access** command, see "Do These Steps Before You Configure 802.1X Operation" on page 13-14.
- On-demand change of a port's configured VLAN membership status to support the current client session.
- Session accounting with a RADIUS server, including the accounting update interval.
- Use of Show commands to display session counters.
- Support for concurrent use of 802.1X and either Web authentication or MAC authentication on the same port.
- For unauthenticated clients that do not have the necessary 802.1X supplicant software (or for other reasons related to unauthenticated clients), there is the option to configure an *Unauthorized-Client VLAN*. This mode allows you to assign unauthenticated clients to an isolated VLAN through which you can provide the necessary supplicant software and/or other services you want to extend to these clients.

User Authentication Methods

The switch offers two methods for using 802.1X access control. Generally, the "Port Based" method supports one 802.1X-authenticated client on a port, which opens the port to an unlimited number of clients. The "User-Based" method supports up to 32 802.1X-authenticated clients on a port. In both cases, there are operating details to be aware of that can influence your choice of methods.

802.1X User-Based Access Control

802.1X operation with access control on a per-user basis provides client-level security that allows LAN access to individual 802.1X clients (up to 32 per port), where each client gains access to the LAN by entering valid user credentials.

This operation improves security by opening a given port only to individually authenticated clients, while simultaneously blocking access to the same port for clients that cannot be authenticated. All sessions must use the same untagged VLAN. Also, an authenticated client can use any tagged VLAN memberships statically configured on the port, provided the client is configured to use the tagged VLAN memberships available on the port. (Note that the session total includes any sessions begun by the Web Authentication or MAC Authentication features covered in chapter 4.) For more information, refer to "Option For Authenticator Ports: Configure Port-Security To Allow Only 802.1X-Authenticated Devices" on page 13-45.

802.1X Port-Based Access Control

802.1X port-based access control provides port-level security that allows LAN access only on ports where a single 802.1X-capable client (supplicant) has entered authorized RADIUS user credentials. For reasons outlined below, this option is recommended for applications where only one client at a time can connect to the port. Using this option, the port processes all traffic as if it comes from the same client. Thus, in a topology where multiple clients can connect to the same port at the same time:

- If the first client authenticates and opens the port, and then another client authenticates, the port responds as if the original client has initiated a reauthentication. With multiple clients authenticating on the port, the RADIUS configuration response to the latest client authentication replaces any other configuration from an earlier client authentication. If all clients use the same configuration this should not be a problem. But if the RADIUS server responds with different configurations for different clients, then the last client authenticated will effectively lock out any previously authenticated client. When *any* client to authenticate closes its session, the port will also close and remain so until another client successfully authenticates.
- The most recent client authentication determines the untagged VLAN membership for the port. Also, any client able to use the port can access any tagged VLAN memberships statically configured on the port, provided the client is configured to use the available, tagged VLAN memberships.
- If the first client authenticates and opens the port, and then one or more other clients connect without trying to authenticate, then the port configuration as determined by the original RADIUS response remains unchanged and all such clients will have the same access as the authenticated client. When the authenticated client closes the session, the port will also be closed to any other, unauthenticated clients that may have also been using the port.

This operation unblocks the port while an authenticated client session is in progress. In topologies where simultaneous, multiple client access is possible this can allow unauthorized and unauthenticated access by another client while an authenticated client is using the port. If you want to allow only authenticated clients on the port, then user-based access control (page 13-4) should be used instead of port-based access control. Using the user-based method enables you to specify up to 32 authenticated clients.

Note

Port-Based 802.1X can operate concurrently with Web-Authentication or MAC-Authentication on the same port. However, this is not a commonly used application and is not generally recommended. For more information, refer to the operating note on page 13-13.

Alternative To Using a RADIUS Server

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 user credential administration, and reduces security by limiting authentication to one Operator password set for all users.

Accounting

The switches covered in this guide also provide RADIUS Network accounting for 802.1X access. Refer to chapter 6, "RADIUS-Administered CoS and Rate-Limiting".

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

a port loses its authenticated client connection, it drops its membership in this VLAN. Note that with multiple clients on a port, all such clients use the same untagged, port-based VLAN membership.

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 a 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 applications, a switch that requires a supplicant to provide the proper credentials 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.

User-Based Authentication: The 802.1X extension in the switches covered in this guide. In this operation, multiple clients on the same port must individually authenticate themselves.

Guest VLAN: See "Unauthorized-Client VLAN".

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.

Port-Based Authentication: In this operation, the first client on a port to authenticate itself unblocks the port for the duration of the client's 802.1X-authenticated session. The switches covered in this guide use port-based authentication.

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 Membership in a VLAN: 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 port-based VLAN at a time.) Where a port is a tagged member of a VLAN, 802.1X Open VLAN mode does not affect the port's access to the VLAN 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 Membership in a VLAN**".

Unauthorized-Client VLAN: A conventional, static VLAN statically configured on the switch. It is used to provide access to a client prior to authentication, and is sometimes termed a *guest* VLAN. 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. An unauthorized-client VLAN is available on a port only if there is no authenticated client already using the port.

Untagged Membership in a VLAN: 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 Membership in a VLAN**".

General 802.1X Authenticator Operation

This operation provides security on a point-to-point link between a 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 13-29.)

Example of the Authentication Process

Suppose that you have configured a port on the switch for 802.1X authentication operation, which blocks access to the LAN through that port. If you then connect an 802.1X-aware client (supplicant) to the port and attempt to log on:

1. The switch responds with an identity request.
2. The client responds with a user name that uniquely defines this request for the client.
3. The switch responds in one of the following ways:
   - If 802.1X 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 on the switch is configured for local authentication, then:
     i. The switch compares the client's credentials to the username and password configured in the switch (Operator 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 for that client.

Note

The switches covered in this guide can use either 802.1X port-based authentication or 802.1X user-based authentication. For more information, refer to "User Authentication Methods" on page 13-4.

VLAN Membership Priority

Following client authentication, an 802.1X port resumes membership in any tagged VLANs for which it is already assigned in the switch configuration. The port also becomes an untagged member of one VLAN according to the following order of options:

a. **1st Priority:** The port joins a VLAN to which it has been assigned by a RADIUS server during client authentication.

b. **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.

c. **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.

A port assigned to a VLAN by an Authorized-Client VLAN configuration (or a RADIUS server) will be an untagged member of the VLAN for the duration of the authenticated session. This applies even if the port is also configured in the switch as a tagged member of the same VLAN.

Note

On the switches covered in this guide, using the same port for both RADIUS-assigned clients and clients using a configured, Authorized-Client VLAN is not recommended. This is because doing so can result in authenticated clients with mutually exclusive VLAN priorities, which means that some authenticated clients can be denied access to the port. Refer to figure 13-1 on page 13-11.

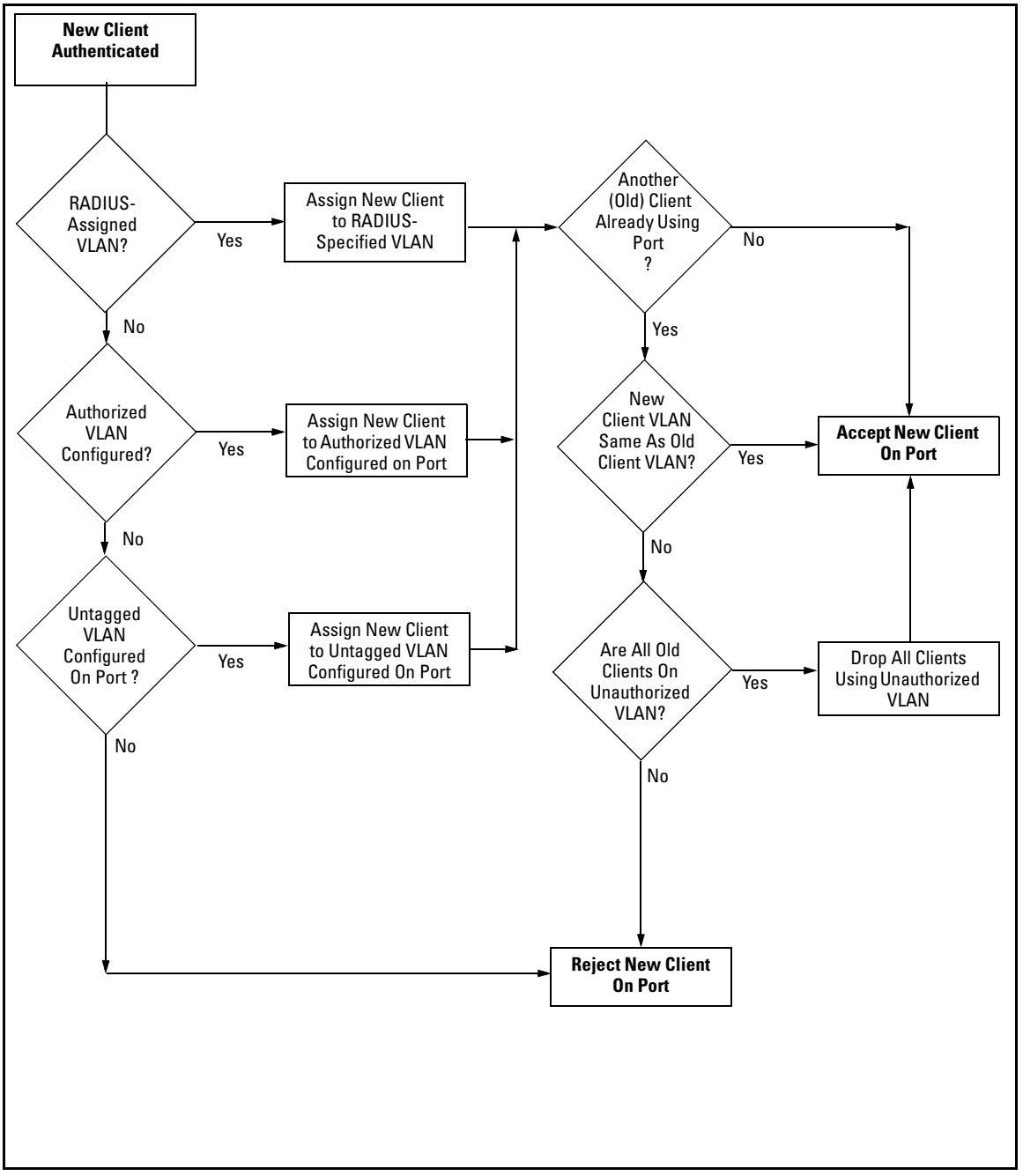


Figure 13-1. Priority of VLAN Assignment for an Authenticated Client

General Operating Rules and Notes

- In the user-based mode, when there is an authenticated client on a port, the following traffic movement is allowed:
  - Multicast and broadcast traffic is allowed on the port.
  - Unicast traffic to authenticated clients on the port is allowed.
  - All traffic from authenticated clients on the port is allowed.
- 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.
- Using user-based 802.1X authentication, when a port on the switch is configured as an authenticator the port allows only authenticated clients up to the currently configured client limit.

  For clients that do not have the proper 802.1X supplicant software, the optional 802.1X Open VLAN mode can be used to open a path for downloading 802.1X supplicant software to a client or to provide other services for unauthenticated clients. Refer to “802.1X Open VLAN Mode” on page 13-29.)
- Using port-based 802.1X authentication, When a port on the switch is configured as an authenticator, one authenticated client opens the port. Other clients that are not running an 802.1X supplicant application can have access to the switch and network through the opened port. If another client uses an 802.1X supplicant application to access the opened port, then a re-authentication occurs using the RADIUS configuration response for the latest client to authenticate. To control access by all clients, use the user-based method.
- Where a switch port is configured with user-based authentication to accept multiple 802.1X (and/or Web- or MAC-Authentication) client sessions, all authenticated clients must use the same port-based, untagged VLAN membership assigned for the earliest, currently active client session. Thus, on a port where one or more authenticated client sessions are already running, all such clients will be on the same untagged VLAN. If a RADIUS server subsequently authenticates a new client, but attempts to re-assign the port to a different, untagged VLAN than the one already in use for the previously existing, authenticated client sessions, the connection for the new client will fail. For more on this topic, refer to “802.1X Open VLAN Mode” on page 13-29. (Note that if the port is statically configured with any tagged VLAN memberships, any authenticated client configured to use these tagged VLANs will have access to them.)

- 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.
- 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 allow authentication of the supplicant. 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 will allow the supplicant to re-authenticate.
- 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.
- Meshing is not supported on ports configured for 802.1X port-access security.
- A port can be configured as an authenticator *or* an 802.1X supplicant, or both. Some configuration instances block traffic flow or allow traffic to flow without authentication. Refer to “Configuring Switch Ports To Operate As Supplicants for 802.1X Connections to Other Switches” on page 13-47.
- 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.

Applying Web Authentication or MAC Authentication Concurrently with Port-Based 802.1X Authentication: While 802.1X port-based access control can operate concurrently with Web Authentication or MAC Authentication, port-based access control is subordinate to Web-Auth and MAC-Auth operation. If 802.1X operates in port-based mode and MAC or Web authentication is enabled on the same port, any 802.1X authentication has no effect on the ability of a client to access the controlled port. That is, the client’s access will be denied until the client authenticates through Web-Auth or MAC-Auth on the port. Note also that a client authenticating with port-based 802.1X does not open the port in the same way that it would if Web-Auth or MAC-Auth were not enabled. That is, any non-authenticating client attempting to access the port after another client authenticates with port-based 802.1X would still have to authenticate through Web-Auth or MAC-Auth.

General Setup Procedure for 802.1X Access Control

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.)

   For switches covered in this guide, the local operator password configured with the password command is not accepted as an 802.1X authenticator credential. The port-access command is used to configure the operator username and password that are used as 802.1X credentials for network access to the switch. 802.1X network access is not allowed unless a password has been configured using the **password port-access** command.

   Syntax: password port-access [user-name <*name*>] <*password* >

   Configures the operator username and password used to access the network through 802.1X authentication.

   user-name <*name*>

   Operator username (text string) used only for local authentication of 802.1X clients. This value is different from the local operator username configured with the **password** *command for management access.*

   <*password*>

   Operator password (text string) used only for local authentication of 802.1X clients. This value is different from the local operator password configured with the **password** *command for management access.*

Figure 13-2 shows how to configure a local operator password for 802.1X access.

```
ProCurve(config)# password port-access user-name Jim secret3
```

Figure 13-2. Example of the Password Port-Access Command

You can save the port-access password for 802.1X authentication in the configuration file by using the **include-credentials** command. For more information, see "Saving Security Credentials in a Config File" on page 2-10. in this guide.

2. Determine the switch ports that you want to configure as authenticators and/or supplicants, and disable LACP on these ports. (For more information on disabling LACP, refer to the "Note" on page 13-19.).

   To display the current configuration of 802.1X, Web-based, and MAC authentication on all switch ports, enter the **show port-access config** command.

```
ProCurve (config)# show port-access config

 Port Access Status Summary
  Port-access authenticator activated [No] : Yes
  Allow RADIUS-assigned dynamic (GVRP) VLANs [No] : Yes

       Supplicant Authenticator Web Auth Mac Auth
  Port Enabled    Enabled       Enabled  Enabled
  ---- ---------- ------------- -------- --------
  1    Yes        No            No       Yes
  2    No         Yes           No       Yes
  3    No         Yes           No       No
  4    No         No            No       No
  5    No         No            No       No
  6    No         No            No       No
  7    No         No            No       No
  8    No         No            No       No
  9    No         No            No       No
  10   No         No            No       No
  11   No         No            No       No
  12   No         No            No       No
  ...
```

Figure 13-3. Example of show port-access config Command Output

3. Determine whether to use user-based access control (page 13-4) or port-based access control (page 13-5).
4. 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 13-29.
5. For any port you want to operate as a supplicant, determine the user credentials. You can either use the same credentials for each port or use unique credentials for individual ports or subgroups of ports. (This can also be the same local username/password pair that you assign to the switch.)
6. 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 the following:

- "802.1X User-Based Access Control" on page 13-4
- "802.1X Port-Based Access Control" on page 13-5
- "Configuring Switch Ports To Operate As Supplicants for 802.1X Connections to Other Switches" on page 13-47.

1. Enable 802.1X user-based or port-based 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 13-19.
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 13-29.
3. Configure the 802.1X authentication type. Options include:
   - Local Operator username and password (using the **password port-access** command).
   - 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.

   Refer to page 13-24.
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 13-25.
5. Enable 802.1X authentication on the switch. Refer to "1. Enable 802.1X Authentication on Selected Ports" on page 13-19.
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. Refer to page 13-45.
8. If you want a port on the switch to operate as a supplicant on 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 13-47.)

Configuring Switch Ports as 802.1X Authenticators

802.1X Authentication Commands	Page
[no] aaa port-access authenticator < *port-list* >	13-19
[auth-vid | clear-statistics | client-limit | control | max-requests | initialize | logoff-period | quiet-period | server-timeout | reauthenticate | reauth-period | supplicant-timeout | tx-period | unauth-period | unauth-vid]	13-19
aaa authentication port-access < local | eap-radius | chap-radius >	13-24
[no] aaa port-access authenticator active	13-18
aaa port-access <*port-list*> controlled-directions <both | in>	13-26
[no] port-security [ethernet] < *port-list* > learn-mode port-access	13-45
802.1X Open VLAN Mode Commands	13-29
802.1X Supplicant Commands	13-47
802.1X-Related Show Commands	13-51
RADIUS server configuration	13-25

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, and consists of two steps:

A. Enable the selected ports as authenticators.

B. Specify either user-based or port-based 802.1X authentication.

(Actual 802.1X operation does not commence until you perform step 5 on page 13-25 to activate 802.1X authentication on the switch.)

Note

If 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.

A. Enable the Selected Ports as Authenticators and Enable the (Default) Port-Based Authentication

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

Enables specified ports to operate as 802.1X authenticators and enables port-based authentication. (To enable user-based authentication, execute this command first, and then execute the client-limit < port-list > version of this command described in the next section.) The **no** *form of the command removes 802.1X authentication from < port-list >. To activate configured 802.1X operation, you must enable 802.1X authentication. Refer to "5. Enable 802.1X Authentication on the switch" on page 13-25.*

B. Specify User-Based Authentication or Return to Port-Based Authentication

User-Based 802.1X Authentication.

Syntax: aaa port-access authenticator client-limit < *port-list* > < 1 - 32 >

Used after executing **aaa port-access authenticator < *port-list* >** *(above) to convert authentication from port-based to user-based. Specifies user-based 802.1X authentication and the maximum number of 802.1X-authenticated client sessions allowed on each of the ports in* **< *port-list* >.** *If a port currently has no authenticated client sessions, the next authenticated client session the port accepts determines the untagged VLAN membership to which the port is assigned during the session. If another client session begins later on the same port while an earlier session is active, the later session will be on the same untagged VLAN membership as the earlier session.*

Note: *Because a switch allows 802.1X authentication and Web or MAC authentication to co-exist on the same port, the sum of authenticated client sessions allowed on a given port for both 802.1X and either Web- or MAC-authentication cannot exceed 32.*

Port-Based 802.1X Authentication.

no aaa port-access authenticator client-limit

Used to convert a port from user-based authentication to port-based authentication, which is the default setting for ports on which authentication is enabled. (Executing **aaa port-access authenticator < *port-list* >** *enables 802.1X authentication on* **< *port-list* >** *and enables port-based authentication—page 13-19.) If a port currently has no authenticated client sessions, the next authenticated client session the port accepts determines the untagged VLAN membership to which the port is assigned during the session. If another authenticated client session begins later on the same port while an earlier session is active, the later session replaces the currently active session and will be on the untagged VLAN membership specified by the RADIUS server for the later session.*

Example: Configuring User-Based 802.1X Authentication

This example enables ports A10-A12 to operate as authenticators, and then configures the ports for user-based authentication.

```
ProCurve(config)# aaa port-access authenticator a10-A12
ProCurve(config)# aaa port-access authenticator a10-A12 client-limit 4
```

Figure 13-4. Example of Configuring User-Based 802.1X Authentication

Example: Configuring Port-Based 802.1X Authentication

This example enables ports A13-A15 to operate as authenticators, and then configures the ports for port-based authentication.

```
ProCurve(config)# aaa port-access authenticator a13-a15
ProCurve(config)# no aaa port-access authenticator a13-a15 client-limit
```

Figure 13-5. Example of Configuring Port-Based 802.1X Authentication

2. Reconfigure Settings for Port-Access

The commands in this section are initially set by default and can be reconfigured as needed.

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

[control < authorized | auto | unauthorized >]

Controls authentication mode on the specified port:

authorized: *Also termed "Force Authorized". Gives access to a device connected to the port. In this case, the device does not have to provide 802.1X credentials or support 802.1X authentication. (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 to get network access. (Optional: You can use the Open VLAN mode to provide a path for clients without 802.1X supplicant software to down-load this software and begin the authentication process. Refer to "802.1X Open VLAN Mode" on page 13-29.)*

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)

— Continued —

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

[supplicant-timeout < 1 - 300 >]

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

[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)*

—Continued—

[reauth-period < 0 - 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 13-29.

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

[logoff-period]< 1 - 999999999 >

Configures the period of time the switch waits for client activity before removing an inactive client from the port. (Default: 300 seconds)

[unauth-period < 0-255 >]

Specifies a delay in seconds for placing a port on the Unauthorized-Client VLAN. This delay allows more time for a client with 802.1X supplicant capability to initiate an authentication session. If a connected client does not initiate a session before the timer expires, the port is assigned to the Unauthenticated-Client VLAN. (Default: 0 seconds)

[auth-vid < *vid* >]

Configures an existing, static VLAN to be the Authorized-Client VLAN. Refer to "802.1X Open VLAN Mode" on page 13-29.

3. Configure the 802.1X Authentication Method

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

You can configure **local**, **chap-radius** or **eap-radius** as the primary password authentication method for the port-access method. You also need to select **none or authorized** as a secondary, or backup, method.

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

Configures **local**, **chap-radius (**MD5**)**, *or* **eap-radius** *as the primary password authentication method for port-access. The default primary authentication is* **local**. *(Refer to the documentation for your RADIUS server application.)*

For switches covered in this guide, you must use the **password port-access** *command to configure the operator username and password for 802.1X access. See "General Setup Procedure for 802.1X Access Control" on page 13-14 for more information.*

[<none | authorized >]

Provides options for secondary authentication. The **none** *option specifies that a backup authentication method is not used. The* **authorized** *option allows access without authentication. (default:* **none***).*

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

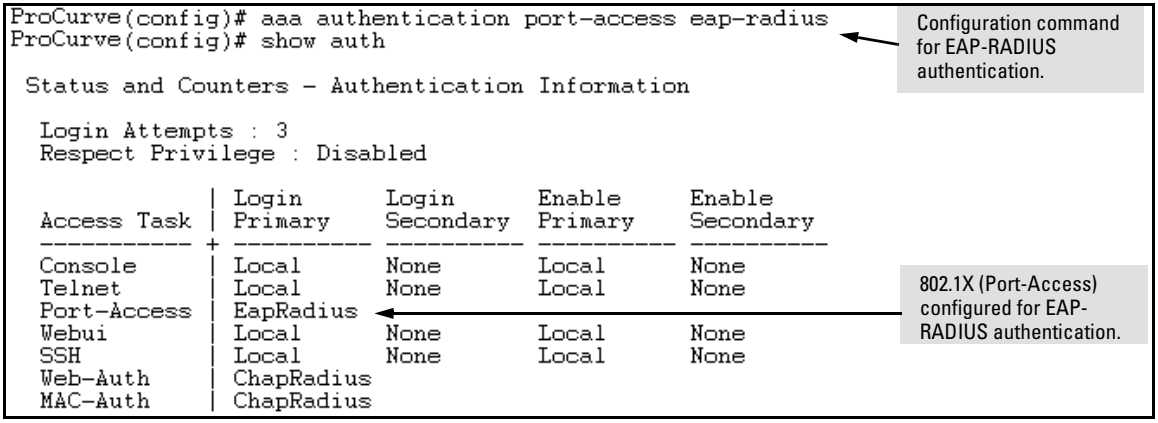


Figure 13-6. Example of 802.1X (Port-Access) Authentication

4. Enter the RADIUS Host IP Address(es)

If you select either **eap-radius** or **chap-radius** for the authentication method, configure the switch to use 1, 2, or 3 RADIUS servers for authentication. The following syntax shows the basic commands. For coverage of all commands related to RADIUS server configuration, refer to chapter 6, "RADIUS Authentication and Accounting".

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.

Syntax: 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.

6. Optional: Reset Authenticator Operation

While 802.1X authentication is operating, you can use the following **aaa port-access authenticator** commands to reset 802.1X authentication and statistics on specified ports.

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

[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.*

[reauthenticate]

On the specified ports, forces reauthentication (unless the authenticator is in "HELD" state).

[clear-statistics]

On the specified ports, clears authenticator statistics counters.

7. Optional: Configure 802.1X Controlled Directions

After you enable 802.1X authentication on specified ports, you can use the **aaa port-access controlled-directions** command to configure how a port transmits traffic before it successfully authenticates a client and enters the authenticated state.

As documented in the IEEE 802.1X standard, an 802.1X-aware port that is unauthenticated can control traffic in either of the following ways:

- In both ingress and egress directions by disabling both the reception of incoming frames and transmission of outgoing frames
- Only in the ingress direction by disabling only the reception of incoming frames.

Prerequisite. As documented in the IEEE 802.1X standard, the disabling of incoming traffic and transmission of outgoing traffic on an 802.1X-aware egress port in an unauthenticated state (using the **aaa port-access controlled-directions in** command) is supported only if:

- The port is configured as an edge port in the network using the **spanning-tree edge-port** command.
- The 802.1s Multiple Spanning Tree Protocol (MSTP) or 802.1w Rapid Spanning Tree Protocol (RSTP) is enabled on the switch. MSTP and RSTP improve resource utilization while maintaining a loop-free network.

For information on how to configure the prerequisites for using the **aaa port-access controlled-directions in** command, see Chapter 4, "Multiple Instance Spanning-Tree Operation" in the *Advanced Traffic Management Guide*.

Syntax: aaa port-access <*port-list*> controlled-directions <both | in>

both *(default)*: *Incoming and outgoing traffic is blocked on an 802.1X-aware port before authentication occurs.*

in: *Incoming traffic is blocked on an 802.1X-aware port before authentication occurs. Outgoing traffic with unknown destination addresses is flooded on unauthenticated 802.1X-aware ports.*

Wake-on-LAN Traffic

The Wake-on-LAN feature is used by network administrators to remotely power on a sleeping workstation (for example, during early morning hours to perform routine maintenance operations, such as patch management and software updates).

The **aaa port-access controlled-direction in** command allows Wake-on-LAN traffic to be transmitted on an 802.1X-aware egress port that has not yet transitioned to the 802.1X authenticated state; the **controlled-direction both** setting prevents Wake-on-LAN traffic to be transmitted on an 802.1X-aware egress port until authentication occurs.

Note

Although the **controlled-direction in** setting allows Wake-on-LAN traffic to traverse the switch through unauthenticated 802.1X-aware egress ports, it does not guarantee that the Wake-on-LAN packets will arrive at their destination. For example, firewall rules on other network devices and VLAN rules may prevent these packets from traversing the network.

Operating Notes

- Using the **aaa port-access controlled-directions in** command, you can enable the transmission of Wake-on-LAN traffic on unauthenticated egress ports that are configured for any of the following port-based security features:
  - 802.1X authentication
  - MAC authentication
  - Web authentication

  Because a port can be configured for more than one type of authentication to protect the switch from unauthorized access, the last setting you configure with the **aaa port-access controlled-directions** command is applied to all authentication methods configured on the switch.

  For information about how to configure and use MAC and Web authentication, refer to chapter 4, “Web and MAC Authentication”.

- To display the currently configured 802.1X Controlled Directions value, enter the **show port-access authenticator config** command as shown in Figure 13-11.
- When an 802.1X-authenticated port is configured with the **controlled-directions in** setting, eavesdrop prevention is not supported on the port.

Example: Configuring 802.1X Controlled Directions

The following example shows how to enable the transmission of Wake-on-LAN traffic in the egress direction on an 802.1X-aware port before it transitions to the 802.1X authenticated state and successfully authenticates a client device.

```
ProCurve(config)# aaa port-access authenticator a10
ProCurve(config)# aaa authentication port-access eap-radius
ProCurve(config)# aaa port-access authenticator active
ProCurve(config)# aaa port-access a10 controlled-directions in
```

Figure 13-7. Example of Configuring 802.1X Controlled Directions

802.1X Open VLAN Mode

Introduction

This section describes how to use the 802.1X Open VLAN mode to provide a path for clients that need to acquire 802.1X supplicant software before proceeding with the authentication process. The Open VLAN mode involves options for configuring unauthorized-client and authorized-client VLANs on ports configured as 802.1X authenticators.

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 VLAN memberships and placing the port in a designated *Unauthorized-Client VLAN* (sometimes termed a *guest* VLAN). In this state the client can proceed with initialization services, such as acquiring IP addressing and 802.1X client software, and starting the authentication process.

Note

On ports configured to allow multiple sessions using 802.1X user-based access control, all clients must use the same untagged VLAN. On a given port where there are no currently active, authenticated clients, the first *authenticated* client determines the untagged VLAN in which the port will operate for all subsequent, overlapping client sessions.

If the switch operates in an environment where some valid clients will not be running 802.1X supplicant software and need to download it from your network. Then, because such clients would need to use the Unauthorized-Client VLAN and authenticated clients would be using a different VLAN (for security reasons), allowing multiple clients on an 802.1X port can result in blocking some or all clients needing to use the Unauthorized-Client VLAN.

On ports configured for port-based 802.1X access control, if multiple clients try to authenticate on the same port, the most recently authenticated client determines the untagged VLAN membership for that port. Clients that connect without trying to authenticate will have access to the untagged VLAN membership that is currently assigned to the port.

VLAN Membership Priorities

Following client authentication, an 802.1X port resumes membership in any tagged VLANs for which it is already assigned in the switch configuration. The port also becomes an untagged member of one VLAN according to the following order of options:

a. **1st Priority:** The port joins a VLAN to which it has been assigned by a RADIUS server during client authentication.

b. **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.

c. **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.

A port assigned to a VLAN by an Authorized-Client VLAN configuration (or a RADIUS server) will be an untagged member of the VLAN for the duration of the authenticated session. This applies even if the port is also configured in the switch as a tagged member of the same VLAN.

Note

After client authentication, the port resumes membership in any tagged VLANs for which it is configured. If the port is a tagged member of a VLAN used for 1 or 2 listed above, then it also 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 or instead of 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 port-based 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 it is configured. See the "Note", above.

Table 13-2. 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 without 802.1X supplicant capability, 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. **Note for a Port Configured To Allow Multiple Client Sessions:** If any previously authenticated clients are using a port assigned to a VLAN other than the Unauthorized-Client VLAN, then a later client that is not running 802.1X supplicant software is blocked on the port until all other, authenticated clients on the port have disconnected.

802.1X Per-Port Configuration	Port Response
Authorized-Client VLAN	• After client authentication, the port drops membership in the Unauthorized-Client VLAN and becomes an untagged member of this VLAN. **Notes:** If the client is running an 802.1X supplicant application when the authentication session begins, and is able to authenticate itself before the switch assigns the port to the Unauthorized-Client VLAN, then the port does not become a member of the Unauthorized-Client VLAN. On the switches covered in this guide, you can use the **unauth-period** command—page 13-23—to delay moving the port into the Unauthorized-Client VLAN. If RADIUS authentication assigns a VLAN and there are no other authenticated clients on the port, then the port 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. • If the port is statically configured as a tagged member of a VLAN, 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.

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 the port to a VLAN, 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, 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. **Note for a Port Configured To Allow Multiple Client Sessions:** If any previously authenticated clients are using a port assigned to a VLAN other than the Unauthorized-Client VLAN (such as a RADIUS-assigned VLAN), then a later client that is not running 802.1X supplicant software is blocked on the port until all other, authenticated clients on the port have disconnected. Refer to figure 13-1 on page 13-11.

802.1X Per-Port Configuration	Port Response
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. • 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. **Note:** An authorized-client VLAN configuration can be overridden by a RADIUS authentication that assigns a VLAN. (Refer to figure 13-1 on page 13-11.)

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 membership in both VLANs is untagged, and the switch allows only one untagged, port-based 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 13-31.)
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. In the case of the multiple clients allowed on switches covered in this guide, the first client to authenticate determines the untagged VLAN membership for the port until all clients have disconnected. Any other clients that cannot operate in that VLAN are blocked at that point. • Port membership in a VLAN assigned to operate as the Authorized-Client VLAN ends when the client disconnects from the port.If a VLAN assignment from a RADIUS server is used instead, the same rule applies. In the case of the multiple clients allowed on switches, the port maintains the same VLAN as long as there is any authenticated client using the VLAN. When the last client disconnects, then the port reverts to only the VLAN(s) for which it is statically configured as a member.

Condition	Rule
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 any other VLANs.) • If the client disconnects, the port leaves the Unauthorized-Client VLAN and re-acquires membership in all the statically configured VLANs to which it belongs. • If the client becomes authenticated, the port leaves the Unauthenticated-Client VLAN and joins the appropriate VLAN. (Refer to "VLAN Membership Priorities" on page 13-30. • In the case of the multiple clients allowed on switches, if an authenticated client is already using the port for a different VLAN, then any other unauthenticated clients needing to use the Unauthorized-Client VLAN are blocked.
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 13-31.) **Note:** This rule assumes: • No alternate VLAN has been assigned by a RADIUS server. • No other authenticated clients are already using the port.
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-client VLAN 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 This rule assumes no other authenticated clients are already using the port on a different VLAN.	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.)

Condition	Rule
Effect of RADIUS-assigned VLAN This rule assumes no other authenticated clients are already using the port on a different VLAN.	The port joins the RADIUS-assigned VLAN as an untagged member.
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 use a manually configured 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.
Switch with a Port Configured To Allow Multiple Authorized-Client Sessions	When a new client is authenticated on a given port: • If no other clients are authenticated on that port, then the port joins one VLAN in the following order of precedence: a. A RADIUS-assigned VLAN, if configured. b. An Authenticated-Client VLAN, if configured. c. A static, port-based VLAN to which the port belongs as an untagged member. d. Any VLAN(s) to which the port is configured as a tagged member (provided that the client can operate in that VLAN). • If another client is already authenticated on the port, then the port is already assigned to a VLAN for the previously-existing client session, and the new client must operate in this same VLAN, regardless of other factors. (This means that a client without 802.1X client authentication software cannot access a configured, Unauthenticated-Client VLAN if another, authenticated client is already using the port.)

Condition	Rule
Note: Limitation on Using an Unauthorized-Client VLAN on an 802.1X Port Configured to Allow Multiple-Client Access	You can optionally enable switches to allow up to 32 clients per-port. The Unauthorized-Client VLAN feature can operate on an 802.1X-configured port regardless of how many clients the port is configured to support. However, all clients on the same port must operate through the same untagged VLAN membership. This means that any client accessing a given port must be able to authenticate and operate on the same VLAN as any other previously authenticated clients that are currently using the port. Thus, an Unauthorized-Client VLAN configured on a switch port that allows multiple 802.1X clients cannot be used if there is already an authenticated client using the port on another VLAN. Also, a client using the Unauthenticated-Client VLAN will be blocked when another client becomes authenticated on the port. For this reason, the best utilization of the Unauthorized-Client VLAN feature is in instances where only one client is allowed per-port. Otherwise, unauthenticated clients are subject to being blocked at any time by authenticated clients using a different VLAN. (Using the same VLAN for authenticated and unauthenticated clients can create a security risk and is not recommended.)

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.

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 13-2 on page 13-32 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 port-control parameter is set to **auto** (the default). (Refer to "1. Enable 802.1X Authentication on Selected Ports" on page 13-19.) 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 < *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.

   Syntax: 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-Authenticated Devices” on page 13-45.

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 13-40.

Syntax: aaa port-access authenticator < *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 13-61.

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", 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. (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 the only authenticated client on a port 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. If there are multiple clients authenticated on the port, if one client loses access and attempts to re-authenticate, that client will be handled as a new client on the port.

- The first client to authenticate on a port configured to support multiple clients will determine the port's VLAN membership for any subsequent clients that authenticate while an active session is already in effect.

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

If 802.1X authentication is disabled on a port or set to **authorized** (Force Authorize), the port can allow access to a non-authenticated client. Port-Security operates with 802.1X authentication only if the selected ports are configured as 802.1X *with* the **control** mode in the port-access authenticator command set to **auto** (the default setting). For example, if port A10 was at a non-default 802.1X setting and you wanted to configure it to support the port-security option, you would use the following **aaa port-access** command:

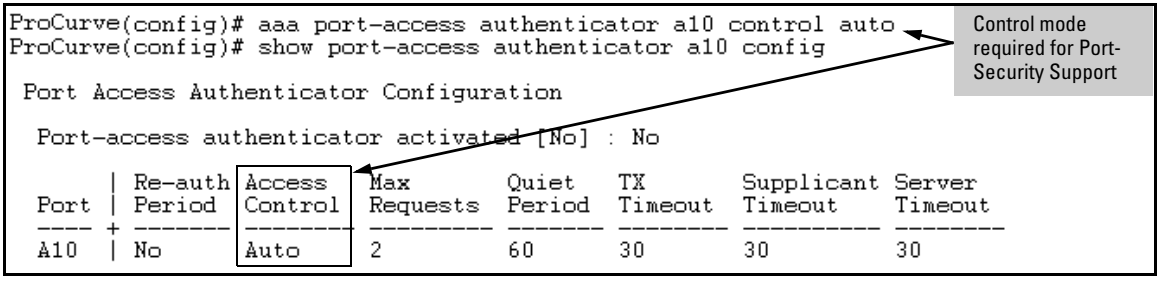


Figure 13-8. Port-Access Support for Port-Security Operation

Port-Security

Note

If 802.1X port-access is configured on a given port, then port-security **learn-mode** for that port must be set to either **continuous** (the default) or **port-access**.

In addition to the above, to use port-security on an authenticator port (chapter 14), use the per-port **client-limit** option to control how many MAC addresses of 802.1X-authenticated devices the port is allowed to learn. (Using **client-limit** sets 802.1X to user-based operation on the specified ports.) When this limit is reached, no further devices can be authenticated until a currently authenticated device disconnects and the current delay period or logoff period has expired.

Configure the port access type.

Syntax: aaa port-access auth < *port-list* > client-limit < 1 - 32 >

Configures user-based 802.1X authentication on the specified ports and sets the number of authenticated devices the port is allowed to learn. For more on this command, refer to "Configuring Switch Ports as 802.1X Authenticators" on page 13-18.)

— Or —

no aaa port-access auth < *port-list* > client-limit

Configures port-based 802.1X authentication on the specified ports, which opens the port. (Refer to "User Authentication Methods" on page 13-4.)

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

A switch port can 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. (A port can operate as both an authenticator and a supplicant.)

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”.

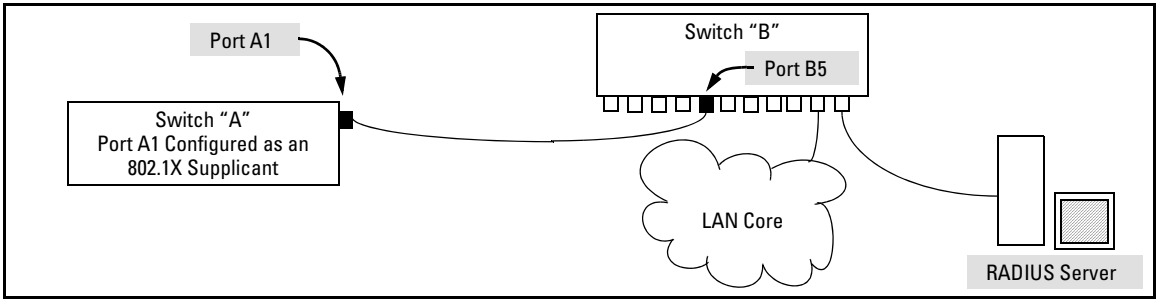


Figure 13-9. Example of Supplicant Operation

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 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, the authenticator compares the switch “A” response to its local username and password.

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.

Supplicant Port Configuration

Enabling a Switch Port as a Supplicant. You can configure a switch port as a supplicant for a point-to-point link to an 802.1X-aware port on another switch. *Configure the port as a supplicant before configuring any supplicant-related parameters.*

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

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

Configuring a Supplicant Switch Port. You must enable supplicant operation on a port before changing 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 credentials 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 opertion. (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 due 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. (Default: Null.)*

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

[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.

[auth-timeout < 1 - 300 >]

Sets the delay period the port waits to receive a challenge from the authenticator. If the request times out, the port sends another 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 13-47 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 delay 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

Show Commands for Port-Access Authenticator

Syntax: show port-access authenticator [*port-list*]
[config | statistics | session-counters | vlan | clients [detailed]]

If you enter the **show port-access authenticator** *command without an optional value, the following configuration information is displayed for all switch ports, or specified ports, that are enabled for 802.1X port-access authentication:*

- **Port -access authenticator activated***: Are any switch ports configured to operate as 802.1X authenticators using the* **aaa port-access authenticator** *command?* **Yes** *or* **No**
- **Allow RADIUS-assigned dynamic (GVRP) VLANs***: Are RADIUS-assigned dynamic (GVRP-learned) VLANs supported for authenticated and unauthenticated client sessions on the switch?* **Yes** *or* **No**
- **Auth Clients***: Number of authorized clients*
- **Unauth Clients***: Number of unauthorized clients*

Syntax: show port-access authenticator [*port-list*]
[config | statistics | session-counters | vlan | clients | clients detailed
—Continued—

- **Untagged VLAN***: VLAN ID number of the untagged VLAN used in client sessions. If the switch supports MAC-based (untagged) VLANs,* **MACbased** *is displayed to show that multiple untagged VLANs are configured for authentication sessions.*
- **Tagged VLANs***: Are tagged VLANs (statically configured or RADIUS-assigned) used for authenticated clients?* **Yes** *or* **No**
- **Port COS***:*
  Yes - *Client-specific CoS (Class of Service) values are applied to more than one authenticated client on the port.*
  No *- No client-specific CoS values are applied to any authenticated client on the port.*
  <***cos-value***>*- Numerical value of the CoS (802.1p priority) applied to inbound traffic from one authenticated client. For client-specific per-port CoS values, enter the* **show port-access web-based clients detailed** *command.*
- **% In Limit***:*
  Yes - *Per-port rate-limiting is applied to inbound traffic from more than one authenticated client.*
  No - *Per-port rate-limiting is not applied to any authenticated client session.*
  <***rate-limit-value***>*- Percentage value of a port's bandwidth applied as a rate limit to one authenticated client.*
- **RADIUS ACL***: Are RADIUS-assigned ACLs used for authenticated clients?* **Yes** *or* **No**

Information on ports not enabled for 802.1X port-access authentication is not displayed.

```
ProCurve(config)# show port-access authenticator

 Port Access Authenticator Status

  Port-access authenticator activated [No] : Yes
  Allow RADIUS-assigned dynamic (GVRP) VLANs [No] : Yes

       Auth    Unauth    | Untagged Tagged Port     % In  RADIUS
  Port Clients Clients   | VLAN     VLANs  COS      Limit ACL
  ---- ------- -------- + -------- ------ -------- ----- ------
  1    1       1        | 4006     Yes    70000000 100   Yes
  2    2       0        | MACbased No     Yes      Yes   Yes
  3    4       0        | 1        Yes    No       No    No
  ...
```

Figure 13-10.Example of show port-access authenticator Command

The information displayed with the **show port-access authenticator** command for individual (config | statistics | session-counters | vlan | clients) options is described below.

Syntax: show port-access authenticator config [*port-list*]

Displays 802.1X port-access authenticator configuration settings, including:

- *Whether port-access authentication is enabled*
- *Whether RADIUS-assigned dynamic VLANs are supported*
- *802.1X configuration of ports that are enabled as 802.1X authenticators (For a description of each setting, refer to the syntax descriptions in "2. Reconfigure Settings for Port-Access" on page 13-21. Use the* **show running** *command to view the current* **client-limit** *configuration available for switches.)*

You can display 802.1X port-access authenticator configuration for all switch ports or specified ports.

802.1X configuration information for ports that are not enabled as 802.1X authenticators is not displayed.

```
ProCurve(config)# show port-access authenticator config

 Port Access Authenticator Configuration

Port-access authenticator activated [No] : Yes
Allow RADIUS-assigned dynamic (GVRP) VLANs [No] : No

      | Re-auth Access   Max   Quiet   TX       Supplicant Server   Cntrl
 Port | Period  Control  Reqs  Period  Timeout  Timeout    Timeout  Dir
 ---- + ------- -------- ----- ------- -------- ---------- -------- -----
 1    | No      Auto     2     60      30       30         30       both
 2    | No      Auto     2     60      30       30         30       in
 ...
```

Figure 13-11.Example of show port-access authenticator config Command

Table 13-3. Field Descriptions of show port-access authenticator config Command Output (Figure 13-11)

Field	Description
Port-access authenticator activated	Whether 802.1X authentication is enabled or disabled on specified port(s).
Port	Port number on switch.
Re-auth Period	Period of time (in seconds) after which clients connected to the port need to be re-authenticated.
Access Control	Port's authentication mode: **Auto:** Network access is allowed to any connected device that supports 802.1X authentication and provides valid 802.1X credentials. **Authorized:** Network access is allowed to any device connected to the port, regardless of whether it meets 802.1X criteria. **Unauthorized:** Network access is blocked to any device connected to the port, regardless of whether the device meets 802.1X criteria.
Max reqs	Number of authentication attempts that must time-out before authentication fails and the authentication session ends.
Quiet Period	Period of time (in seconds) during which the port does not try to acquire a supplicant.
TX Timeout	Period of time (in seconds) that the port waits to retransmit the next EAPOL PDU during an authentication session.
Supplicant Timeout	Period of time (in seconds) that the switch waits for a supplicant response to an EAP request.
Server Timeout	Period of time (in seconds) that the switch waits for a server response to an authentication request.
Cntrl Dir	Directions in which flow of incoming and outgoing traffic is blocked on 802.1X-aware port that has not yet entered the authenticated state: **Both:** Incoming and outgoing traffic is blocked on port until authentication occurs. **In:** Only incoming traffic is blocked on port before authentication occurs. Outgoing traffic with unknown destination addresses is flooded on the unauthenticated 802.1X-aware port.

Syntax: show port-access authenticator statistics [*port-list*]

Displays statistical information for all switch ports or specified ports that are enabled as 802.1X authenticators, including:

- *Whether port-access authentication is enabled*
- *Whether RADIUS-assigned dynamic VLANs are supported*
- *802.1X supplicant's MAC address as determined by the content of the last EAPOL frame received on the port*
- *802.1X traffic statistics from received and transmitted packets*

802.1X configuration information for ports that are not enabled as an 802.1X authenticators is not displayed.

```
ProCurve(config)# show port-access authenticator statistics

 Port Access Authenticator Statistics

  Port-access authenticator activated [No] : Yes
  Allow RADIUS-assigned dynamic (GVRP) VLANs [No] : No

       Source           TX     TX    RX     RX      RX      RX    RX
  Port MAC address      ReqId  Req   Start  Logoff  RespId  Resp  Errors
  ---- -------------    ------ ----- ------ ------- ------- ----- -------
  2    001560-b3ea48  1      0     0      0       0       0     0
```

Figure 13-12.Example of show port-access authenticator statistics Command

Syntax: show port-access authenticator session-counters [*port-list*]

Displays information for active 802.1X authentication sessions on all switch ports or specified ports that are enabled as 802.1X authenticators, including:

- *802.1X frames received and transmitted on each port*
- *Duration and status of active 802.1X authentication sessions (***in-progress** *or* **terminated***)*
- *User name of 802.1X supplicant included in 802.1X response packets, configured with the* **aaa port-access supplicant identity** *<username> command (see page 13-49).*

802.1X configuration information for ports that are not enabled as an 802.1X authenticators is not displayed.

```
ProCurve(config)# show port-access authenticator session-counters

 Port Access Authenticator Session Counters

  Port-access authenticator activated [No] : Yes
  Allow RADIUS-assigned dynamic (GVRP) VLANs [No] : No

                               Session     Session
  Port Frames In  Frames Out  Time(sec.)  Status      User
  ---- ---------- ----------- ----------- ----------- -------
  2     45623     45623       20          in-progress bert
```

Figure 13-13.Example of show port-access authenticator session-counters Command

Syntax: show port-access authenticator vlan [*port-list*]

Displays the following information on the VLANs configured for use in 802.1X port-access authentication on all switch ports, or specified ports, that are enabled as 802.1X authenticator:

- *Authentication mode used on each port, configured with the* **aaa port-access authenticator control** *command (see page 13-21)*
- *VLAN ID (if any) to be used for traffic from 802.1X-authenticated clients*
- *VLAN ID (if any) to be used for traffic from unauthenticated clients*

802.1X configuration information for ports that are not enabled as an 802.1X authenticators is not displayed.

```
ProCurve(config)# show port-access authenticator vlan

 Port Access Authenticator VLAN Configuration

  Port-access authenticator activated [No] : Yes
  Allow RADIUS-assigned dynamic (GVRP) VLANs [No] : No

       Access   Unauth   Auth
  Port Control  VLAN ID  VLAN ID
  ---- -------- -------- --------
  2    Auto     0        0
```

Figure 13-14.Example of show port-access authenticator vlan Command

Syntax: show port-access authenticator clients [*port-list*]

Displays the session status, name, and address for each 802.1X port-access-authenticated client on the switch. Multiple authenticated clients may be displayed for the same port. The IP address displayed is taken from the DHCP binding table (learned through the DHCP Snooping feature).

- *If DHCP snooping is not enabled on the switch,* **n/a** *(not available) is displayed for a client's IP address.*
- *If an 802.1X-authenticated client uses an IPv6 address,* **n/a - IPv6** *is displayed.*
- *If DHCP snooping is enabled but no MAC-to-IP address binding for a client is found in the DHCP binding table,* **n/a - no info** *is displayed.*

```
ProCurve (config)# show port-access authenticator clients

 Port Access Authenticator Client Status

Port  Client Name  MAC Address    IP Address      Session Status
----- ------------ -------------  --------------- --------------
1     webuser1     001321-eb8063  192.192.192.192 Authenticated
1     webuser2     001560-b3ea48  n/a - no info   Authenticating
1     webuser3     000000-111111  n/a - IPv6      Authenticating
3     webuser4     000000-111112  n/a             Authenticating
```

Figure 13-15. Example of show port-access authenticator clients Command Output

Syntax: show port-access authenticator clients <*port-list*> detailed

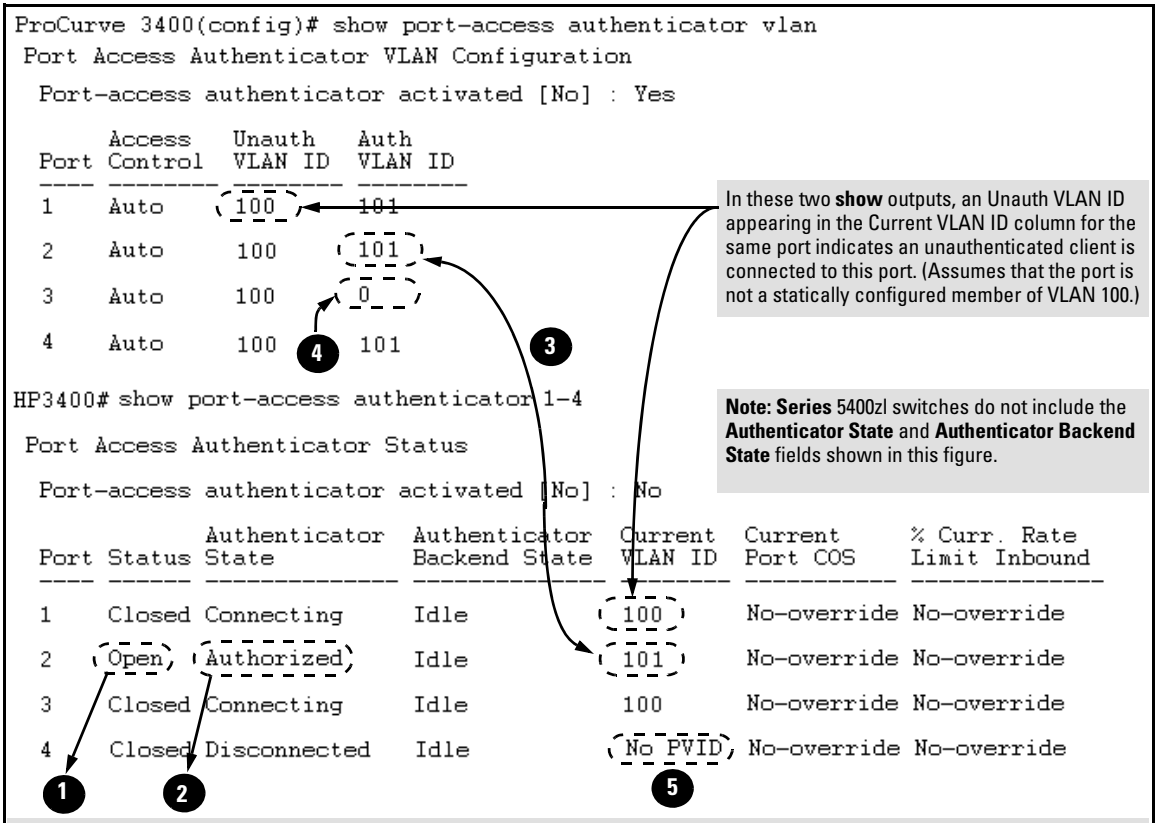
Displays detailed information on the status of 802.1X-authenticated client sessions on specified ports.

```
ProCurve (config)# show port-access authenticator clients 5 detailed

 Port Access Authenticator Client Status Detailed

  Client Base Details :
   Port           : 5
   Session Status : Open             Session Time(sec) : 999999999
   Frames In      : 999999999        Frames Out        : 99999999
   Username       : webuser1         MAC Address       : 001321-eb8063
   IP             : 2001:fecd:ba23:cd1f:dcb1:1010:9234:4088

  Access Policy Details :
   COS Map        : 70000000         In Limit %        : 87
   Untagged VLAN  : 3096             Out Limit %       : 100
   Tagged VLANs   : 1, 3, 5, 6, 334, 2066
   RADIUS-ACL List :
     deny in udp from any to 10.2.8.233 CNT
        Hit Count: 0
     permit in udp from any to 10.2.8.233 CNT
        Hit Count: 0
     deny in tcp from any to 10.2.8.233 CNT
        Hit Count: 0
     permit in tcp from any to 10.2.8.233 CNT
        Hit Count: 0
     permit in tcp from any to 0.0.0.0/0 CNT
        Hit Count: 0
```

Figure 13-16. Example of show port-access authenticator clients detailed Command Output

Viewing 802.1X Open VLAN Mode Status

You can examine the switch's current VLAN status by using the **show port-access authenticator vlan** and **show port-access authenticator < *port-list* >** commands as illustrated in figure 13-17. Table 13-2 describes the data that these two commands display. Figure 13-18 shows related VLAN data that can help you to see how the switch is using statically configured VLANs to support 802.1X operation.



Items 1 through 3 indicate that an authenticated client is connected to port 2:

1. **Open** in the Status column
2. **Authorized** in the Authenticator State column
3. The Auth VLAN ID (**101**) is also in the Current VLAN ID column. (This assumes that the port is not a statically configured member of VLAN 101.)
4. A "0" in the row for port 3 indicates there is no Authorized VLAN configured for port 3.
5. No PVID" means there is currently no untagged VLAN membership on port 4.

Figure 13-17. Example Showing Ports Configured for Open VLAN Mode

Thus, in the output shown in figure 13-17:

- When the **Auth VLAN ID** is configured and matches the **Current VLAN ID**, 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**, 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 12 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 13-1. Output for Determining Open VLAN Mode Status (Figure 13-17, Upper)

Status Indicator	Meaning
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.) **Authorized:** 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.) **Unauthorized:** 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.
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.

Table 13-3. Output for Determining Open VLAN Mode Status (Figure 13-17, Lower)

Status Indicator	Meaning
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.
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.
Current Port CoS **% Curr. Rate Limit Inbound**	*Refer to the section describing RADIUS support for Identity-Driven Management—IDM—in chapter 6, "RADIUS Authentication and Accounting" in this guide.*

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.

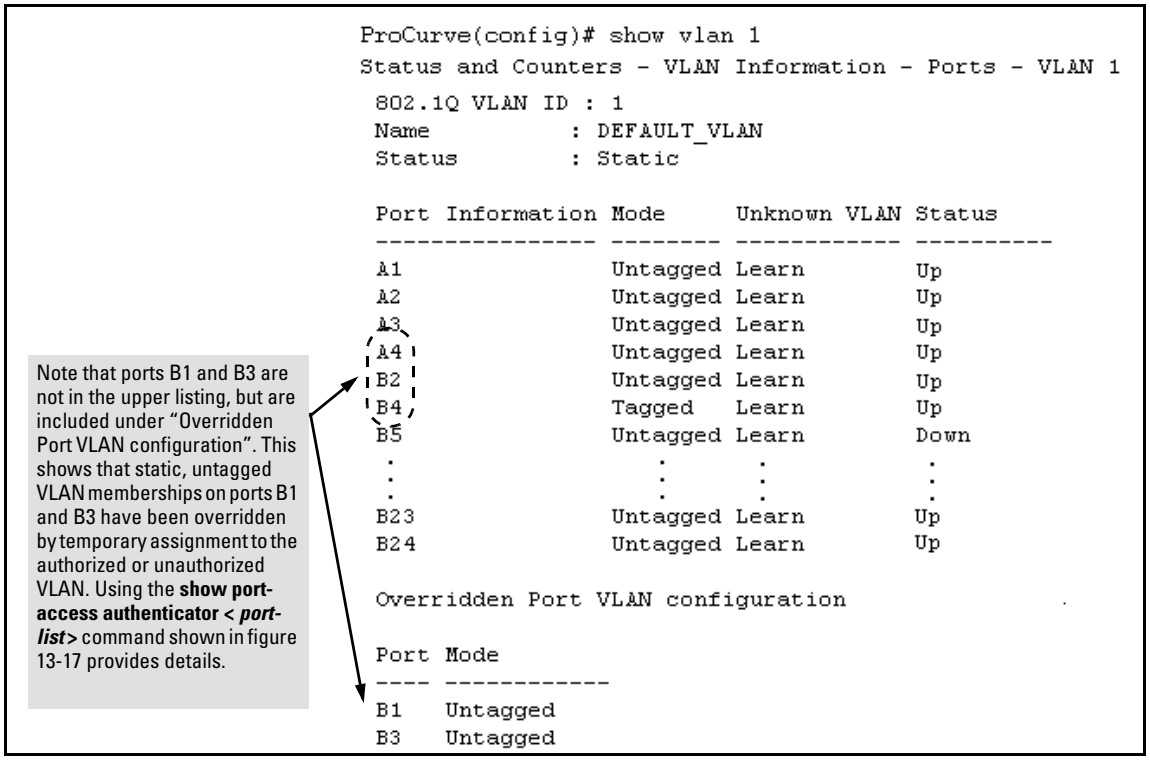


Figure 13-18.Example of Showing a VLAN with Ports Configured for Open VLAN Mode

Show Commands for Port-Access Supplicant

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

show port-access supplicant [< *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 13-49).*

For descriptions of the supplicant parameters, refer to "Configuring a Supplicant Switch Port" on page 13-49.

show port-access supplicant [< *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 < *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 < *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.)

Using a RADIUS server to authenticate clients, you can provide port-level security protection from unauthorized network access for the following authentication methods:

- 802.1X: Port-based or client-based access control to open a port for client access after authenticating valid user credentials.
- MAC address: Authenticates a device's MAC address to grant access to the network.
- Web-browser interface: Authenticates clients for network access using a web page for user login.

Note

You can use 802.1X (port-based or client-based) authentication and either Web or MAC authentication at the same time on a port, with a maximum of 32 clients allowed on the port. (The default is one client.) Web authentication and MAC authentication are mutually exclusive on the same port. Also, you must disable LACP on ports configured for any of these authentication methods. For more information, see "Web and MAC Authentication" on page 4-1 in this guide.

VLAN Assignment on a Port

Following client authentication, VLAN configurations on a port are managed as follows when you use 802.1X, MAC, or Web authentication:

- The port resumes membership in any tagged VLANs for which it is already assigned in the switch configuration. Tagged VLAN membership allows a port to be a member of multiple VLANs simultaneously.
- The port is temporarily assigned as a member of an untagged (static or dynamic) VLAN for use during the client session according to the following order of options.
  a. The port joins the VLAN to which it has been assigned by a RADIUS server during client authentication.
  b. If RADIUS authentication does not include assigning the port to a VLAN, then the switch assigns the port to the authorized-client VLAN configured for the authentication method.
  c. If the port does not have an authorized-client VLAN configured, but is configured for membership in an untagged VLAN, the switch assigns the port to this untagged VLAN.

Operating Notes

- During client authentication, a port assigned to a VLAN by a RADIUS server or an authorized-client VLAN configuration is an untagged member of the VLAN for the duration of the authenticated session. This applies even if the port is also configured in the switch as a tagged member of the same VLAN. The following restrictions apply:
  - If the port is assigned as a member of an untagged *static* VLAN, the VLAN must already be configured on the switch. If the static VLAN configuration does not exist, the authentication fails.

- If the port is assigned as a member of an untagged *dynamic* VLAN that was learned through GVRP, the dynamic VLAN configuration must exist on the switch at the time of authentication and GVRP-learned dynamic VLANs for port-access authentication must be enabled.

  If the dynamic VLAN does not exist or if you have not enabled the use of a dynamic VLAN for authentication sessions on the switch, the authentication fails.

- To enable the use of a GVRP-learned (dynamic) VLAN as the untagged VLAN used in an authentication session, enter the **aaa port-access gvrp-vlans** command, as described in "Enabling the Use of GVRP-Learned Dynamic VLANs in Authentication Sessions" on page 13-72.
- Enabling the use of dynamic VLANs in an authentication session offers the following benefits:
  - You avoid the need of having static VLANs pre-configured on the switch.
  - You can centralize the administration of user accounts (including user VLAN IDs) on a RADIUS server.

  For information on how to enable the switch to dynamically create 802.1Q-compliant VLANs on links to other devices using the GARP VLAN Registration Protocol (GVRP), see the chapter on "GVRP" in the *Advanced Traffic Management Guide*.
- For an authentication session to proceed, a port must be an untagged member of the (static or dynamic) VLAN assigned by the RADIUS server (or an authorized-client VLAN configuration). The port temporarily drops any current untagged VLAN membership.

  If the port is not already a member of the RADIUS-assigned (static or dynamic) untagged VLAN, the switch temporarily reassigns the port as an untagged member of the required VLAN (for the duration of the session). *At the same time, if the port is already configured as an untagged member of a different VLAN, the port loses access to the other VLAN for the duration of the session.* (A port can be an untagged member of only one VLAN at a time.)

  When the authentication session ends, the switch removes the temporary untagged VLAN assignment and re-activates the temporarily disabled, untagged VLAN assignment.
- If GVRP is already enabled on the switch, the temporary untagged (static or dynamic) VLAN created on the port for the authentication session is advertised as an existing VLAN.

If this temporary VLAN assignment causes the switch to disable a different untagged static or dynamic VLAN configured on the port (as described in the preceding bullet and in "Example of Untagged VLAN Assignment in a RADIUS-Based Authentication Session" on page 13-69), the disabled VLAN assignment is not advertised. When the authentication session ends, the switch:

- Removes the temporary untagged VLAN assignment and stops advertising it.
- Re-activates and resumes advertising the temporarily disabled, untagged VLAN assignment.

- If you modify a VLAN ID configuration on a port during an 802.1X, MAC, or Web authentication session, the changes do not take effect until the session ends.
- When a switch port is configured with RADIUS-based authentication to accept multiple 802.1X and/or MAC or Web authentication client sessions, all authenticated clients must use the same port-based, untagged VLAN membership assigned for the earliest, currently active client session.

  Therefore, on a port where one or more authenticated client sessions are already running, all such clients are on the same untagged VLAN. If a RADIUS server subsequently authenticates a new client, but attempts to re-assign the port to a different, untagged VLAN than the one already in use for the previously existing, authenticated client sessions, the connection for the new client will fail.

Example of Untagged VLAN Assignment in a RADIUS-Based Authentication Session

The following example shows how an untagged static VLAN is temporarily assigned to a port for use during an 802.1X authentication session. In the example, an 802.1X-aware client on port A2 has been authenticated by a RADIUS server for access to VLAN 22. However, port A2 is not configured as a member of VLAN 22 but as a member of untagged VLAN 33 as shown in Figure 13-19.

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:

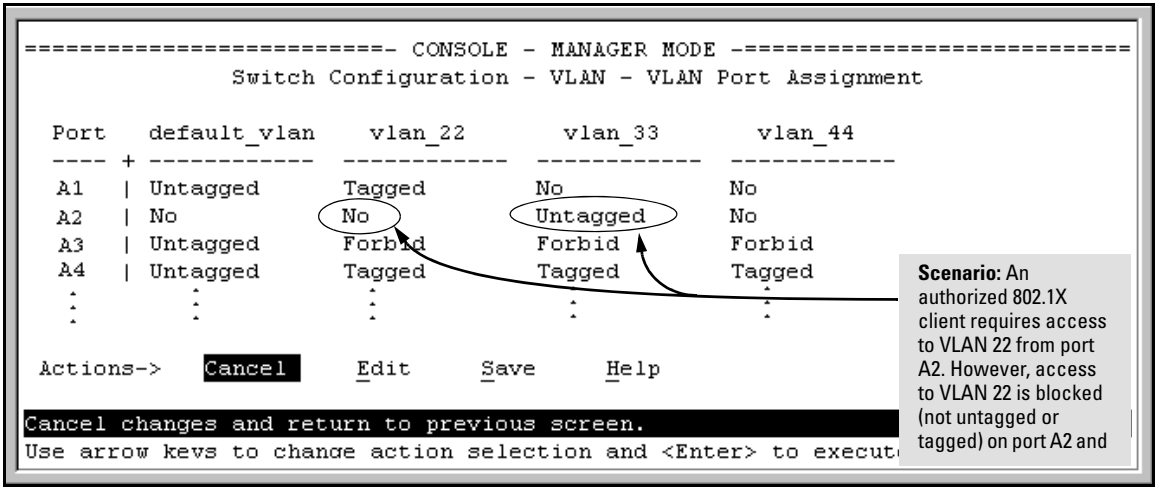


Figure 13-19.Example of an Active VLAN Configuration

In Figure 13-19, if RADIUS authorizes an 802.1X client on port A2 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).

To view the temporary VLAN assignment as a change in the active configuration, use the **show vlan <*vlan-id*>** command as shown in Figure 13-18 where **<*vlan-id*>** is the (static or dynamic) VLAN used in the authenticated client session.

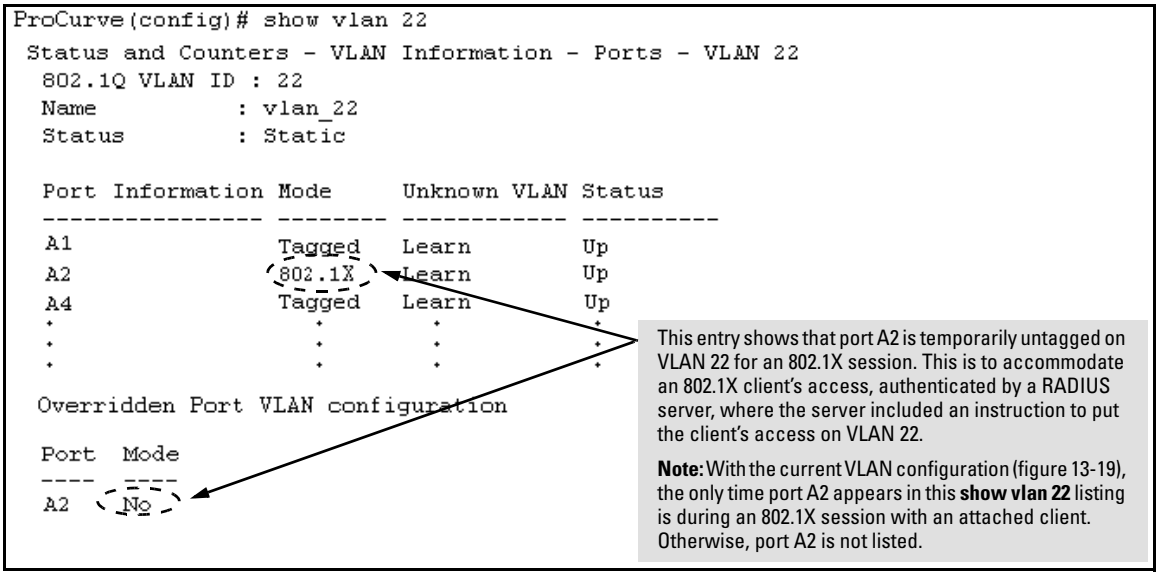


Figure 13-20.The Active Configuration for VLAN 22 Temporarily Changes for the 802.1X Session

However, as shown in Figure 13-19, because VLAN 33 is configured as untagged on port A2 and because a port can be untagged on only one VLAN, port A2 loses access to VLAN 33 for the duration of the 802.1X session on VLAN 22.

You can verify the temporary loss of access to VLAN 33 by entering the **show vlan 33** command as shown in Figure 13-21.

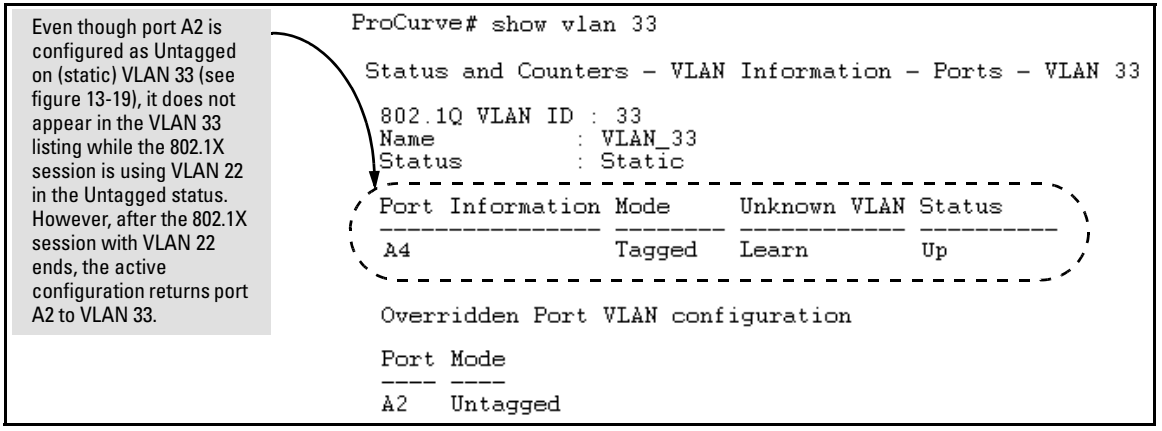


Figure 13-21.The Active Configuration for VLAN 33 Temporarily Drops Port 22 for the 802.1X Session

When the 802.1X client's session on port A2 ends, the port removes the temporary untagged VLAN membership. The static VLAN (VLAN 33) that is "permanently" configured as untagged on the port becomes available again. Therefore, 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 as shown in Figure 13-22.

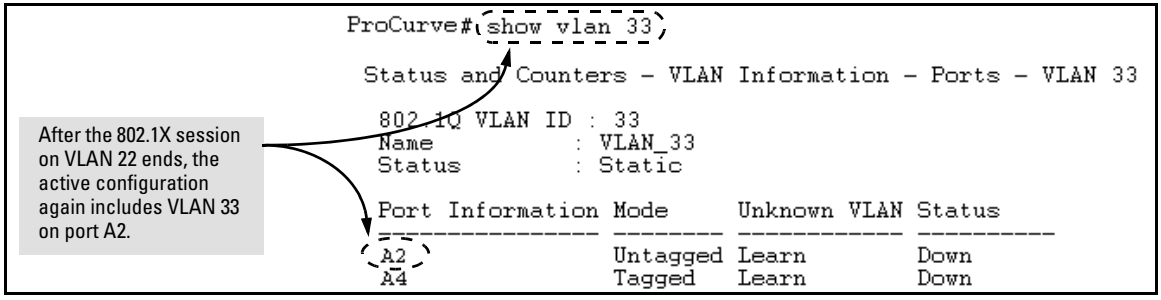


Figure 13-22.The Active Configuration for VLAN 33 Restores Port A2 After the 802.1X Session Ends

Enabling the Use of GVRP-Learned Dynamic VLANs in Authentication Sessions

Syntax: aaa port-access gvrp-vlans

Enables the use of dynamic VLANs (learned through GVRP) in the temporary untagged VLAN assigned by a RADIUS server on an authenticated port in an 802.1X, MAC, or Web authentication session.

Enter the **no** *form of this command to disable the use of GVRP-learned VLANs in an authentication session.*

For information on how to enable a switch to dynamically create 802.1Q-compliant VLANs, see the chapter on "GVRP" in the Advanced Traffic Management Guide.

Notes*:*

1. If a port is assigned as a member of an untagged dynamic VLAN, the dynamic VLAN configuration must exist at the time of authentication and GVRP for port-access authentication must be enabled on the switch.

If the dynamic VLAN does not exist or if you have not enabled the use of a dynamic VLAN for authentication sessions on the switch, the authentication fails.

Syntax: aaa port-access gvrp-vlans
—Continued—

2. After you enable dynamic VLAN assignment in an authentication session, it is recommended that you use the **interface unknown-vlans** *command on a per-port basis to prevent denial-of-service attacks. The* **interface unknown-vlans** *command allows you to:*

- *Disable the port from sending advertisements of existing GVRP-created VLANs on the switch.*
- *Drop all GVRP advertisements received on the port.*

For more information, refer to the chapter on "GVRP" in the Advanced Traffic Management Guide.

3. If you disable the use of dynamic VLANs in an authentication session using the **no aaa port-access gvrp-vlans** *command, client sessions that were authenticated with a dynamic VLAN continue and are not deauthenticated.*

(This behavior differs form how static VLAN assignment is handled in an authentication session. If you remove the configuration of the static VLAN used to create a temporary client session, the 802.1X, MAC, or Web authenticated client is deauthenticated.)

However, if a RADIUS-configured dynamic VLAN used for an authentication session is deleted from the switch through normal GVRP operation (for example, if no GVRP advertisements for the VLAN are received on any switch port), authenticated clients using this VLAN are deauthenticated.

Note

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 13-4. 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 as a Supplicant" on page 13-49.
`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 6-53).
`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.