Chapter 4
Configuring 802.1X Port Security

Overview

HP devices support the IEEE 802.1X standard for authenticating devices attached to LAN ports. Using 802.1X port security, you can configure an HP device to grant access to a port based on information supplied by a client to an authentication server.

When a user logs on to a network that uses 802.1X port security, the HP device grants (or doesn't grant) access to network services after the user is authenticated by an authentication server. The user-based authentication in 802.1X port security provides an alternative to granting network access based on a user's IP address, MAC address, or subnetwork.

This chapter is divided into the following sections:

- “How 802.1X Port Security Works” on page 4-1 explains basic concepts about 802.1X port security.
- “Configuring 802.1X Port Security” on page 4-9 describes how to set up 802.1X port security on HP devices using the Command Line Interface (CLI).
- “Displaying 802.1X Information” on page 4-18 describes the commands used to display information about an 802.1X port security configuration.
- “Sample 802.1X Configurations” on page 4-28 shows diagrams of two 802.1X port security configurations and the CLI commands used for implementing them.

IETF RFC Support

HP’s implementation of 802.1X port security supports the following RFCs:

- RFC 2284 PPP Extensible Authentication Protocol (EAP)
- RFC 2865 Remote Authentication Dial In User Service (RADIUS)
- RFC 2869 RADIUS Extensions

How 802.1X Port Security Works

This section explains the basic concepts behind 802.1X port security, including device roles, how the devices communicate, and the procedure used for authenticating clients.

Device Roles in an 802.1X Configuration

The 802.1X standard defines the roles of Client/Supplicant, Authenticator, and Authentication Server in a network.
The Client (known as a **Supplicant** in the 802.1X standard) provides username/password information to the Authenticator. The Authenticator sends this information to the Authentication Server. Based on the Client’s information, the Authentication Server determines whether the Client can use services provided by the Authenticator. The Authentication Server passes this information to the Authenticator, which then provides services to the Client, based on the authentication result.

Figure 4.1 illustrates these roles.

**Figure 4.1 Authenticator, Client/Supplicant, and Authentication Server in an 802.1X configuration**

---

**Authenticator** – The device that controls access to the network. In an 802.1X configuration, the HP device serves as the Authenticator. The Authenticator passes messages between the Client and the Authentication Server. Based on the identity information supplied by the Client, and the authentication information supplied by the Authentication Server, the Authenticator either grants or does not grant network access to the Client.

**Client/Supplicant** – The device that seeks to gain access to the network. Clients must be running software that supports the 802.1X standard (for example, the Windows XP operating system). Clients can either be directly connected to a port on the Authenticator, or can be connected by way of a hub.

**Authentication Server** – The device that validates the Client and specifies whether or not the Client may access services on the device. HP supports Authentication Servers running RADIUS.

**Communication Between the Devices**

For communication between the devices, 802.1X port security uses the **Extensible Authentication Protocol** (EAP), defined in RFC 2284. The 802.1X standard specifies a method for encapsulating EAP messages so that they can be carried over a LAN. This encapsulated form of EAP is known as EAP over LAN (EAPOL). The standard also specifies a means of transferring the EAPOL information between the Client/Supplicant, Authenticator, and Authentication Server.
EAPOL messages are passed between the **Port Access Entity (PAE)** on the Supplicant and the Authenticator. Figure 4.2 shows the relationship between the Authenticator PAE and the Supplicant PAE.

**Figure 4.2 Authenticator PAE and Supplicant PAE**

**Authenticator PAE** – The Authenticator PAE communicates with the Supplicant PAE, receiving identifying information from the Supplicant. Acting as a RADIUS client, the Authenticator PAE passes the Supplicant's information to the Authentication Server, which decides whether the Supplicant can gain access to the port. If the Supplicant passes authentication, the Authenticator PAE grants it access to the port.

**Supplicant PAE** – The Supplicant PAE supplies information about the Client to the Authenticator PAE and responds to requests from the Authenticator PAE. The Supplicant PAE can also initiate the authentication procedure with the Authenticator PAE, as well as send logoff messages.

**Controlled and Uncontrolled Ports**

A physical port on the device used with 802.1X port security has two virtual access points: a **controlled** port and an **uncontrolled** port. The controlled port provides full access to the network. The uncontrolled port provides access only for EAPOL traffic between the Client and the Authentication Server. When a Client is successfully authenticated, the controlled port is opened to the Client. Figure 4.3 illustrates this concept.
Before a Client is authenticated, only the uncontrolled port on the Authenticator is open. The uncontrolled port allows only EAPOL frames to be exchanged between the Client and the Authentication Server. The controlled port is in the unauthorized state and allows no traffic to pass through.

During authentication, EAPOL messages are exchanged between the Supplicant PAE and the Authenticator PAE, and RADIUS messages are exchanged between the Authenticator PAE and the Authentication Server. See “Message Exchange During Authentication” on page 4-4 for an example of this process. If the Client is successfully authenticated, the controlled port becomes authorized, and traffic from the Client can flow through the port normally.

By default, all controlled ports on the HP device are placed in the authorized state, allowing all traffic. When authentication is activated on an 802.1X-enabled interface, the interface's controlled port is placed initially in the unauthorized state. When a Client connected to the port is successfully authenticated, the controlled port is then placed in the authorized state until the Client logs off. See “Enabling 802.1X Port Security” on page 4-10 for more information.

**Message Exchange During Authentication**

Figure 4.4 illustrates a sample exchange of messages between an 802.1X-enabled Client, an HP device acting as Authenticator, and a RADIUS server acting as an Authentication Server.
In this example, the Authenticator (the HP device) initiates communication with an 802.1X-enabled Client. When the Client responds, it is prompted for a username (255 characters maximum) and password. The Authenticator passes this information to the Authentication Server, which determines whether the Client can access services provided by the Authenticator. When the Client is successfully authenticated by the RADIUS server, the port is authorized. When the Client logs off, the port becomes unauthorized again.

Starting in release 07.6.04, HP’s 802.1X implementation supports dynamic VLAN assignment. If one of the attributes in the Access-Accept message sent by the RADIUS server specifies a VLAN identifier, and this VLAN is available on the HP device, the client's port is moved from its default VLAN to the specified VLAN. When the client disconnects from the network, the port is placed back in its default VLAN. See “Configuring Dynamic VLAN Assignment for 802.1X Ports” on page 4-16 for more information.

If a Client does not support 802.1X, authentication cannot take place. The HP device sends EAP-Request/Identity frames to the Client, but the Client does not respond to them.

When a Client that supports 802.1X attempts to gain access through a non-802.1X-enabled port, it sends an EAP start frame to the HP device. When the device does not respond, the Client considers the port to be authorized, and starts sending normal traffic.

HP devices support Identity and MD5-challenge request types in EAP Request/Response messages. However, devices running software release 07.8.00 has support for the following 802.1X authentication challenge types:

- **EAP-TLS (RFC 2716)** – EAP Transport Level Security (TLS) provides strong security by requiring both client and authentication server to be identified and validated through the use of public key infrastructure (PKI) digital certificates. EAP-TLS establishes a tunnel between the client and the authentication server to protect messages from unauthorized users’ eavesdropping activities. Since EAP-TLS requires PKI digital certificates
on both the clients and the authentication servers, the roll out, maintenance, and scalability of this authentication method is much more complex than other methods. EAP-TLS is best for installations with existing PKI certificate infrastructures.

- **EAP-TTLS (Internet-Draft)** – The EAP Tunneled Transport Level Security (TTLS) is an extension of EAP-TLS. Like TLS, EAP-TTLS provides strong authentication; however, it requires only the authentication server to be validated by the client through a certificate exchange between the server and the client. Clients are authenticated by the authentication server using user names and passwords.

  A TLS tunnel can be used to protect EAP messages and existing user credential services such as Active Directory, RADIUS, and LDAP. Backward compatibility for other authentication protocols such as PAP, CHAP, MS-CHAP, and MS-CHAP-V2 are also provided by EAP-TTLS. EAP-TTLS is not considered foolproof and can be fooled into sending identity credentials if TLS tunnels are not used. EAP-TTLS is suited for installations that require strong authentication without the use of mutual PKI digital certificates.

- **PEAP (Internet-Draft)** – Protected EAP Protocol (PEAP) is an Internet-Draft that is similar to EAP-TTLS. PEAP client authenticates directly with the backend authentication server. The authenticator acts as a pass-through device, which does not need to understand the specific EAP authentication protocols.

  Unlike EAP-TTLS, PEAP does not natively support user name and password to authenticate clients against an existing user database such as LDAP. PEAP secures the transmission between the client and authentication server with a TLS encrypted tunnel. PEAP also allows other EAP authentication protocols to be used. It relies on the mature TLS keying method for its key creation and exchange. PEAP is best suited for installations that require strong authentication without the use of mutual certificates.

**NOTE:** If the 802.1X Client will be sending a packet that is larger than 1500 bytes, then the following must be configured on the HP device:

- On devices with EP modules, `default-mtu 1700` must be configured.
- On devices with Standard modules, `jumbo 1920` must be configured.

Configuration for these challenge types is the same as for the EAP-MD5 challenge type.

**Authenticating Multiple Hosts Connected to the Same Port**

HP devices support 802.1X authentication for ports with more than one host connected to them. Figure 4.5 illustrates a sample configuration where multiple hosts are connected to a single 802.1X port.
The way the HP device authenticates Clients in a multiple-host configuration depends on the software release running on the device:

- In releases prior to 07.8.00, services are provided on a port based on the authentication of a single Client. When one Client is successfully authenticated, all hosts connected to the port are allowed access to the network. The HP device forwards traffic from all of the connected hosts for as long as the authenticated Client stays connected. When the authenticated Client disconnects from the network, authentication is removed for the other connected hosts as well.

- Starting in release 07.8.00, if there are multiple hosts connected to a single 802.1X-enabled port, the HP device authenticates each of them individually. Each host’s authentication status is independent of the others, so that if one authenticated host disconnects from the network, it has no effect on the authentication status of any of the other authenticated hosts.

By default, traffic from hosts that cannot be authenticated by the RADIUS server is dropped in hardware. You can optionally configure the HP device to assign the port to a “restricted” VLAN if authentication of the Client is unsuccessful.

**How 802.1X Multiple-Host Authentication Works (Release 07.8.00 and Later)**

In release 07.8.00 and later, when multiple hosts are connected to a single 802.1X-enabled port on an HP device (as in Figure 4.5), 802.1X authentication is performed in the following way:

1. One of the 802.1X-enabled Clients attempts to log into a network in which an HP device serves as an Authenticator.
2. The HP device creates an internal session (called a dot1x-mac-session) for the Client. A dot1x-mac-session serves to associate a Client’s MAC address and username with its authentication status.
3. The HP device performs 802.1X authentication for the Client. Messages are exchanged between the HP device and the Client, and between the device and the Authentication Server (RADIUS server). The result of this process is that the Client is either successfully authenticated or not authenticated, based on the username and password supplied by the client.

4. If the Client is successfully authenticated, the Client's dot1x-mac-session is set to “access-is-allowed”. This means that traffic from the Client can be forwarded normally.

5. If authentication for the Client is unsuccessful, an authentication-failure action is taken. The authentication-failure action can be either to drop traffic from the Client in hardware (the default), or to place the port in a “restricted” VLAN.
   - If the authentication-failure action is to drop traffic from the Client, then the device waits for a specified amount of time (defined with the timeout quiet-period command, by default 60 seconds), then attempts to authenticate the Client again. After three unsuccessful authentication attempts, the Client's dot1x-mac-session is set to “access-denied”, causing traffic from the Client to be dropped in hardware.
     
     You can optionally configure the number of authentication attempts the device makes before dropping traffic from the Client. See "Specifying the Number of Authentication Attempts the Device Makes Before Dropping Packets" on page 4-15 for information on how to do this.
   - If the authentication-failure action is to place the port in a “restricted” VLAN, if the Client's dot1x-mac-session is set to “access-restricted” then the port is moved to the specified restricted VLAN, and traffic from the Client is forwarded normally.

6. When the Client disconnects from the network, the HP device deletes the Client's dot1x-mac-session. This does not affect the dot1x-mac-session or authentication status (if any) of the other hosts connected on the port.

Notes
   - The Client's dot1x-mac-session establishes a relationship between the username and MAC address used for authentication. If a user attempts to gain access from different Clients (with different MAC addresses), he or she would need to be authenticated from each Client.
   - If a Client has been denied access to the network (that is, the Client's dot1x-mac-session is set to “access-denied”), then you can cause the Client to be re-authenticated by manually disconnecting the Client from the network, or by using the clear dot1x mac-session command. See “Clearing a dot1x-mac-session for a MAC Address” on page 4-16 for information on this command.
   - When a Client has been denied access to the network, its dot1x-mac-session is aged out if no traffic is received from the Client's MAC address over a fixed hardware aging period (70 seconds), plus a configurable software aging period. You can optionally change the software aging period for dot1x-mac-sessions or disable aging altogether. After the denied Client's dot1x-mac-session is aged out, traffic from that Client is no longer blocked, and the Client can be re-authenticated.
     
     In addition, you can configure disable aging for the dot1x-mac-session of Clients that have been granted either full access to the network, or have been placed in a restricted VLAN. After a Client's dot1x-mac-session ages out, the Client must be re-authenticated. See “Disabling Aging for dot1x-mac-sessions” on page 4-15 for more information.
   - Dynamic IP ACL and MAC address filter assignment is not supported in an 802.1X multiple-host configuration. If a RADIUS server returns an Access-Accept message that specifies an IP ACL or MAC address filter for the Client, these attributes are ignored.

Dynamic VLAN Assignment in an 802.1X Multiple-Host Configuration (Release 07.8.00 and Later)

Dynamic VLAN assignment allows an 802.1X-enabled port to be assigned to a VLAN based on information received from the RADIUS server. Attributes in the RADIUS Access-Accept message can specify a VLAN identifier; if this VLAN is available on the HP device, the Client's port can be moved from its default VLAN to the specified VLAN.
Dynamic VLAN assignment is supported in 802.1X multiple-host configurations. The following considerations apply when a Client in a 802.1X multiple-host configuration is successfully authenticated, and the RADIUS Access-Accept message specifies a VLAN for the port:

- If the port is not already a member of a RADIUS-specified VLAN, and the RADIUS Access-Accept message specifies the name or ID of a valid VLAN on the HP device, then the port is placed in that VLAN.
- If the port is already a member of a RADIUS-specified VLAN, and the RADIUS Access-Accept message specifies the name or ID of a different VLAN, then it is considered an authentication failure. The port’s VLAN membership is not changed.
- If the port is already a member of a RADIUS-specified VLAN, and the RADIUS Access-Accept message specifies the name or ID of that same VLAN, then traffic from the Client is forwarded normally.
- If the RADIUS Access-Accept message specifies the name or ID of a VLAN that does not exist on the HP device, then it is considered an authentication failure.
- If the port is a tagged or dual-mode port, and the RADIUS Access-Accept message specifies the name or ID of a valid VLAN on the HP device, then the port is placed in that VLAN. If the port is already a member of the RADIUS-specified VLAN, no further action is taken. Note that the Client’s dot1x-mac-session is set to “access-is-allowed” for the RADIUS-specified VLAN only. If traffic from the Client’s MAC address is received on any other VLAN, it is dropped.
- If the RADIUS Access-Accept message does not contain any VLAN information, the Client’s dot1x-mac-session is set to “access-is-allowed”. If the port is already in a RADIUS-specified VLAN, it remains in that VLAN.

802.1X Port Security and sFlow
sFlow is a system for observing traffic flow patterns and quantities within and among a set of Routing Switches. sFlow works by taking periodic samples of network data and exporting this information to a collector.

When you enable sFlow forwarding on an 802.1X-enabled interface, the samples taken from the interface include the user name string at the inbound and/or outbound port, if that information is available.

For more information on sFlow, see the “sFlow” section in the “Remote Network Monitoring” chapter of the Advanced Configuration and Management Guide for ProCurve 9300/9400 Series Routing Switches.

Configuring 802.1X Port Security

Configuring 802.1X port security on an HP device consists of the following tasks:

1. Configuring the HP device’s interaction with the Authentication Server:
   - “Configuring an Authentication Method List for 802.1X” on page 4-10
   - “Setting RADIUS Parameters” on page 4-10
   - “Configuring Dynamic VLAN Assignment for 802.1X Ports” on page 4-16 (optional)

2. Configuring the HP device’s role as the Authenticator:
   - “Enabling 802.1X Port Security” on page 4-10
   - “Initializing 802.1X on a Port” on page 4-14 (optional)

3. Configuring the HP device’s interaction with Clients:
   - “Configuring Periodic Re-Authentication” on page 4-12 (optional)
   - “Re-Authenticating a Port Manually” on page 4-12 (optional)
   - “Setting the Quiet Period” on page 4-12 (optional)
   - “Setting the Interval for Retransmission of EAP-Request/Identity Frames” on page 4-12 (optional)
   - “Specifying the Number of EAP-Request/Identity Frame Retransmissions” on page 4-13 (optional)
• “Specifying the Security Hold Time” on page 4-13 (optional)
• “Specifying a Timeout for Retransmission of EAP-Request Frames to the Client” on page 4-14 (optional)
• “Allowing Access to Multiple Hosts” on page 4-14 (optional)
• “Defining MAC Filters for EAP Frames” on page 4-16 (optional)

Configuring an Authentication Method List for 802.1X

To use 802.1X port security, you must specify an authentication method to be used to authenticate Clients. HP supports RADIUS authentication with 802.1X port security. To use RADIUS authentication with 802.1X port security, you create an authentication method list for 802.1X and specify RADIUS as an authentication method, then configure communication between the HP device and RADIUS server.

For example:

ProCurveRS(config)# aaa authentication dot1x default radius

Syntax: [no] aaa authentication dot1x default <method-list>

For the <method-list>, enter at least one of the following authentication methods:

radius – Use the list of all RADIUS servers that support 802.1X for authentication.
none – Use no authentication. The Client is automatically authenticated without the device using information supplied by the Client.

NOTE: If you specify both radius and none, make sure radius comes before none in the method list.

Setting RADIUS Parameters

To use a RADIUS server to authenticate access to an HP device, you must identify the server to the HP device. For example:

ProCurveRS(config)# radius-server host 209.157.22.99 auth-port 1812 acct-port 1813 default key mirabeau dot1x

Syntax: radius-server host <ip-addr> | <server-name> [authentication-only | accounting-only | default] [key 0 | 1 <string>] [dot1x]

The <ip-addr> | <server-name> parameter is either an IP address or an ASCII text string.

The <string> parameter indicates that this RADIUS server supports the 802.1X standard. A RADIUS server that supports the 802.1X standard can also be used to authenticate non-802.1X authentication requests.

NOTE: To implement 802.1X port security, at least one of the RADIUS servers identified to the HP device must support the 802.1X standard.

Enabling 802.1X Port Security

By default, 802.1X port security is disabled on HP devices. To enable the feature on the device and enter the dot1x configuration level, enter the following command:

ProCurveRS(config)# dot1x-enable
ProCurveRS(config-dot1x)#

Syntax: [no] dot1x-enable
At the dot1x configuration level, you can enable 802.1X port security on all interfaces at once, on individual interfaces, or on a range of interfaces.

For example, to enable 802.1X port security on all interfaces on the device, enter the following command:

```plaintext
ProCurveRS(config-dot1x)# enable all
```

**Syntax:** `[no] enable all`

To enable 802.1X port security on interface 3/11, enter the following command:

```plaintext
ProCurveRS(config-dot1x)# enable ethernet 3/11
```

**Syntax:** `[no] enable <portnum>`

To enable 802.1X port security on interfaces 3/11 through 3/16, enter the following command:

```plaintext
ProCurveRS(config-dot1x)# enable ethernet 3/11 to 3/16
```

**Syntax:** `[no] enable <portnum> to <portnum>`

### Setting the Port Control

To activate authentication on an 802.1X-enabled interface, you specify the kind of **port control** to be used on the interface. An interface used with 802.1X port security has two virtual access points: a controlled port and an uncontrolled port.

- The controlled port can be either the authorized or unauthorized state. In the authorized state, it allows normal traffic to pass between the Client and the Authenticator. In the unauthorized state, it allows no traffic to pass through.

- The uncontrolled port allows only EAPOL traffic between the Client and the Authentication Server.

See Figure 4.3 on page 4-4 for an illustration of this concept.

By default, all controlled ports on the device are in the authorized state, allowing all traffic. When you activate authentication on an 802.1X-enabled interface, its controlled port is placed in the unauthorized state. When a Client connected to the interface is successfully authenticated, the controlled port is then placed in the authorized state. The controlled port remains in the authorized state until the Client logs off.

To activate authentication on an 802.1X-enabled interface, you configure the interface to place its controlled port in the unauthorized state when a Client is authenticated by an Authentication Server. To do this, enter commands such as the following:

```plaintext
ProCurveRS(config)# interface e 3/1
ProCurveRS(config-if-3/1)# dot1x port-control auto
```

**Syntax:** `[no] dot1x port-control [force-authorized | force-unauthorized | auto]`

When an interface’s control type is set to **auto**, the its controlled port is initially set to unauthorized, but is changed to authorized when the connecting Client is successfully authenticated by an Authentication Server.

The port control type can be one of the following:

- **force-authorized** – The port’s controlled port is placed unconditionally in the authorized state, allowing all traffic. This is the default state for ports on the HP device.

- **force-unauthorized** – The controlled port is placed unconditionally in the unauthorized state.

- **auto** – The controlled port is unauthorized until authentication takes place between the Client and Authentication Server. Once the Client passes authentication, the port becomes authorized. This has the effect of activating authentication on an 802.1X-enabled interface.
NOTE: You cannot enable 802.1X port security on ports that have any of the following features enabled:

- Link aggregation
- Metro Ring Protocol (MRP)
- Tagged port
- Mirror port
- Trunk port

In releases prior to 07.6.04, 802.1X port security could not be enabled on a port where Layer 2 switching was disabled (with the route-only command), and an 802.1X port could not be specified as a member of a virtual interface (ve). Both of these restrictions were removed in release 07.6.04.

Configuring Periodic Re-Authentication

You can configure the device to periodically re-authenticate Clients connected to 802.1X-enabled interfaces. When you enable periodic re-authentication, the device re-authenticates Clients every 3,600 seconds by default. You can optionally specify a different re-authentication interval of between 1 – 4294967295 seconds.

To configure periodic re-authentication using the default interval of 3,600 seconds, enter the following command:

ProCurveRS(config-dot1x)# re-authentication

Syntax: [no] re-authentication

To configure periodic re-authentication with an interval of 2,000 seconds, enter the following commands:

ProCurveRS(config-dot1x)# re-authentication
ProCurveRS(config-dot1x)# timeout re-authperiod 2000

Syntax: [no] timeout re-authperiod <seconds>

The re-authentication interval is a global setting, applicable to all 802.1X-enabled interfaces. If you want to re-authenticate Clients connected to a specific port manually, use the dot1x re-authenticate command. See “Re-Authenticating a Port Manually”, below.

Re-Authenticating a Port Manually

When periodic re-authentication is enabled, by default the HP device re-authenticates Clients connected to an 802.1X-enabled interface every 3,600 seconds (or the time specified by the dot1x timeout re-authperiod command). You can also manually re-authenticate Clients connected to a specific port.

For example, to re-authenticate Clients connected to interface 3/1, enter the following command:

ProCurveRS# dot1x re-authenticate e 3/1

Syntax: dot1x re-authenticate <portnum>

Setting the Quiet Period

If the HP device is unable to authenticate the Client, the HP device waits a specified amount of time before trying again. The amount of time the HP device waits is specified with the quiet-period parameter. The quiet-period parameter can be from 0 – 4294967295 seconds. The default is 60 seconds.

For example, to set the quiet period to 30 seconds, enter the following command:

ProCurveRS(config-dot1x)# timeout quiet-period 30

Syntax: [no] timeout quiet-period <seconds>

Setting the Interval for Retransmission of EAP-Request/Identity Frames

When the HP device sends a Client an EAP-request/identity frame, it expects to receive an EAP-response/identity frame from the Client. If the Client does not send back an EAP-response/identity frame, the device waits a
specifying a timeout for retransmission of messages to the Authentication Server.

When performing authentication, the HP device receives EAPOL frames from the Client and passes the messages on to the RADIUS server. The device expects a response from the RADIUS server within 30 seconds. If the RADIUS server does not send a response within 30 seconds, the HP device retransmits the message to the RADIUS server. The time constraint for retransmission of messages to the Authentication Server can be between 0 – 4294967295 seconds.

For example, to configure the device to retransmit a message if the Authentication Server does not respond within 45 seconds, enter the following command:

```
ProCurveRS(config-dot1x)# server-timeout 45
```
**Syntax:** `servertimeout <seconds>`

**Specifying a Timeout for Retransmission of EAP-Request Frames to the Client**

Acting as an intermediary between the RADIUS Authentication Server and the Client, the HP device receives RADIUS messages from the RADIUS server, encapsulates them as EAPOL frames, and sends them to the Client. When the HP device relays an EAP-Request frame from the RADIUS server to the Client, it expects to receive a response from the Client within 30 seconds. If the Client does not respond within the allotted time, the device retransmits the EAP-Request frame to the Client. The time constraint for retransmission of EAP-Request frames to the Client can be between 0 – 4,294,967,295 seconds.

For example, to configure the device to retransmit an EAP-Request frame if the Client does not respond within 45 seconds, enter the following command:

```
ProCurveRS(config-dot1x)# supptimeout 45
```

**Syntax:** `supptimeout <seconds>`

---

**Initializing 802.1X on a Port**

To initialize 802.1X port security on a port, enter a command such as the following:

```
ProCurveRS# dot1x initialize e 3/1
```

**Syntax:** `dot1x initialize <portnum>`

---

**Allowing Access to Multiple Hosts**

HP devices support 802.1X authentication for ports with more than one host connected to them. Multiple-host authentication works differently according to the software release running on the HP device:

- In releases prior to 07.8.00, services are provided on a port based on the authentication of a single Client. When one Client is successfully authenticated, all hosts connected to the port are allowed access to the network. See “Configuring 802.1X Multiple-Host Authentication (Releases Prior to 07.8.00)”.

- Starting in release 07.8.00, if there are multiple hosts connected to a single 802.1X-enabled port, the HP device authenticates each of them individually. See “Configuring 802.1X Multiple-Host Authentication (Release 07.8.00 and Later)”.

**Configuring 802.1X Multiple-Host Authentication (Releases Prior to 07.8.00)**

To enable 802.1X port security in a multiple-host configuration, an HP device running a release prior to 07.8.00 must be configured to allow multiple Clients on the same port. When one Client is successfully authenticated, all Clients connected to the port are allowed access to the network. When the authenticated Client logs off the network, the port becomes unauthorized again. Each time an authenticated Client logs off, the port becomes unauthorized.

To allow multiple 802.1X Clients on the same port, enter the following command:

```
ProCurveRS(config-if-3/1)# dot1x multiple-hosts
```

**Syntax:** `[no] dot1x multiple-hosts`

By default multiple-host access is disabled. See Figure 4.7 on page 4-29 for a sample 802.1X configuration with multiple hosts connected to one port.

---

**NOTE:** When the **port-control** parameter on an 802.1X-enabled interface is set to **force-authorized**, the HP device allows connections from multiple Clients, regardless of whether the **multiple-hosts** parameter is used in the interface’s configuration.

**Configuring 802.1X Multiple-Host Authentication (Release 07.8.00 and Later)**

When multiple hosts are connected to the same 802.1X-enabled port, the functionality described in “How 802.1X Multiple-Host Authentication Works (Release 07.8.00 and Later)” on page 4-7 is enabled by default. You can optionally do the following:
• Specify the authentication-failure action
• Specify the number of authentication attempts the device makes before dropping packets
• Disabling aging for dot1x-mac-sessions
• Configure aging time for blocked Clients
• Clear the dot1x-mac-session for a MAC address

Specifying the Authentication-Failure Action
In an 802.1X multiple-host configuration, if RADIUS authentication for a Client is unsuccessful, traffic from that
Client is either dropped in hardware (the default), or the Client's port is placed in a "restricted" VLAN. You can
specify which of these two authentication-failure actions is to be used. If the authentication-failure action is to
place the port in a restricted VLAN, you can specify the ID of the restricted VLAN.

To specify that the authentication-failure action is to place the Client's port in a restricted VLAN, enter the following
command:

ProCurveRS(config)# dot1x-enable
ProCurveRS(config-dot1x)# auth-fail-action restricted-vlan

Syntax: [no] auth-fail-action restricted-vlan

To specify the ID of the restricted VLAN as VLAN 300, enter the following command:

ProCurveRS(config-dot1x)# auth-fail-vlanid 300

Syntax: [no] auth-fail-vlanid <vlan-id>

Specifying the Number of Authentication Attempts the Device Makes Before Dropping Packets
When the authentication-failure action is to drop traffic from the Client, and the initial authentication attempt made
by the device to authenticate the Client is unsuccessful, then the HP device waits for a specified amount of time
-defined with the timeout quiet-period command, by default 60 seconds), then attempts to authenticate the Client
again. After three unsuccessful authentication attempts, the Client's dot1x-mac-session is set to “access-denied”,
causing traffic from the Client to be dropped in hardware.

You can optionally configure the number of authentication attempts the device makes before dropping traffic from
the Client. To do so, enter a command such as the following:

ProCurveRS(config-dot1x)# auth-fail-max-attempts 2

Syntax: [no] auth-fail-max-attempts <attempts>

By default, the device makes 3 attempts to authenticate a Client before dropping packets from the Client. You can
specify between 1 – 10 authentication attempts.

Disabling Aging for dot1x-mac-sessions
The dot1x-mac-sessions for Clients authenticated or denied by a RADIUS server are aged out if no traffic is
received from the Client's MAC address for a certain period of time. After a Client's dot1x-mac-session is aged
out, the Client must be re-authenticated.

• Permitted dot1x-mac-sessions, which are the dot1x-mac-sessions for authenticated Clients, as well as for
non-authenticated Clients whose ports have been placed in the restricted VLAN, are aged out if no traffic is
received from the Client's MAC address over the HP device's normal MAC aging interval.

• Denied dot1x-mac-sessions, which are the dot1x-mac-sessions for non-authenticated Clients that are
blocked by the HP device are aged out if no traffic is received from the Client's MAC address over a fixed
hardware aging period (70 seconds), plus a configurable software aging period. (See the next section for
more information on configuring the software aging period).

You can optionally disable aging of the permitted and/or denied dot1x-mac-sessions on the HP device.

To disable aging of the permitted dot1x-mac-sessions, enter the following command:

ProCurveRS(config-dot1x)# mac-session-aging no-aging permitted-mac-only

Syntax: [no] mac-session-aging no-aging permitted-mac-only
To disable aging of the denied dot1x-mac-sessions, enter the following command:

    ProCurveRS(config-dot1x)# mac-session-aging no-aging denied-mac-only

**Syntax:** [no] mac-session-aging no-aging denied-mac-only

**Specifying the Aging Time for Blocked Clients**

When the HP device is configured to drop traffic from non-authenticated Clients, traffic from the blocked Clients is dropped in hardware, without being sent to the CPU. A Layer 2 CAM entry is created that drops traffic from the blocked Client’s MAC address in hardware. If no traffic is received from the blocked Client’s MAC address for a certain amount of time, this Layer 2 CAM entry is aged out. If traffic is subsequently received from the Client’s MAC address, then an attempt can be made to authenticate the Client again.

Aging of the Layer 2 CAM entry for a blocked Client’s MAC address occurs in two phases, known as **hardware aging** and **software aging**. The hardware aging period is fixed at 70 seconds and is non-configurable. The software aging time is configurable through the CLI.

Once the HP device stops receiving traffic from a blocked Client’s MAC address, the hardware aging begins and lasts for a fixed period of time. After the hardware aging period ends, the software aging period begins. The software aging period lasts for a configurable amount of time (by default 120 seconds). After the software aging period ends, the blocked Client’s MAC address ages out, and can be authenticated again if the HP device receives traffic from the Client’s MAC address.

To change the length of the software aging period for a blocked Client’s MAC address, enter a command such as the following:

    ProCurveRS(config)# mac-session-aging max-age 180

**Syntax:** [no] mac-session-aging max-age <seconds>

You can specify from 1 – 65535 seconds. The default is 120 seconds.

**Clearing a dot1x-mac-session for a MAC Address**

You can clear the dot1x-mac-session for a specified MAC address, so that the Client with that MAC address can be re-authenticated by the RADIUS server. For example:

    ProCurveRS# clear dot1x mac-session 00e0.1234.abd4

**Syntax:** clear dot1x mac-session <mac-address>

**Defining MAC Filters for EAP Frames**

You can create MAC address filters to permit or deny EAP frames. To do this, you specify the HP device’s 802.1X group MAC address as the destination address in a MAC filter, then apply the filter to an interface.

For example, the following command creates a MAC filter that denies frames with the destination MAC address of 0180.c200.0003, which is the HP device’s 802.1X group MAC address:

    ProCurveRS(config)# mac filter 1 deny any 0180.c200.0003 ffff.ffff.ffff

The following commands apply this filter to interface e 3/1:

    ProCurveRS(config)# interface e 3/1
    ProCurveRS(config-if-3/1)# mac filter-group 1

See “Defining MAC Address Filters” in the *Installation and Basic Configuration Guide for ProCurve 9300 Series Routing Switches* for more information.

**Configuring Dynamic VLAN Assignment for 802.1X Ports**

Starting in release 07.6.04, HP’s 802.1X implementation supports assigning a port to a VLAN dynamically, based on information received from an Authentication Server.

When a client/supplicant successfully completes the EAP authentication process, the Authentication Server (the RADIUS server) sends the Authenticator (the HP device) a RADIUS Access-Accept message that grants the client access to the network. The RADIUS Access-Accept message contains attributes set for the user in the user's access profile on the RADIUS server.
If one of the attributes in the Access-Accept message specifies a VLAN identifier, and this VLAN is available on the HP device, the client's port is moved from its default VLAN to the specified VLAN. When the client disconnects from the network, the port is placed back in its default VLAN.

**NOTE:** This feature is supported on port-based VLANs only. This feature cannot be used to place an 802.1X-enabled port into a Layer 3 protocol VLAN.

To enable 802.1X VLAN ID support, you must add the following attributes to a user's profile on the RADIUS server:

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>Type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tunnel-Type</td>
<td>064</td>
<td>13 (decimal) – VLAN</td>
</tr>
<tr>
<td>Tunnel-Medium-Type</td>
<td>065</td>
<td>6 (decimal) – 802</td>
</tr>
<tr>
<td>Tunnel-Private-Group-ID</td>
<td>081</td>
<td>&lt;vlan-name&gt; (string) – either the name or the number of a VLAN configured on the HP device.</td>
</tr>
</tbody>
</table>

The device reads the attributes as follows:

- If the Tunnel-Type or the Tunnel-Medium-Type attributes in the Access-Accept message do not have the values specified above, the HP device ignores the three Attribute-Value pairs. The client becomes authorized, but the client's port is not dynamically placed in a VLAN.
- If the Tunnel-Type or the Tunnel-Medium-Type attributes in the Access-Accept message do have the values specified above, but there is no value specified for the Tunnel-Private-Group-ID attribute, the client will not become authorized.
- When the HP device receives the value specified for the Tunnel-Private-Group-ID attribute, it checks whether the <vlan-name> string matches the name of a VLAN configured on the device. If there is a VLAN on the device whose name matches the <vlan-name> string, then the client's port is placed in the VLAN whose ID corresponds to the VLAN name.
- If the <vlan-name> string does not match the name of a VLAN, the HP device checks whether the string, when converted to a number, matches the ID of a VLAN configured on the device. If it does, then the client's port is placed in the VLAN with that ID.
- If the <vlan-name> string does not match either the name or the ID of a VLAN configured on the device, then the client will not become authorized.

The `show interface` command displays the VLAN to which an 802.1X-enabled port has been dynamically assigned, as well as the port from which it was moved (that is, the port's default VLAN). See "Displaying Dynamically Assigned VLAN Information" on page 4-22 for sample output indicating the port's dynamically assigned VLAN.

**Using Dynamic VLAN Assignment with the MAC Port Security Feature**

The MAC port security feature can be configured on 802.1X-enabled ports. The MAC port security feature allows the HP device to learn a limited number of "secure" MAC addresses on an interface. The interface will forward only packets with source MAC addresses that match these secure addresses. If the interface receives a packet with a source MAC address that is different from any of the secure addresses, it is considered a security violation, and subsequent packets from the violating MAC address can be dropped, or the port can be disabled entirely.

If a port has been disabled due to a MAC port security violation, 802.1X clients attempting to connect over the port cannot be authorized. In addition, 802.1X clients connecting from non-secure MAC addresses cannot be authorized.

To use 802.1X dynamic VLAN assignment with the MAC port security feature on an interface, you must set the number of secure MAC addresses to two or more. For example:

```bash
ProCurveRS(config)# int e 3/2
```
ProCurveRS(config-if-e100-3/2)# port security
ProCurveRS(config-port-security-e100-3/2)# maximum 2
ProCurveRS(config-port-security-e100-3/2)# exit

See the "Using the MAC Port Security Feature" on page 5-1 for more information.

NOTE: There is small chance that an interface can be inadvertently disabled when both 802.1X (with dynamic VLAN assignment) and the MAC port security feature are enabled on the interface. When this happens, disable then re-enable the interface to bring the interface back up.

Displaying 802.1X Information

You can display the following 802.1X-related information:

- Information about the 802.1X configuration on the device and on individual ports
- Statistics about the EAPOL frames passing through the device
- Information about 802.1X-enabled ports dynamically assigned to a VLAN
- Information about the user-defined and dynamically applied MAC filters and IP ACLs currently active on the device
- Information about the 802.1X multiple-host configuration

Displaying 802.1X Configuration Information

To display information about the 802.1X configuration on the HP device, enter the following command:

ProCurveRS# show dot1x
PAE Capability: Authenticator Only
system-auth-control: Enable
re-authentication: Disable
global-filter-strict-security: Enable
quiet-period: 60 Seconds
tx-period: 30 Seconds
supptimeout: 30 Seconds
servertimeout: 30 Seconds
maxreq: 2
re-authperiod: 3600 Seconds
security-hold-time: 60 Seconds
Protocol Version: 1

Syntax: show dot1x

The following table describes the information displayed by the show dot1x command.

<table>
<thead>
<tr>
<th>This Field...</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td>PAE Capability</td>
<td>The Port Access Entity (PAE) role for the HP device. This is always &quot;Authenticator Only&quot;.</td>
</tr>
<tr>
<td>system-auth-control</td>
<td>Whether system authentication control is enabled on the device. The dot1x-enable command enables system authentication control on the device.</td>
</tr>
</tbody>
</table>
### Table 4.1: Output from the show dot1x command (Continued)

<table>
<thead>
<tr>
<th>This Field...</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td>re-authentication</td>
<td>Whether periodic re-authentication is enabled on the device. See “Configuring Periodic Re-Authentication” on page 4-12. When periodic re-authentication is enabled, the device automatically re-authenticates Clients every 3,600 seconds by default.</td>
</tr>
<tr>
<td>quiet-period</td>
<td>When the HP device is unable to authenticate a Client, the amount of time the HP device waits before trying again (default 60 seconds). See “Setting the Quiet Period” on page 4-12 for information on how to change this setting.</td>
</tr>
<tr>
<td>tx-period</td>
<td>When a Client does not send back an EAP-response/identity frame, the amount of time the HP device waits before retransmitting the EAP-request/identity frame to a Client (default 30 seconds). See “Setting the Interval for Retransmission of EAP-Request/Identity Frames” on page 4-12 for information on how to change this setting.</td>
</tr>
<tr>
<td>supp-timeout</td>
<td>When a Client does not respond to an EAP-request frame, the amount of time before the HP device retransmits the frame. See “Specifying a Timeout for Retransmission of EAP-Request Frames to the Client” on page 4-14 for information on how to change this setting.</td>
</tr>
<tr>
<td>server-timeout</td>
<td>When the Authentication Server does not respond to a message sent from the Client, the amount of time before the HP device retransmits the message. See “Specifying a Timeout for Retransmission of Messages to the Authentication Server” on page 4-13 for information on how to change this setting.</td>
</tr>
<tr>
<td>max-req</td>
<td>The number of times the HP device retransmits an EAP-request/identity frame if it does not receive an EAP-response/identity frame from a Client (default 2 times). See “Specifying the Number of EAP-Request/Identity Frame Retransmissions” on page 4-13 for information on how to change this setting.</td>
</tr>
<tr>
<td>re-authperiod</td>
<td>How often the device automatically re-authenticates Clients when periodic re-authentication is enabled (default 3,600 seconds). See “Configuring Periodic Re-Authentication” on page 4-12 for information on how to change this setting.</td>
</tr>
<tr>
<td>security-hold-time</td>
<td>The amount of time the device disables an interface when it detects multiple Clients trying to connect on the interface, when the <code>multiple-hosts</code> command is not present in the interface's configuration. See “Specifying the Security Hold Time” on page 4-13 for information on how to change this setting.</td>
</tr>
<tr>
<td>Protocol Version</td>
<td>The version of the 802.1X protocol in use on the device.</td>
</tr>
</tbody>
</table>
To display information about the 802.1X configuration on an individual port, enter a command such as the following:

ProCurveRS# show dot1x config e 1/3

Port 1/3 Configuration:
Authenticator PAE state: AUTHENTICATED
Backend Authentication state: IDLE
AdminControlledDirections: BOTH
OperControlledDirections: BOTH
AuthControlledPortControl: Auto
AuthControlledPortStatus: authorized
quiet-period: 60 Seconds
tx-period: 30 Seconds
supptimeout: 30 Seconds
servertimeout: 30 Seconds
maxreq: 2
re-authperiod: 3600 Seconds
security-hold-time: 60 Seconds
re-authentication: Disable
multiple-hosts: Disable
filter-strict-security: Enable
Protocol Version: 1

Syntax: show dot1x config <portnum>

The following additional information is displayed in the show dot1x config command for an interface:

<table>
<thead>
<tr>
<th>This Field...</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authenticator PAE state</td>
<td>The current status of the Authenticator PAE state machine. This can be INITIALIZE, DISCONNECTED, CONNECTING, AUTHENTICATING, AUTHENTICATED, ABORTING, HELD, FORCE_AUTH, or FORCE_UNAUTH. <strong>Note:</strong> When the Authenticator PAE state machine is in the AUTHENTICATING state, if the reAuthenticate, eapStart, eapLogoff, or authTimeout parameters are set to TRUE, it may place the Authenticator PAE state machine indefinitely in the ABORTING state. If this should happen, use the dot1x initialize command to initialize 802.1X port security on the port, or unplug the Client or hub connected to the port, then reconnect it.</td>
</tr>
<tr>
<td>Backend Authentication state</td>
<td>The current status of the Backend Authentication state machine. This can be REQUEST, RESPONSE, SUCCESS, FAIL, TIMEOUT, IDLE, or INITIALIZE.</td>
</tr>
<tr>
<td>AdminControlledDirections</td>
<td>Indicates whether an unauthorized controlled port exerts control over communication in both directions (disabling both reception of incoming frames and transmission of outgoing frames), or just in the incoming direction (disabling only reception of incoming frames). On HP devices, this parameter is set to BOTH.</td>
</tr>
</tbody>
</table>
### Table 4.2: Output from the show dot1x config command for an interface (Continued)

<table>
<thead>
<tr>
<th>This Field...</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td>OperControlledDirections</td>
<td>The setting for the OperControlledDirections parameter, as defined in the 802.1X standard. According to the 802.1X standard, if the AdminControlledDirections parameter is set to BOTH, the OperControlledDirections parameter is unconditionally set to BOTH. Since the AdminControlledDirections parameter on HP devices is always set to BOTH, the OperControlledDirections parameter is also set to BOTH.</td>
</tr>
<tr>
<td>AuthControlledPortControl</td>
<td>The port control type configured for the interface. If set to auto, authentication is activated on the 802.1X-enabled interface.</td>
</tr>
<tr>
<td>AuthControlledPortStatus</td>
<td>The current status of the interface's controlled port: either authorized or unauthorized.</td>
</tr>
<tr>
<td>multiple-hosts</td>
<td>Whether the port is configured to allow multiple Supplicants accessing the interface on the HP device through a hub. See “Allowing Access to Multiple Hosts” on page 4-14 for information on how to change this setting.</td>
</tr>
</tbody>
</table>

### Displaying 802.1X Statistics

To display 802.1X statistics for an individual port, enter a command such as the following:

```
ProCurveRS# show dot1x statistics e 3/3
```

Port 3/3 Statistics:
RX EAPOL Start: 0
RX EAPOL Logoff: 0
RX EAPOL Invalid: 0
RX EAPOL Total: 0
RX EAP Resp/Id: 0
RX EAP Resp other than Resp/Id: 0
RX EAP Length Error: 0
Last EAPOL Version: 0
Last EAPOL Source: 0007.9550.0B83
TX EAPOL Total: 217
TX EAP Req/Id: 163
TX EAP Req other than Req/Id: 0

**Syntax:** show dot1x statistics <portnum>

The following table describes the information displayed by the `show dot1x statistics` command for an interface.

### Table 4.3: Output from the show dot1x statistics command

<table>
<thead>
<tr>
<th>This Field...</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td>RX EAPOL Start</td>
<td>The number of EAPOL-Start frames received on the port.</td>
</tr>
<tr>
<td>RX EAPOL Logoff</td>
<td>The number of EAPOL-Logoff frames received on the port.</td>
</tr>
<tr>
<td>RX EAPOL Invalid</td>
<td>The number of invalid EAPOL frames received on the port.</td>
</tr>
<tr>
<td>RX EAPOL Total</td>
<td>The total number of EAPOL frames received on the port.</td>
</tr>
</tbody>
</table>
Table 4.3: Output from the show dot1x statistics command (Continued)

<table>
<thead>
<tr>
<th>This Field...</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td>RX EAP Resp/Id</td>
<td>The number of EAP-Response/Identity frames received on the port</td>
</tr>
<tr>
<td>RX EAP Resp other than Resp/Id</td>
<td>The total number of EAPOL-Response frames received on the port that were not EAP-Response/Identity frames.</td>
</tr>
<tr>
<td>RX EAP Length Error</td>
<td>The number of EAPOL frames received on the port that have an invalid packet body length.</td>
</tr>
<tr>
<td>Last EAPOL Version</td>
<td>The version number of the last EAPOL frame received on the port.</td>
</tr>
<tr>
<td>Last EAPOL Source</td>
<td>The source MAC address in the last EAPOL frame received on the port.</td>
</tr>
<tr>
<td>TX EAPOL Total</td>
<td>The total number of EAPOL frames transmitted on the port.</td>
</tr>
<tr>
<td>TX EAP Req/Id</td>
<td>The number of EAP-Request/Identity frames transmitted on the port.</td>
</tr>
<tr>
<td>TX EAP Req other than Req/Id</td>
<td>The number of EAP-Request frames transmitted on the port that were not EAP-Request/Identity frames.</td>
</tr>
</tbody>
</table>

**Clearing 802.1X Statistics**

You can clear the 802.1X statistics counters on all interfaces at once, on individual interfaces, or on a range of interfaces.

For example, to clear the 802.1X statistics counters on all interfaces on the device, enter the following command:

```
ProCurveRS# clear dot1x statistics all
```

*Syntax:* `clear dot1x statistics all`

To clear the 802.1X statistics counters on interface e 3/11, enter the following command:

```
ProCurveRS# clear dot1x statistics e 3/11
```

*Syntax:* `clear dot1x statistics <portnum>`

**Displaying Dynamically Assigned VLAN Information**

The `show interface` command displays the VLAN to which an 802.1X-enabled port has been dynamically assigned, as well as the port from which it was moved (that is, the port's default VLAN).
The following is an example of the **show interface** command indicating the port's dynamically assigned VLAN. Information about the dynamically assigned VLAN is shown in bold type.

ProCurveRS# show interface e 12/2
FastEthernet12/2 is up, line protocol is up
    Hardware is FastEthernet, address is 0204.80a0.4681 (bia 0204.80a0.4681)
    Configured speed auto, actual 100Mbit, configured duplex fdx, actual fdx
    **Member of L2 VLAN ID 2 (dot1x-RADIUS assigned), original L2 VLAN ID is 1,**
    port is untagged, port state is FORWARDING
    STP configured to ON, priority is level0, flow control enabled
    mirror disabled, monitor disabled
    Not member of any active trunks
    Not member of any configured trunks
    No port name
    MTU 1518 bytes
    300 second input rate: 0 bits/sec, 0 packets/sec, 0.00% utilization
    300 second output rate: 256 bits/sec, 0 packets/sec, 0.00% utilization
    3 packets input, 192 bytes, 0 no buffer
    Received 0 broadcasts, 0 multicasts, 3 unicasts
    0 input errors, 0 CRC, 0 frame, 0 ignored
    0 runts, 0 giants, DMA received 3 packets
    919 packets output, 58816 bytes, 0 underruns
    Transmitted 1 broadcasts, 916 multicasts, 2 unicasts
    0 output errors, 0 collisions, DMA transmitted 919 packets

In this example, the 802.1X-enabled port has been moved from VLAN 1 to VLAN 2. When the client disconnects, the port will be moved back to VLAN 1.

The **show run** command also indicates the VLAN to which the port has been dynamically assigned. The output can differ depending on whether GARP VLAN Registration Protocol (GVRP) is enabled on the device:

- **Without GVRP** – When you enter the **show run** command, the output indicates that the port is a member of the VLAN to which it was dynamically assigned through 802.1X. If you then enter the **write memory** command, the VLAN to which the port is currently assigned becomes the port's default VLAN in the device's configuration.

- **With GVRP** – When you enter the **show run** command, if the VLAN name supplied by the RADIUS server corresponds to a VLAN learned through GVRP, then the output indicates that the port is a member of the VLAN to which it was originally assigned (not the VLAN to which it was dynamically assigned).

If the VLAN name supplied by the RADIUS server corresponds to a statically configured VLAN, the output indicates that the port is a member of the VLAN to which it was dynamically assigned through 802.1X. If you then enter the **write memory** command, the VLAN to which the port is currently assigned becomes the port's default VLAN in the device's configuration.

**Displaying Information About Dynamically Applied MAC Filters and IP ACLs**

You can display information about the user-defined and dynamically applied MAC filters and IP ACLs currently active on the device.

**Displaying User-Defined MAC Filters and IP ACLs**

To display the user-defined MAC filters active on the device, enter the following command:

ProCurveRS# show dot1x mac-address-filter

Port 1/3 (User defined MAC Address Filter):
    mac filter 1 permit any any

**Syntax:** show dot1x mac-address-filter

To display the user-defined IP ACLs active on the device, enter the following command:
ProCurveRS# show dot1x ip-acl

Port 1/3 (User defined IP ACLs):

Extended IP access list Port_1/3_E_IN
permit udp any any

Extended IP access list Port_1/3_E_OUT
permit udp any any

**Syntax:** show dot1x ip-acl

**Displaying Dynamically Applied MAC Filters and IP ACLs**

To display the dynamically applied MAC address filters active on an interface, enter a command such as the following:

ProCurveRS# show dot1x mac-address-filter e 1/3

Port 1/3 MAC Address Filter information:
- 802.1X Dynamic MAC Address Filter:
  - mac filter-group 2
- Port default MAC Address Filter:
  - No mac address filter is set

**Syntax:** show dot1x mac-address-filter <portnum> | all

The all keyword displays all dynamically applied MAC address filters active on the device.

To display the dynamically applied IP ACLs active on an interface, enter a command such as the following:

ProCurveRS# show dot1x ip-acl e 1/3

Port 1/3 IP ACL information:
- 802.1X dynamic IP ACL (user defined) in:
  - ip access-list extended Port_1/3_E_IN in
- Port default IP ACL in:
  - No inbound ip access-list is set
- 802.1X dynamic IP ACL (user defined) out:
  - ip access-list extended Port_1/3_E_OUT out
- Port default IP ACL out:
  - No outbound ip access-list is set

**Syntax:** show dot1x ip-acl <portnum> | all

The all keyword displays all dynamically applied IP ACLs active on the device.

**Displaying 802.1X Multiple-Host Authentication Information (Release 07.8.00 and Later)**

You can display the following information about 802.1X multiple-host authentication:

- Information about the 802.1X multiple-host configuration
- The dot1x-mac-sessions on each port
- The number of users connected on each port in a 802.1X multiple-host configuration

**Displaying 802.1X Multiple-Host Configuration Information**

In release 07.8.00 and later, the output of the `show dot1x` and `show dot1x config` commands displays information related to 802.1X multiple-host authentication.
The following is an example of the output of the `show dot1x` command. The information related to multiple-host authentication is highlighted in bold.

ProCurveRS# show dot1x

```
Number of Ports enabled : 2
Re-Authentication : Enabled
Authentication-fail-action : Restricted VLAN
Authentication Failure VLAN : 111
Mac Session Aging : Disabled for permitted MAC sessions
Mac Session max-age : 60 seconds
Protocol Version : 1
quiet-period : 5 Seconds
tx-period : 30 Seconds
supptimeout : 30 Seconds
servertimeout : 30 Seconds
maxreq : 2
re-authperiod : 3600 Seconds
security-hold-time : 60 Seconds
re-authentication : Enable
Flow based multi-user policy : Disable
```

**Syntax:** `show dot1x`

Table 4.4 describes the bold fields in the display.

<table>
<thead>
<tr>
<th>This Field...</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication-fail-action</td>
<td>The configured authentication-failure action. This can be Restricted VLAN or Block Traffic.</td>
</tr>
<tr>
<td>Authentication Failure VLAN</td>
<td>If the authentication-failure action is Restricted VLAN, the ID of the VLAN to which unsuccessfully authenticated Client ports are assigned.</td>
</tr>
<tr>
<td>Mac Session Aging</td>
<td>Whether aging for dot1x-mac-sessions has been enabled or disabled for permitted or denied dot1x-mac-sessions.</td>
</tr>
<tr>
<td>Mac Session max-age</td>
<td>The configured software aging time for dot1x-mac-sessions.</td>
</tr>
<tr>
<td>Flow based multi-user policy</td>
<td>The dynamically assigned IP ACLs and MAC address filters used in the 802.1X multiple-host configuration. Note that release 07.8.00 does not support dynamically assigned IP ACLs and MAC address filters in an 802.1X multiple-host configuration. This functionality will be added in a future release.</td>
</tr>
</tbody>
</table>

In release 07.8.00, the output of the `show dot1x config` command for an interface was changed so it displays only the configured port control for the interface. For example:

ProCurveRS# show dot1x config e 1/3

Port-Control: control-auto

**Syntax:** `show dot1x config <portnum>`

Table 4.5 lists the field in the display.
Table 4.5: Output from the show dot1x config command

<table>
<thead>
<tr>
<th>This Field...</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port-Control</td>
<td>The configured port control type for the interface. This can be one of the following:</td>
</tr>
<tr>
<td></td>
<td><strong>force-authorized</strong> – The port's controlled port is placed unconditionally in the authorized state, allowing all traffic. This is the default state for ports on the HP device.</td>
</tr>
<tr>
<td></td>
<td><strong>force-unauthorized</strong> – The controlled port is placed unconditionally in the unauthorized state. No authentication takes place for any connected 802.1X Clients.</td>
</tr>
<tr>
<td></td>
<td><strong>auto</strong> – The authentication status for each 802.1X Client depends on the authentication status returned from the RADIUS server.</td>
</tr>
</tbody>
</table>

Displaying Information About the dot1x-mac-sessions on Each Port

To display information about the dot1x-mac-sessions on each port on the device, enter the following command:

```
ProCurveRS# show dot1x mac-session
```

<table>
<thead>
<tr>
<th>Port</th>
<th>MAC/IP Address(username)</th>
<th>Vlan</th>
<th>Age</th>
<th>CAM</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0007.e90f.eb30 :kingcobra</td>
<td>102</td>
<td>permit</td>
<td>1</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>0007.e90f.eaal :cobra</td>
<td>102</td>
<td>permit</td>
<td>6</td>
<td>N/A</td>
</tr>
</tbody>
</table>

**Syntax:** `show dot1x mac-session`

Table 4.6 describes the information displayed by the **show dot1x mac-session** command.

Table 4.6: Output from the show dot1x mac-session command

<table>
<thead>
<tr>
<th>This Field...</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>The port on which the dot1x-mac-session exists.</td>
</tr>
<tr>
<td>MAC/IP Address(username)</td>
<td>The MAC address of the Client and the username used for RADIUS authentication.</td>
</tr>
<tr>
<td>Vlan</td>
<td>The VLAN to which the port is currently assigned.</td>
</tr>
</tbody>
</table>
Table 4.6: Output from the show dot1x mac-session command (Continued)

<table>
<thead>
<tr>
<th>This Field...</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auth-State</td>
<td>The authentication state of the dot1x-mac-session. This can be one of the following: permit – The Client has been successfully authenticated, and traffic from the Client is being forwarded normally. blocked – Authentication failed for the Client, and traffic from the Client is being dropped in hardware. restricted – Authentication failed for the Client, but traffic from the Client is allowed in the restricted VLAN only. init - The Client is in the process of 802.1X authentication, or has not started the authentication process.</td>
</tr>
<tr>
<td>Age</td>
<td>The software age of the dot1x-mac-session.</td>
</tr>
<tr>
<td>CAM Index</td>
<td>If the MAC address is blocked, the index entry for the Layer 2 CAM entry created for this MAC address. If the MAC address is not blocked, either through successful authentication or through being placed in the restricted VLAN, then “N/A” is displayed. If the hardware aging period has expired, then “ffff” is displayed for the MAC address during the software aging period.</td>
</tr>
</tbody>
</table>

Displaying Information About the Ports in an 802.1X Multiple-Host Configuration

To display information about the ports in an 802.1X multiple-host configuration, enter the following command:

ProCurveRS# show dot1x mac-session brief

<table>
<thead>
<tr>
<th>Port</th>
<th>Number of users</th>
<th>Number of Authorized users</th>
<th>Dynamic VLAN</th>
<th>Dynamic Filters</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>2</td>
<td>yes</td>
<td>no</td>
</tr>
</tbody>
</table>

Syntax: show dot1x mac-session brief

The following table describes the information displayed by the show dot1x mac-session brief command.

Table 4.7: Output from the show dot1x mac-session brief command

<table>
<thead>
<tr>
<th>This Field...</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>Information about the users connected to each port.</td>
</tr>
<tr>
<td>Number of users</td>
<td>The number of users connected to the port.</td>
</tr>
<tr>
<td>Number of Authorized users</td>
<td>The number of users connected to the port that have been successfully authenticated.</td>
</tr>
<tr>
<td>Dynamic VLAN</td>
<td>Whether the port is a member of a RADIUS-specified VLAN.</td>
</tr>
<tr>
<td>Dynamic Filters</td>
<td>Whether RADIUS-specified IP ACLs or MAC address filters have been applied to the port.</td>
</tr>
</tbody>
</table>
Sample 802.1X Configurations

This section illustrates a sample point-to-point configuration and a sample hub configuration that use 802.1X port security.

Point-to-Point Configuration

Figure 4.6 illustrates a sample 802.1X configuration with Clients connected to three ports on the HP device. In a point-to-point configuration, only one 802.1X Client can be connected to each port.

The following commands configure the HP device in Figure 4.6:

```
ProCurveRS(config)# aaa authentication dot1x default radius
ProCurveRS(config)# radius-server host 192.168.9.22 auth-port 1812 acct-port 1813
default key mirabeau dot1x
ProCurveRS(config)# dot1x-enable e 1 to 3
ProCurveRS(config-dot1x)# re-authentication
ProCurveRS(config-dot1x)# timeout re-authperiod 2000
ProCurveRS(config-dot1x)# timeout quiet-period 30
ProCurveRS(config-dot1x)# timeout tx-period 60
ProCurveRS(config-dot1x)# max-req 6
ProCurveRS(config-dot1x)# exit
```
ProCurveRS(config)# interface e 1
ProCurveRS(config-if-e100-1)# dot1x port-control auto
ProCurveRS(config-if-e100-1)# exit
ProCurveRS(config)# interface e 2
ProCurveRS(config-if-e100-2)# dot1x port-control auto
ProCurveRS(config-if-e100-2)# exit
ProCurveRS(config)# interface e 3
ProCurveRS(config-if-e100-3)# dot1x port-control auto
ProCurveRS(config-if-e100-3)# exit

Hub Configuration (Releases Prior to 07.8.00)

Figure 4.7 illustrates a configuration where three 802.1X-enabled Clients are connected to a hub, which is connected to a port on the HP device. The configuration is similar to that in Figure 4.6, except that 802.1X port security is enabled on only one port, and the **multiple-hosts** command is used to allow multiple Clients on the port.

Figure 4.7 Sample 802.1X configuration using a hub

Clients/Supplicants running 802.1X-compliant client software
The following commands configure the HP device in Figure 4.7:

```
ProCurveRS(config)# aaa authentication dot1x default radius
ProCurveRS(config)# radius-server host 192.168.9.22 auth-port 1812 acct-port 1813
default key mirabeau dot1x
ProCurveRS(config)# dot1x-enable e 1
ProCurveRS(config-dot1x)# re-authentication
ProCurveRS(config-dot1x)# timeout re-authperiod 2000
ProCurveRS(config-dot1x)# timeout quiet-period 30
ProCurveRS(config-dot1x)# timeout tx-period 60
ProCurveRS(config-dot1x)# max-req 6
ProCurveRS(config-dot1x)# exit
ProCurveRS(config)# interface e 1
ProCurveRS(config-if-e100-1)# dot1x port-control auto
ProCurveRS(config-if-e100-1)# dot1x multiple-hosts
ProCurveRS(config-if-e100-1)# exit
```