auth-fail-action restricted-vlan
  Specifies the authentication-failure action for 802.1X multiple-host configurations. 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 use this command to specify which of these two authentication-failure actions is to be used.

  EXAMPLE:
  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
  Possible values: N/A
  Default value: If this command is not configured, traffic from a non-authenticated Client is dropped in hardware.

auth-fail-max-attempts
  Specifies the number of authentication attempts the HP device makes before dropping packets when the authentication-failure action for 802.1X multiple-host configurations is to drop traffic from the Client.

  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 use this command to configure the number of authentication attempts the device makes before dropping traffic from the Client.

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

  Syntax: [no] auth-fail-max-attempts <attempts>
  Possible values: You can specify between 1 – 10 authentication attempts.
  Default value: By default, the device makes 3 attempts to authenticate a Client before dropping packets from the Client.
auth-fail-vlanid

Specifies the ID of the restricted VLAN if the authentication-failure action in an 802.1X multiple-host configuration is to place non-authenticated Client ports in a restricted VLAN.

**EXAMPLE:**
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>

**Possible values:** VLAN ID (other than the Default VLAN)

**Default value:** None

enable

Enables 802.1X port security on the device. You can enable 802.1X port security on all interfaces at once, on individual interfaces, or on a range of interfaces.

**EXAMPLE:**
For example, to enable 802.1X port security on all interfaces on the device:

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

To enable 802.1X port security on interface 3/11:

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

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

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

**Syntax:** [no] enable all

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

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

**Possible values:** Interface number

**Default value:** By default, 802.1X port security is disabled.

end

Moves activity to the privileged EXEC level from any level of the CLI except the user EXEC level.

**EXAMPLE:**
To move to the privileged level, enter the following from any level of the CLI.

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

**Syntax:** end

**Possible values:** N/A

**Default value:** N/A

exit

Moves activity up one level from the current level. In this case, activity will be moved to the global level.

**EXAMPLE:**

```
ProCurveRS(config-dot1x)# exit
ProCurveRS(config)#
```

**Syntax:** exit

**Possible values:** N/A
Default value: N/A

**mac-session-aging max-age**

Specifies the aging time for blocked Clients in an 802.1X multiple-host configuration.

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.

**EXAMPLE:**

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>

**Possible values:** 1 – 65535 seconds

**Default value:** 120 seconds

**mac-session-aging no-aging**

Disables aging for dot1x-mac-sessions in an 802.1X multiple-host configuration.

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 use this command to disable aging of the permitted and/or denied dot1x-mac-sessions on the HP device.

**EXAMPLE:**

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

```
ProCurveRS(config-dot1x)# 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 permitted-mac-only | denied-mac-only

**Possible values:** N/A

**Default value:** N/A
maxreq
Specifies the maximum number of EAP-request/identity frame retransmissions the device sends to an 802.1X-enabled Client. If no EAP-response/identity frame is received from the Client after the specified number of EAP-request/identity frame retransmissions, the device restarts the authentication process with the Client.

**EXAMPLE:**
To configure the device to retransmit an EAP-request/identity frame to a Client a maximum of three times, enter the following command:

```
ProCurveRS(config-dot1x)# maxreq 3
```

**Syntax:** maxreq <value>

**Possible values:** 1 – 10 retransmissions

**Default value:** 2 retransmissions

**no**
Disables other commands. To disable a command, place the word no before the command.

quit
Returns you from any level of the CLI to the User EXEC mode.

**EXAMPLE:**
```
ProCurveRS(config-dot1x)# quit
ProCurveRS>
```

**Syntax:** quit

**Possible values:** N/A

**Default value:** N/A

re-authentication
Configures 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 with the `timeout re-authperiod` command.

**EXAMPLE:**
```
ProCurveRS(config-dot1x)# re-authentication
```

**Syntax:** [no] re-authentication

**Possible values:** N/A

**Default value:** N/A

servertimeout
Specifies the amount of time the device waits for a response from a RADIUS server before retransmitting the message to the RADIUS server.

**EXAMPLE:**
```
ProCurveRS(config-dot1x)# servertimeout 45
```

**Syntax:** servertimeout <seconds>

**Possible values:** 0 – 4294967295 seconds

**Default value:** 30 seconds

show
Displays a variety of configuration and statistical information about the device. See “Show Commands” on page 40-1.
**supptimeout**

Specifies the amount of time the device waits for a response from an 802.1X-enabled Client before retransmitting the EAP-Request frame to the Client.

**EXAMPLE:**

ProCurveRS(config-dot1x)# supptimeout 45

**Syntax:** supptimeout <seconds>

**Possible values:** 0 – 4294967295 seconds

**Default value:** 30 seconds

**timeout quiet-period**

If the HP device is unable to authenticate an 802.1X-enabled Client, specifies how long the device waits before trying again.

**EXAMPLE:**

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

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

**Possible values:** 0 – 4294967295 seconds

**Default value:** 60 seconds

**timeout re-authperiod**

When periodic re-authentication is enabled, specifies how often the device re-authenticates Clients. 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.

**EXAMPLE:**

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

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

**Possible values:** 0 – 4294967295 seconds

**Default value:** 3,600 seconds

**timeout security-hold-time**

Specifies the amount of time an interface is placed in the unauthorized state if multiple Clients try to connect on the interface (provided that the `multiple-hosts` command is not used).

**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.

**EXAMPLE:**

ProCurveRS(config-dot1x)# timeout security-hold-time 120

**Syntax:** [no] timeout security-hold-time <seconds>

**Possible values:** 0 – 4294967295 seconds

**Default value:** 60 seconds

**timeout tx-period**

Specifies how long the device waits for a Client to send back an EAP-response/identity frame after the device has sent an EAP-request/identity frame. If the Client does not send back an EAP-response/identity frame during this time, the device retransmits the EAP-request/identity frame.
**EXAMPLE:**
ProCurveRS(config-dot1x)# timeout tx-period 60

**Syntax:** [no] timeout tx-period <seconds>

**Possible values:** 0 – 4294967295 seconds

**Default value:** 30 seconds

**write memory**
Saves the running configuration into the startup-config file.

**EXAMPLE:**
ProCurveRS(config-port-security)# wr mem

**Syntax:** write memory

**Possible values:** N/A

**Default value:** N/A

**write terminal**
Displays the running configuration of the HP device on the terminal screen.

**NOTE:** This command is equivalent to the `show running-config` command.

**EXAMPLE:**
ProCurveRS(config-port-security)# wr term

**Syntax:** write terminal

**Possible values:** N/A

**Default value:** N/A