Overview

Multi-device port authentication is a way to configure an HP device to forward or block traffic from a MAC address based on information received from a RADIUS server.

This chapter is divided into the following sections:

- “How Multi-Device Port Authentication Works” below explains basic concepts about multi-device port authentication.
- “Configuring Multi-Device Port Authentication” on page 6-2 describes how to set up multi-device port authentication on HP devices using the Command Line Interface (CLI).
- “Displaying Multi-Device Port Authentication Information” on page 6-8 describes the commands used to display information about a multi-device port authentication configuration.

NOTE: This feature is supported on HP devices running Enterprise software release 07.6.06 or higher.

How Multi-Device Port Authentication Works

The multi-device port authentication feature is a mechanism by which incoming traffic originating from a specific MAC address is switched or forwarded by the device only if the source MAC address is successfully authenticated by a RADIUS server. The MAC address itself is used as the username and password for RADIUS authentication; the user does not need to provide a specific username and password to gain access to the network. If RADIUS authentication for the MAC address is successful, traffic from the MAC address is forwarded in hardware.

If the RADIUS server cannot validate the user's MAC address, then it is considered an authentication failure, and a specified authentication-failure action can be taken. The default authentication-failure action is to drop traffic from the non-authenticated MAC address in hardware. You can also configure the device to move the port on which the non-authenticated MAC address was learned into a restricted or “guest” VLAN, which may have limited access to the network.

RADIUS Authentication

The multi-device port authentication feature communicates with the RADIUS server to authenticate a newly found MAC address. The HP device supports multiple RADIUS servers; if communication with one of the RADIUS servers times out, the others are tried in sequential order. If a response from a RADIUS server is not received within a specified time (by default, 3 seconds) the RADIUS session times out, and the device retries the request up to three times. If no response is received, the next RADIUS server is chosen, and the request is sent for authentication.
The RADIUS server is configured with the usernames and passwords of authenticated users. For multi-device port authentication, the username and password is the MAC address itself; that is, the device uses the MAC address for both the username and the password in the request sent to the RADIUS server. For example, given a MAC address of 0007e90feaa1, the users file on the RADIUS server would be configured with a username and password both set to 0007e90feaa1. When traffic from this MAC address is encountered on a MAC-authentication-enabled interface, the device sends the RADIUS server an Access-Request message with 0007e90feaa1 as both the username and password. The format of the MAC address sent to the RADIUS server is configurable through the CLI.

The request for authentication from the RADIUS server is successful only if the username and password provided in the request matches an entry in the users database on the RADIUS server. When this happens, the RADIUS server returns an Access-Accept message back to the HP device. When the RADIUS server returns an Access-Accept message for a MAC address, that MAC address is considered authenticated, and traffic from the MAC address is forwarded normally by the HP device.

**Authentication-Failure Actions**

If the MAC address does not match the username and password of an entry in the users database on the RADIUS server, then the RADIUS server returns an Access-Reject message. When this happens, it is considered an authentication failure for the MAC address. When an authentication failure occurs, the HP device can either drop traffic from the MAC address in hardware (the default), or move the port on which the traffic was received to a restricted VLAN.

**Dynamic VLAN Assignment**

The multi-device port authentication feature supports *dynamic VLAN assignment*, where a port can be placed in a VLAN based on the MAC address learned on that interface. When a MAC address is successfully authenticated, the RADIUS server sends the HP device a RADIUS Access-Accept message that allows the HP device to forward traffic from that MAC address. The RADIUS Access-Accept message can also contain attributes set for the MAC address in its 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 port is moved from its default VLAN to the specified VLAN.

To enable dynamic VLAN assignment for authenticated MAC addresses, you must add the following attributes to the profile for the MAC address on the RADIUS server, then enable dynamic VLAN assignment on multi-device port authentication-enabled interfaces.

<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>

**Support for Authenticating Multiple MAC Addresses on an Interface**

The multi-device port authentication feature allows multiple MAC addresses to be authenticated or denied authentication on each interface. The maximum number of MAC addresses that can be authenticated on each interface is limited only by the amount of system resources available on the HP device.

**Configuring Multi-Device Port Authentication**

Configuring multi-device port authentication on the HP device consists of the following tasks:

- Enabling multi-device port authentication globally and on individual interfaces
- Specifying the format of the MAC addresses sent to the RADIUS server (optional)
Configuring Multi-Device Port Authentication

- Specifying the authentication-failure action (optional)
- Defining MAC address filters (optional)
- Configuring dynamic VLAN assignment (optional)
- Specifying to which VLAN a port is moved after its RADIUS-specified VLAN assignment expires (optional)
- Saving dynamic VLAN assignments to the startup-config file (optional)
- Enabling denial of service attack protection (optional)
- Clearing authenticated MAC addresses (optional)
- Disabling aging for authenticated MAC addresses (optional)
- Specifying the aging time for blocked MAC addresses (optional)

Enabling Multi-Device Port Authentication

To enable multi-device port authentication, you first enable the feature globally on the device, then enable it on individual interfaces.

To globally enable multi-device port authentication on the device, enter the following command:

```
ProCurveRS(config)# mac-authentication enable
```

**Syntax:** `[no] mac-authentication enable`

To enable multi-device port authentication on an individual interface, enter a command such as the following:

```
ProCurveRS(config)# mac-authentication enable ethernet 3/1
```

**Syntax:** `[no] mac-authentication enable <portnum> | all`

The all option enables the feature on all interfaces at once.

You can enable the feature on an interface at the interface CONFIG level. For example:

```
ProCurveRS(config)# interface e 3/1
ProCurveRS(config-if-e100-3/1)# mac-authentication enable
```

**Syntax:** `[no] mac-authentication enable

You can also configure multi-device port authentication commands on a range of interfaces. For example:

```
ProCurveRS(config)# int e 3/1 to 3/12
ProCurveRS(config-mif-3/1-3/12)# mac-authentication enable
```

Specifying the Format of the MAC Addresses Sent to the RADIUS Server

When multi-device port authentication is configured, the HP device authenticates MAC addresses by sending username and password information to a RADIUS server. The username and password is the MAC address itself; that is, the device uses the MAC address for both the username and the password in the request sent to the RADIUS server.

By default, the MAC address is sent to the RADIUS server in the format xxxxxxxxxx. You can optionally configure the device to send the MAC address to the RADIUS server in the format xx-xx-xx-xx-xx-xx, or the format xxxxx.xxxx.xxxx. To do this, enter a command such as the following:

```
ProCurveRS(config)# mac-authentication auth-passwd-format xxxx.xxxx.xxxx
```

**Syntax:** `[no] mac-authentication auth-passwd-format xxxx.xxxx.xxxx | xx-xx-xx-xx-xx-xx | xxxxx.xxxx.xxxx`

Specifying the Authentication-Failure Action

When RADIUS authentication for a MAC address fails, you can configure the device to perform one of two actions:

- Drop traffic from the MAC address in hardware (the default)
- Move the port on which the traffic was received to a restricted VLAN
To configure the device to move the port to a restricted VLAN when multi-device port authentication fails, enter commands such as the following:

```bash
ProCurveRS(config)# interface e 3/1
ProCurveRS(config-if-e100-3/1)# mac-authentication auth-fail-action restrict-vlan 100
```

**Syntax:** [no] mac-authentication auth-fail-action restrict-vlan [<vlan-id>]

If the ID for the restricted VLAN is not specified at the interface level, the global restricted VLAN ID applies for the interface.

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

```bash
ProCurveRS(config)# mac-authentication auth-fail-vlan-id 200
```

**Syntax:** [no] mac-authentication auth-fail-vlan-id <vlan-id>

The command above applies globally to all MAC-authentication-enabled interfaces.

Note that the restricted VLAN must already exist on the device. You cannot configure the restricted VLAN to be a non-existent VLAN. If the port is a tagged or dual-mode port, you cannot use a restricted VLAN as the authentication-failure action.

To configure the device to drop traffic from non-authenticated MAC addresses in hardware, enter commands such as the following:

```bash
ProCurveRS(config)# interface e 3/1
ProCurveRS(config-if-e100-3/1)# mac-authentication auth-fail-action block-traffic
```

**Syntax:** [no] mac-authentication auth-fail-action block-traffic

Dropping traffic from non-authenticated MAC addresses is the default behavior when multi-device port authentication is enabled.

**Defining MAC Address Filters**

You can specify MAC addresses that do not have to go through multi-device port authentication. These MAC addresses are considered pre-authenticated, and are not subject to RADIUS authentication. To do this, you can define MAC address filters that specify the MAC addresses to exclude from multi-device port authentication.

You should use a MAC address filter when the RADIUS server itself is connected to an interface where multi-device port authentication is enabled. If a MAC address filter is not defined for the MAC address of the RADIUS server and applied on the interface, the RADIUS authentication process would fail since the device would drop all packets from the RADIUS server itself.

For example, the following command defines a MAC address filter for address 0010.dc58.aca4:

```bash
ProCurveRS(config)# mac-authentication mac-filter 1 permit 0010.dc58.aca4
```

**Syntax:** [no] mac-authentication mac-filter <filter>

The following commands apply the MAC address filter on an interface so that address 0010.dc58.aca4 is excluded from multi-device port authentication:

```bash
ProCurveRS(config)# interface e 3/1
ProCurveRS(config-if-e100-3/1)# mac-authentication apply-mac-auth-filter 1
```

**Syntax:** [no] mac-authentication apply-mac-auth-filter <filter-id>

**Configuring Dynamic VLAN Assignment**

An interface can be dynamically assigned to a VLAN based on the MAC address learned on that interface. When a MAC address is successfully authenticated, the RADIUS server sends the HP device a RADIUS Access-Accept message that allows the HP device to forward traffic from that MAC address. The RADIUS Access-Accept message can also contain attributes set for the MAC address in its 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 port is moved from its default VLAN to the specified VLAN.

To enable dynamic VLAN assignment for authenticated MAC addresses, you must add the following attributes to the profile for the MAC address on the RADIUS server, then enable dynamic VLAN assignment on multi-device port authentication-enabled interfaces. See “Dynamic VLAN Assignment” on page 6-2 for a list of the attributes that must be set on the RADIUS server.

To enable dynamic VLAN assignment on a multi-device port authentication-enabled interface, enter commands such as the following:

```
ProCurveRS(config)# interface e 3/1
ProCurveRS(config-if-e100-3/1)# mac-authentication enable-dynamic-vlan
```

**Syntax:** `[no] mac-authentication enable-dynamic-vlan`

If a previous authentication attempt for a MAC address failed, and as a result the port was placed in the restricted VLAN, but a subsequent authentication attempt was successful, the RADIUS Access-Accept message may specify a VLAN for the port. By default, the HP device moves the port out of the restricted VLAN and into the RADIUS-specified VLAN. You can optionally configure the device to ignore the RADIUS-specified VLAN in the RADIUS Access-Accept message, and leave the port in the restricted VLAN.

To do this, enter the following command:

```
ProCurveRS(config)# mac-authentication no-override-restrict-vlan
```

**Syntax:** `[no] mac-authentication no-override-restrict-vlan`

**Notes:**

- For untagged ports, if the VLAN ID provided by the RADIUS server is valid, then the port is removed from its current VLAN and moved to the RADIUS-specified VLAN as an untagged port.
- For tagged ports, if the VLAN ID provided by the RADIUS server is valid, then the port is added to the RADIUS-specified VLAN as a tagged port.
- If you configure dynamic VLAN assignment on a multi-device port authentication enabled interface, and the Access-Accept message returned by the RADIUS server does not contain a Tunnel-Private-Group-ID attribute, then it is considered an authentication failure, and the configured authentication failure action is performed for the MAC address.
- If the `<vlan-name>` string does not match either the name or the ID of a VLAN configured on the device, then it is considered an authentication failure, and the configured authentication failure action is performed for the MAC address.
- For tagged or dual-mode ports, if the VLAN ID provided by the RADIUS server does not match the VLAN ID in the tagged packet that contains the authenticated MAC address as its source address, then it is considered an authentication failure, and the configured authentication failure action is performed for the MAC address.
- If an untagged port had previously been assigned to a VLAN though dynamic VLAN assignment, and then another MAC address is authenticated on the same port, but the RADIUS Access-Accept message for the second MAC address specifies a different VLAN, then it is considered an authentication failure for the second MAC address, and the configured authentication failure action is performed. Note that this applies only if the first MAC address has not yet aged out. If the first MAC address has aged out, then dynamic VLAN assignment would work as expected for the second MAC address.

**Specifying to Which VLAN a Port Is Moved After Its RADIUS-Specified VLAN Assignment Expires**

When a port is dynamically assigned to a VLAN through the authentication of a MAC address, and the MAC session for that address is deleted on the HP device, then by default the port is removed from its RADIUS-assigned VLAN and placed back in the VLAN where it was originally assigned.

A port can be removed from its RADIUS-assigned VLAN when any of the following occur:

- The link goes down for the port
The MAC session is manually deleted with the **mac-authentication clear-mac-session** command.

The MAC address that caused the port to be dynamically assigned to a VLAN ages out.

For example, say port 1/1 is currently in VLAN 100, to which it was assigned when MAC address 0007.eaa1.e90f was authenticated by a RADIUS server. The port was originally configured to be in VLAN 111. If the MAC session for address 0007.eaa1.e90f is deleted, then port 1/1 is moved from VLAN 100 back into VLAN 111.

You can optionally specify an alternate VLAN to which to move the port when the MAC session for the address is deleted. For example, to place the port in the restricted VLAN, enter commands such as the following:

```
ProCurveRS(config)# interface e 3/1
ProCurveRS(config-if-e100-3/1)# mac-auth move-back-to-old-vlan port-restrict-vlan
```

**Syntax:** `[no] mac-authentication move-back-to-old-vlan disable | port-configured-vlan | system-default-vlan`

- The **disable** keyword disables moving the port back to its original VLAN. The port would stay in its RADIUS-assigned VLAN.
- The **port-configured-vlan** keyword removes the port from its RADIUS-assigned VLAN and places it back in the VLAN where it was originally assigned. This is the default.
- The **port-restrict-vlan** keyword removes the port from its RADIUS-assigned VLAN and places it in the restricted VLAN.
- The **system-default-vlan** keyword removes the port from its RADIUS-assigned VLAN and places it in the DEFAULT-VLAN.

### Saving Dynamic VLAN Assignments to the Startup-Config File

You can configure the HP device to save the RADIUS-specified VLAN assignments to the device's startup-config file. To do this, enter the following command:

```
ProCurveRS(config)# mac-authentication save-dynamicvlan-to-config
```

**Syntax:** `[no] mac-authentication save-dynamicvlan-to-config`

By default, the dynamic VLAN assignments are not saved to the startup-config file. Entering the `show running-config` command does not display dynamic VLAN assignments, although they can be displayed with the `show vlan` and `show authenticated-mac-address detail` commands.

### Enabling Denial of Service Attack Protection

The HP device does not start forwarding traffic from an authenticated MAC address in hardware until the RADIUS server authenticates the MAC address; traffic from the non-authenticated MAC addresses is sent to the CPU. A denial of service (DoS) attack could be launched against the device where a high volume of new source MAC addresses is sent to the device, causing the CPU to be overwhelmed with performing RADIUS authentication for these MAC addresses. In addition, the high CPU usage in such an attack could prevent the RADIUS response from reaching the CPU in time, causing the device to make additional authentication attempts.

To limit the susceptibility of the HP device to such attacks, you can configure the device to use multiple RADIUS servers, which can share the load when there are a large number of MAC addresses that need to be authenticated. The HP device can run a maximum of 10 RADIUS clients per server and will attempt to authenticate with a new RADIUS server if current one times out.

In addition, you can configure the HP device to limit the rate of authentication attempts sent to the RADIUS server. When the multi-device port authentication feature is enabled, it keeps track of the number of RADIUS authentication attempts made per second. When you also enable the DoS protection feature, if the number of RADIUS authentication attempts for MAC addresses learned on an interface per second exceeds a configurable rate (by default 512 authentication attempts per second), the device considers this a possible DoS attack and disables the port. You must then manually re-enable the port.

The DoS protection feature is disabled by default. To enable it on an interface, enter commands such as the following:

```
ProCurveRS(config)# interface e 3/1
```
Configuring Multi-Device Port Authentication

ProCurveRS(config-if-e100-3/1)# mac-authentication dos-protection enable

**Syntax:** [no] mac-authentication dos-protection enable

To specify a maximum rate for RADIUS authentication attempts, enter commands such as the following:

ProCurveRS(config)# interface e 3/1
ProCurveRS(config-if-e100-3/1)# mac-authentication dos-protection mac-limit 256

**Syntax:** [no] mac-authentication dos-protection mac-limit <number>

You can specify a rate from 1 – 65535 authentication attempts per second. The default is a rate of 512 authentication attempts per second.

Clearing Authenticated MAC Addresses

The HP device maintains an internal table of the authenticated MAC addresses (viewable with the *show authenticated-mac-address* command). You can clear the contents of the authenticated MAC address table either entirely, or just for the entries learned on a specified interface. In addition, you can clear the MAC session for an address learned on a specific interface.

To clear the entire contents of the authenticated MAC address table, enter the following command:

ProCurveRS(config)# clear auth-mac-table

**Syntax:** clear auth-mac-table

To clear the authenticated MAC address table of entries learned on a specified interface, enter a command such as the following:

ProCurveRS(config)# clear auth-mac-table e 3/1

**Syntax:** clear auth-mac-table <portnum>

To clear the MAC session for an address learned on a specific interface, enter commands such as the following:

ProCurveRS(config)# interface e 3/1
ProCurveRS(config-if-e100-3/1)# mac-authentication clear-mac-session 00e0.1234.abd4

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

This command removes the Layer 2 CAM entry created for the specified MAC address. If the HP device receives traffic from the MAC address again, the MAC address is authenticated again.

Disabling Aging for Authenticated MAC Addresses

MAC addresses that have been authenticated or denied by a RADIUS server are aged out if no traffic is received from the MAC address for a certain period of time.

- Authenticated MAC addresses or non-authenticated MAC addresses that have been placed in the restricted VLAN are aged out if no traffic is received from the MAC address over the device’s normal MAC aging interval.

- Non-authenticated MAC addresses that are blocked by the device are aged out if no traffic is received from the 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 for MAC addresses subject to authentication, either for all MAC addresses or for those learned on a specified interface.

To disable aging for all MAC addresses subject to authentication on all interfaces where multi-device port authentication has been enabled, enter the following command:

ProCurveRS(config)# mac-authentication disable-aging

To disable aging for all MAC addresses subject to authentication on a specific interface where multi-device port authentication has been enabled, enter commands such as the following:

ProCurveRS(config)# interface e 3/1
ProCurveRS(config-if-e100-3/1)# mac-authentication disable-aging

Syntax: [no] mac-authentication disable-aging

Specifying the Aging Time for Blocked MAC Addresses

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

Aging of the Layer 2 CAM entry for a blocked 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 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 MAC address ages out, and can be authenticated again if the HP device receives traffic from the MAC address.

To change the length of the software aging period for blocked MAC addresses, enter a command such as the following:

ProCurveRS(config)# mac-authentication max-age 180

Syntax: [no] mac-authentication max-age <seconds>

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

Displaying Multi-Device Port Authentication Information

You can display the following information about the multi-device port authentication configuration:

- Information about authenticated MAC addresses
- Information about the multi-device port authentication configuration
- Authentication Information for a specific MAC address or port
- Multi-device port authentication settings and authenticated MAC addresses for each port where the multi-device port authentication feature is enabled
- The MAC addresses that have been successfully authenticated
- The MAC addresses for which authentication was not successful

Displaying Authenticated MAC Address Information

To display information about authenticated MAC addresses on the ports where the multi-device port authentication feature is enabled, enter the following command:

ProCurveRS# show authenticated-mac-address

<table>
<thead>
<tr>
<th>Port</th>
<th>Vlan</th>
<th>Accepted MACs</th>
<th>Rejected MACs</th>
<th>Attempted-MACs</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/18</td>
<td>100</td>
<td>1</td>
<td>100</td>
<td>0</td>
</tr>
<tr>
<td>1/20</td>
<td>40</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1/22</td>
<td>100</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>4/5</td>
<td>30</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Syntax: show authenticated-mac-address
The following table describes the information displayed by the `show authenticated-mac-address` command.

Table 6.1: Output from the `show authenticated-mac-address` command

<table>
<thead>
<tr>
<th>This Field...</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>The port number where the multi-device port authentication feature is enabled.</td>
</tr>
<tr>
<td>Vlan</td>
<td>The VLAN to which the port has been assigned.</td>
</tr>
<tr>
<td>Accepted MACs</td>
<td>The number of MAC addresses that have been successfully authenticated</td>
</tr>
<tr>
<td>Rejected MACs</td>
<td>The number of MAC addresses for which authentication has failed.</td>
</tr>
<tr>
<td>Attempted-MACs</td>
<td>The rate at which authentication attempts are made for MAC addresses.</td>
</tr>
</tbody>
</table>

Displaying Multi-Device Port Authentication Configuration Information

To display information about the multi-device port authentication configuration, enter the following command:

```
ProCurveRS# show authenticated-mac-address configuration
```

<table>
<thead>
<tr>
<th>Feature enabled</th>
<th>: Yes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Ports enabled</td>
<td>: 4</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-------</td>
</tr>
<tr>
<td>Port Fail-Action Fail-vlan Dyn-vlan MAC-filter</td>
<td>-------</td>
</tr>
<tr>
<td>1/18 Block Traffic 1 No No</td>
<td>-------</td>
</tr>
<tr>
<td>1/20 Block Traffic 1 No No</td>
<td>-------</td>
</tr>
<tr>
<td>1/22 Block Traffic 1 No Yes</td>
<td>-------</td>
</tr>
<tr>
<td>4/5 Block Traffic 1 No No</td>
<td>-------</td>
</tr>
</tbody>
</table>

**Syntax**: `show authenticated-mac-address configuration`

The following table describes the information displayed by the `show authenticated-mac-address configuration` command.

Table 6.2: Output from the `show authenticated-mac-address configuration` command

<table>
<thead>
<tr>
<th>This Field...</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Feature enabled</td>
<td>Whether the multi-device port authentication feature is enabled on the HP device.</td>
</tr>
<tr>
<td>Number of Ports enabled</td>
<td>The number of ports on which the multi-device port authentication feature is enabled.</td>
</tr>
<tr>
<td>Port</td>
<td>Information for each multi-device port authentication-enabled port.</td>
</tr>
<tr>
<td>Fail-Action</td>
<td>What happens to traffic from a MAC address for which RADIUS authentication has failed: either block the traffic or assign the MAC address to a restricted VLAN.</td>
</tr>
</tbody>
</table>
Table 6.2: Output from the show authenticated-mac-address configuration command (Continued)

<table>
<thead>
<tr>
<th>This Field...</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fail-vlan</td>
<td>The restricted VLAN to which non-authenticated MAC addresses are assigned, if the Fail-Action is to assign the MAC address to a restricted VLAN.</td>
</tr>
<tr>
<td>Dyn-vlan</td>
<td>Whether RADIUS dynamic VLAN assignment is enabled for the port.</td>
</tr>
<tr>
<td>MAC-filter</td>
<td>Whether a MAC filter has been applied to this port to specify pre-authenticated MAC addresses.</td>
</tr>
</tbody>
</table>

Displaying Multi-Device Port Authentication Information for a Specific MAC Address or Port

To display authentication information for a specific MAC address or port, enter a command such as the following:

ProCurveRS# show authenticated-mac-address 0007.e90f.ea1

<table>
<thead>
<tr>
<th>MAC/IP Address</th>
<th>Port</th>
<th>Vlan</th>
<th>Authenticated Time</th>
<th>Age</th>
<th>CAM Index</th>
</tr>
</thead>
<tbody>
<tr>
<td>0007.e90f.ea1</td>
<td>1/18</td>
<td>100</td>
<td>00d01h10m06s</td>
<td>0</td>
<td>N/A</td>
</tr>
</tbody>
</table>

**Syntax:** show authenticated-mac-address <mac-address> | <ip-address> | <portnum>

The <ip-address> parameter lists the MAC address associated with the specified IP address.

The <portnum> parameter lists the MAC addresses on the specified port.

The following table describes the information displayed by the `show authenticated-mac-address` command for a specified MAC address or port.

Table 6.3: Output from the show authenticated-mac-address <address> command

<table>
<thead>
<tr>
<th>This Field...</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC/IP Address</td>
<td>The MAC address for which information is displayed. If the packet for which multi-device port authentication was performed also contained an IP address, then the IP address is displayed as well.</td>
</tr>
<tr>
<td>Port</td>
<td>The port on which the MAC address was learned.</td>
</tr>
<tr>
<td>Vlan</td>
<td>The VLAN to which the MAC address was assigned.</td>
</tr>
<tr>
<td>Authenticated</td>
<td>Whether the MAC address was authenticated.</td>
</tr>
<tr>
<td>Time</td>
<td>The time at which the MAC address was authenticated. If the clock is set on the HP device, then the actual date and time are displayed. If the clock has not been set, then the time is displayed relative to when the device was last restarted.</td>
</tr>
<tr>
<td>Age</td>
<td>The age of the MAC address entry in the authenticated MAC address list.</td>
</tr>
</tbody>
</table>
**Table 6.3: Output from the show authenticated-mac-address <address> command (Continued)**

<table>
<thead>
<tr>
<th>This Field...</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<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 Multi-Device Port Authentication Settings and Authenticated MAC Addresses**

To display the multi-device port authentication settings and authenticated MAC addresses for a port where the feature is enabled, enter the following command:

```
ProCurveRS# show authenticated-mac-address detail e 1/18
```

<table>
<thead>
<tr>
<th>Port</th>
<th>Dynamic-Vlan Assignment</th>
<th>RADIUS failure action</th>
<th>Override-restrict-vlan</th>
<th>Vlan</th>
<th>DOS attack protection</th>
<th>Accepted Mac Addresses</th>
<th>Rejected Mac Addresses</th>
<th>Authentication in progress</th>
<th>Authentication attempts</th>
<th>RADIUS timeouts</th>
<th>Aging of MAC-sessions</th>
<th>Max-Age of MAC-sessions</th>
<th>MAC Filter applied</th>
<th>MAC/IP Address</th>
<th>RADIUS Server</th>
<th>Authenticated</th>
<th>Time</th>
<th>Age</th>
<th>CAM Index</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/18</td>
<td>Disabled</td>
<td>Block Traffic</td>
<td>No</td>
<td>100</td>
<td>( RADIUS assigned: No)</td>
<td>100</td>
<td>0</td>
<td>0</td>
<td>61250</td>
<td>Enabled</td>
<td>120 seconds</td>
<td></td>
<td>No</td>
<td>00e0.1234.abd4</td>
<td>25.25.25.20</td>
<td>No</td>
<td>00d06h32m50s</td>
<td>224</td>
<td>083d</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>00e0.1234.abd5</td>
<td>25.25.25.20</td>
<td>No</td>
<td>00d06h32m50s</td>
<td>225</td>
<td>0843</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>00e0.1234.abd6</td>
<td>25.25.25.20</td>
<td>No</td>
<td>00d06h34m10s</td>
<td>216</td>
<td>084f</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>00e0.1234.abd7</td>
<td>25.25.25.20</td>
<td>No</td>
<td>00d06h34m50s</td>
<td>212</td>
<td>0862</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>00e0.1234.abd0</td>
<td>25.25.25.20</td>
<td>No</td>
<td>00d06h34m10s</td>
<td>217</td>
<td>081d</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>00e0.1234.abd1</td>
<td>25.25.25.20</td>
<td>No</td>
<td>00d06h32m50s</td>
<td>223</td>
<td>083a</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>00e0.1234.abd2</td>
<td>25.25.25.20</td>
<td>No</td>
<td>00d06h38m50s</td>
<td>189</td>
<td>0813</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>00e0.1234.abd3</td>
<td>25.25.25.20</td>
<td>No</td>
<td>00d06h32m50s</td>
<td>225</td>
<td>0840</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>00e0.1234.abdc</td>
<td>25.25.25.20</td>
<td>No</td>
<td>00d06h34m50s</td>
<td>211</td>
<td>0816</td>
</tr>
</tbody>
</table>

**Syntax:** `show authenticated-mac-address [<portnum>]`

Omitting the `<portnum>` parameter displays information for all interfaces where the multi-device port authentication feature is enabled.
The following table describes the information displayed by the `show authenticated-mac-address` command.

<table>
<thead>
<tr>
<th>This Field...</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>The port to which this information applies.</td>
</tr>
<tr>
<td>Dynamic-Vlan Assignment</td>
<td>Whether RADIUS dynamic VLAN assignment has been enabled for the port.</td>
</tr>
<tr>
<td>RADIUS failure action</td>
<td>What happens to traffic from a MAC address for which RADIUS authentication has failed: either block the traffic or assign the MAC address to a restricted VLAN.</td>
</tr>
<tr>
<td>No-override-restrict-vlan</td>
<td>Whether a port can be dynamically assigned to a VLAN specified by a RADIUS server, if the port had been previously placed in the restricted VLAN because a previous attempt at authenticating a MAC address on that port failed.</td>
</tr>
<tr>
<td>Vlan</td>
<td>The VLAN to which the port is assigned, and whether the port had been dynamically assigned to the VLAN by a RADIUS server.</td>
</tr>
<tr>
<td>DOS attack protection</td>
<td>Whether denial of service attack protection has been enabled for multi-device port authentication, limiting the rate of authentication attempts sent to the RADIUS server.</td>
</tr>
<tr>
<td>Accepted Mac Addresses</td>
<td>The number of MAC addresses that have been successfully authenticated.</td>
</tr>
<tr>
<td>Rejected Mac Addresses</td>
<td>The number of MAC addresses for which authentication has failed.</td>
</tr>
<tr>
<td>Authentication in progress</td>
<td>The number of MAC addresses for which authentication is pending.</td>
</tr>
<tr>
<td>Authentication attempts</td>
<td>The total number of authentication attempts made for MAC addresses on an interface, including pending authentication attempts.</td>
</tr>
<tr>
<td>RADIUS timeouts</td>
<td>The number of times the session between the HP device and the RADIUS server timed out.</td>
</tr>
<tr>
<td>Aging of MAC-sessions</td>
<td>Whether software aging of MAC addresses is enabled.</td>
</tr>
<tr>
<td>Max-Age of MAC-sessions</td>
<td>The configured software aging period.</td>
</tr>
<tr>
<td>MAC Filter applied</td>
<td>Whether a MAC filter has been applied to this port to specify pre-authenticated MAC addresses.</td>
</tr>
<tr>
<td>MAC/IP Address</td>
<td>The MAC addresses learned on the port. If the packet for which multi-device port authentication was performed also contained an IP address, then the IP address is displayed as well.</td>
</tr>
<tr>
<td>RADIUS Server</td>
<td>The IP address of the RADIUS server used for authenticating the MAC addresses.</td>
</tr>
<tr>
<td>Authenticated</td>
<td>Whether the MAC address has been authenticated by the RADIUS server.</td>
</tr>
</tbody>
</table>
Table 6.4: Output from the show authenticated-mac-address command (Continued)

<table>
<thead>
<tr>
<th>This Field...</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time</td>
<td>The time at which the MAC address was authenticated. If the clock is set on the HP device, then the actual date and time are displayed. If the clock has not been set, then the time is displayed relative to when the device was last restarted.</td>
</tr>
<tr>
<td>Age</td>
<td>The age of the MAC address entry in the authenticated MAC address list.</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 the Authenticated MAC Addresses**

To display the MAC addresses that have been successfully authenticated, enter the following command:

`ProCurveRS# show auth-mac-addresses authorized-mac`

*Syntax:* show auth-mac-addresses authorized-mac

**Displaying the Non-Authenticated MAC Addresses**

To display the MAC addresses for which authentication was not successful, enter the following command:

`ProCurveRS# show auth-mac-addresses unauthorized-mac`

*Syntax:* show auth-mac-addresses unauthorized-mac