

Web and MAC Authentication

Contents

Overview	4-2
Web Authentication	4-2
MAC Authentication	4-3
Authorized and Unauthorized Client VLANs	4-3
RADIUS-Based Authentication	4-4
Wireless Clients	4-4
How Web and MAC Authentication Operate	4-5
Web-based Authentication	4-5
Customized Login Web Pages	4-8
MAC-based Authentication	4-8
Terminology	4-10
Operating Rules and Notes	4-11
Setup Procedure for Web/MAC Authentication	4-13
Before You Configure Web/MAC Authentication	4-13
Configuring the RADIUS Server To Support MAC Authentication ..	4-16
Using Customized Login Web Pages for Enhanced Web Authentication	4-16
Configuring a DNS Server for Enhanced Web Authentication	4-27
Configuring the Switch To Access a RADIUS Server	4-27
Configuring Web Authentication	4-29
Configuration Commands for Web Authentication	4-31
Show Commands for Web Authentication	4-38
Configuring MAC Authentication on the Switch	4-44
Configuration Commands for MAC Authentication	4-45
Show Commands for MAC-Based Authentication	4-48
Client Status	4-54

Overview

Feature	Default	Menu	CLI	Web
Configure Web Authentication	n/a	—	4-17	—
Configure MAC Authentication	n/a	—	4-32	—
Display Web Authentication Status and Configuration	n/a	—	4-26	—
Display MAC Authentication Status and Configuration	n/a	—	4-36	—

Web and MAC authentication are designed for employment on the “edge” of a network to provide port-based security measures for protecting private networks and a switch from unauthorized access. Because neither method requires clients to run special supplicant software (unlike 802.1X authentication), both Web and MAC authentication are suitable for legacy systems and temporary access situations where introducing supplicant software is not an attractive option. Only a web browser (for Web authentication) or a MAC address (for MAC authentication) is required.

Both Web and MAC authentication methods rely on a RADIUS server to authenticate network access. This simplifies access security management by allowing you to control access from a master database in a single server. (You can use up to three RADIUS servers to provide backups in case access to the primary server fails.) It also means the same credentials can be used for authentication, regardless of which switch or switch port is the current access point into the LAN.

On a port configured for Web or MAC Authentication, the switch operates as a port-access authenticator using a RADIUS server and the CHAP protocol. Inbound traffic is processed by the switch alone, until authentication occurs. Some traffic from the switch to an unauthorized client is supported (for example, broadcast or unknown destination packets) before authentication occurs.

Web Authentication

The Web Authentication (Web-Auth) method uses a web page login to authenticate users for access to the network. When a client connects to the switch and opens a web browser, the switch automatically presents a login page.

Note

A proxy server is not supported for use by a browser on a client device that accesses the network through a port configured for web authentication.

- In the login page, a client enters a username and password, which the switch forwards to a RADIUS server for authentication. After authenticating a client, the switch grants access to the secured network. Besides a web browser, the client needs no special supplicant software.

MAC Authentication

The MAC Authentication (MAC-Auth) method grants access to a secure network by authenticating devices for access to the network. When a device connects to the switch, either by direct link or through the network, the switch forwards the device's MAC address to the RADIUS server for authentication. The RADIUS server uses the device MAC address as the username and password, and grants or denies network access in the same way that it does for clients capable of interactive logons. (The process does not use either a client device configuration or a logon session.) MAC authentication is well-suited for clients that are not capable of providing interactive logons, such as telephones, printers, and wireless access points. Also, because most RADIUS servers allow for authentication to depend on the source switch and port through which the client connects to the network, you can use MAC-Auth to “lock” a particular device to a specific switch and port.

Note

802.1X port-access and either Web authentication or MAC authentication can be configured at the same time on the same port. A maximum of 32 clients is supported on the port. (The default is one client.)

Web authentication, MAC authentication, MAC lockdown, MAC lockout, and port-security are mutually exclusive on a given port. If you configure any of these authentication methods on a port, you must disable LACP on the port.

Authorized and Unauthorized Client VLANs

Web-Auth and MAC-Auth provide a port-based solution in which a port belongs to one, untagged VLAN at a time. The switch supports up to 32 simultaneous client sessions per port. All authenticated client sessions operate in the same untagged VLAN. (If you want the switch to simultaneously support multiple client sessions in different VLANs for a network application, design your system so that clients request network access on different switch ports.)

In the default configuration, the switch blocks access to all clients that the RADIUS server does not authenticate. However, you can configure an individual port to provide limited network services and access to unauthorized clients by using an “unauthorized” VLAN for each session. The unauthorized VLAN ID assignment can be the same for all ports, or different, depending on the services and access you plan to allow for unauthenticated clients.

You configure access to an optional, unauthorized VLAN when you configure Web and MAC authentication on a port.

RADIUS-Based Authentication

In Web and MAC authentication, you use a RADIUS server to temporarily assign a port to a static VLAN to support an authenticated client. When a RADIUS server authenticates a client, the switch-port membership during the client’s connection is determined according to the following hierarchy:

1. A RADIUS-assigned VLAN
2. An authorized VLAN specified in the Web- or MAC-Auth configuration for the subject port.
3. A static, port-based, untagged VLAN to which the port is configured. A RADIUS-assigned VLAN has priority over switch-port membership in any VLAN.

Wireless Clients

You can allow wireless clients to move between switch ports under Web/MAC Authentication control. Clients may move from one Web-authorized port to another or from one MAC-authorized port to another. This capability allows wireless clients to move from one access point to another without having to reauthenticate.

How Web and MAC Authentication Operate

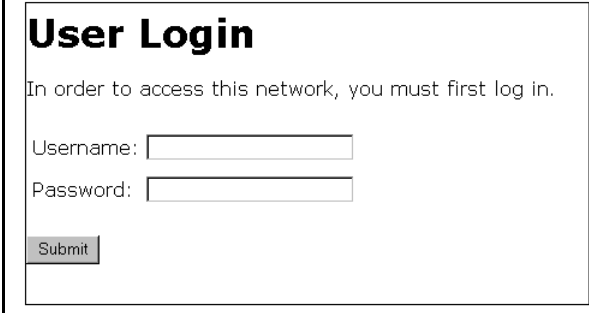
Before gaining access to the network, a client first presents authentication credentials to the switch. The switch then verifies the credentials with a RADIUS authentication server. Successfully authenticated clients receive

access to the network, as defined by the System Administrator. Clients who fail to authenticate successfully receive no network access or limited network access as defined by the System Administrator.

Web-based Authentication

When a client connects to a Web-Auth enabled port, communication is redirected to the switch. A temporary IP address is assigned by the switch and a login screen is presented for the client to enter their username and password.

The default User Login screen is shown in Figure 4-1.



User Login

In order to access this network, you must first log in.

Username:

Password:

Figure 4-1. Example of Default User Login Screen

When a client connects to the switch, it sends a DHCP request to receive an IP address to connect to the network. To avoid address conflicts in a secure network, you can specify a temporary IP address pool to be used by DHCP by configuring the **dhcp-addr** and **dhcp-lease** options when you enable web authentication with the **aaa port-access web-based** command.

The Secure Socket Layer (SSLv3/TLSv1) feature provides remote web access to the network via authenticated transactions and encrypted paths between the switch and management station clients capable of SSL/TLS. If you have enabled SSL on the switch, you can specify the **ssl-login** option when you configure web authentication so that clients who log in to specified ports are redirected to a secure login page (<https://...>) to enter their credentials.

The switch passes the supplied username and password to the RADIUS server for authentication and displays the following progress message:

Authenticating...

Please wait while your credentials are verified.

Figure 4-2. Progress Message During Authentication

If the client is authenticated and the maximum number of clients allowed on the port (**client-limit**) has not been reached, the port is assigned to a static, untagged VLAN for network access. After a successful login, a client may be redirected to a URL if you specify a URL value (**redirect-url**) when you configure web authentication.

Access Granted

You have been authenticated. Please wait while network connection refreshes itself.

Time (sec) Remaining:

Figure 4-3. Authentication Completed

The assigned VLAN is determined, in order of priority, as follows:

1. If there is a RADIUS-assigned VLAN, then, for the duration of the client session, the port belongs to this VLAN and temporarily drops all other VLAN memberships.
2. If there is no RADIUS-assigned VLAN, then, for the duration of the client session, the port belongs to the authorized VLAN (**auth-vid** if configured) and temporarily drops all other VLAN memberships.
3. If neither 1 or 2, above, apply, but the port is an untagged member of a statically configured, port-based VLAN, then the port remains in this VLAN.
4. If neither 1, 2, or 3, above, apply, then the client session does not have access to any statically configured, untagged VLANs and client access is blocked.

The assigned port VLAN remains in place until the session ends. Clients may be forced to reauthenticate after a fixed period of time (**reauth-period**) or at any time during a session (**reauthenticate**). An implicit logoff period can be set if there is no activity from the client after a given amount of time (**logoff-period**). In addition, a session ends if the link on the port is lost, requiring reauthentication of all clients. Also, if a client moves from one port to another and client

moves have not been enabled (**client-moves**) on the ports, the session ends and the client must reauthenticate for network access. At the end of the session the port returns to its pre-authentication state. Any changes to the port's VLAN memberships made while it is an authorized port take affect at the end of the session.

A client may not be authenticated due to invalid credentials or a RADIUS server timeout. The **max-retries** parameter specifies how many times a client may enter their credentials before authentication fails. The **server-timeout** parameter sets how long the switch waits to receive a response from the RADIUS server before timing out. The **max-requests** parameter specifies how many authentication attempts may result in a RADIUS server timeout before authentication fails. The switch waits a specified amount of time (**quiet-period**) before processing any new authentication requests from the client.

Network administrators may assign unauthenticated clients to a specific static, untagged VLAN (**unauth-vid**), to provide access to specific (guest) network resources. If no VLAN is assigned to unauthenticated clients the port is blocked and no network access is available. Should another client successfully authenticate through that port any unauthenticated clients on the **unauth-vid** are dropped from the port.

MAC-based Authentication

When a client connects to a MAC-Auth enabled port traffic is blocked. The switch immediately submits the client's MAC address (in the format specified by the **addr-format**) as its certification credentials to the RADIUS server for authentication.

If the client is authenticated and the maximum number of MAC addresses allowed on the port (**addr-limit**) has not been reached, the port is assigned to a static, untagged VLAN for network access.

The assigned VLAN is determined, in order of priority, as follows:

1. If there is a RADIUS-assigned VLAN, then, for the duration of the client session, the port belongs to this VLAN and temporarily drops all other VLAN memberships.
2. If there is no RADIUS-assigned VLAN, then, for the duration of the client session, the port belongs to the Authorized VLAN (**auth-vid** if configured) and temporarily drops all other VLAN memberships.
3. If neither 1 or 2, above, apply, but the port is an untagged member of a statically configured, port-based VLAN, then the port remains in this VLAN.

Web and MAC Authentication

How Web and MAC Authentication Operate

-
-
-
4. If neither 1, 2, or 3, above, apply, then the client session does not have access to any statically configured, untagged VLANs and client access is blocked.

The assigned port VLAN remains in place until the session ends. Clients may be forced to reauthenticate after a fixed period of time (**reauth-period**) or at any time during a session (**reauthenticate**). An implicit logoff period can be set if there is no activity from the client after a given amount of time (**logoff-period**). In addition, a session ends if the link on the port is lost, requiring reauthentication of all clients. Also, if a client moves from one port to another and client moves have not been enabled (**addr-moves**) on the ports, the session ends and the client must reauthenticate for network access. At the end of the session the port returns to its pre-authentication state. Any changes to the port's VLAN memberships made while it is an authenticated port take affect at the end of the session.

A client may not be authenticated due to invalid credentials or a RADIUS server timeout. The **server-timeout** parameter sets how long the switch waits to receive a response from the RADIUS server before timing out. The **max-requests** parameter specifies how many authentication attempts may result in a RADIUS server timeout before authentication fails. The switch waits a specified amount of time (**quiet-period**) before processing any new authentication requests from the client.

Network administrators may assign unauthenticated clients to a specific static, untagged VLAN (**unauth-vid**), to provide access to specific (guest) network resources. If no VLAN is assigned to unauthenticated clients the port remains in its original VLAN configuration. Should another client successfully authenticate through that port any unauthenticated clients are dropped from the port.

Terminology

Authorized-Client VLAN: Like the Unauthorized-Client VLAN, this is a conventional, static, untagged, port-based VLAN previously configured on the switch by the System Administrator. The intent in using this VLAN is to provide authenticated clients with network access and services. When the client connection terminates, the port drops its membership in this VLAN.

Authentication Server: The entity providing an authentication service to the switch. In the case of a ProCurve Switch 8212zl running Web/MAC-Authentication, this is a RADIUS server.

Authenticator: In ProCurve switch applications, a device such as a ProCurve Switch 8212zl that requires a client or device to provide the proper credentials (MAC address, or username and password) before being allowed access to the network.

CHAP: Challenge Handshake Authentication Protocol. Also known as “CHAP-RADIUS”.

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

Redirect URL: A System Administrator-specified web page presented to an authorized client following Web Authentication. ProCurve recommends specifying this URL when configuring Web Authentication on a switch. Refer to **aaa port-access web-based [e] < port-list > [redirect-url < url >]** on page 4-25.

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

Unauthorized-Client VLAN: A conventional, static, untagged, port-based VLAN previously configured on the switch by the System Administrator. It is used to provide limited network access and services to clients who are not authenticated.

Operating Rules and Notes

- The switch supports concurrent 802.1X and either Web- or MAC-authentication operation on a port (with up to 32 clients allowed). However, concurrent operation of Web- or MAC-authentication with other types of authentication on the same port is not supported. That is, the following authentication types are *mutually exclusive* on a given port:
 - Web Authentication (with or without 802.1X)
 - MAC Authentication (with or without 802.1X)
 - MAC lockdown
 - MAC lockout
 - Port-Security
- Order of Precedence for Port Access Management (highest to lowest):
 - a. MAC lockout
 - b. MAC lockdown or Port Security
 - c. Port-based Access Control (802.1X) or Web Authentication or MAC Authentication

Port Access Management

When configuring a port for Web or MAC Authentication, be sure that a higher precedent port access management feature is not enabled on the port. For example, be sure that Port Security is disabled on a port before configuring the port for Web or MAC Authentication. If Port Security is enabled on the port this misconfiguration does not allow Web or MAC Authentication to occur.

- VLANs: If your LAN does not use multiple VLANs, then you do not need to configure VLAN assignments in your RADIUS server or consider using either Authorized or Unauthorized VLANs. If your LAN does use multiple VLANs, then some of the following factors may apply to your use of Web-Auth and MAC-Auth.
 - Web-Auth and MAC-Auth operate only with port-based VLANs. Operation with protocol VLANs is not supported, and clients do not have access to protocol VLANs during Web-Auth and MAC-Auth sessions.
 - A port can belong to one, untagged VLAN during any client session. Where multiple authenticated clients may simultaneously use the same port, they must all be capable of operating on the same VLAN.

- During an authenticated client session, the following hierarchy determines a port's VLAN membership:
 1. If there is a RADIUS-assigned VLAN, then, for the duration of the client session, the port belongs to this VLAN and temporarily drops all other VLAN memberships.
 2. If there is no RADIUS-assigned VLAN, then, for the duration of the client session, the port belongs to the Authorized VLAN (if configured) and temporarily drops all other VLAN memberships.
 3. If neither 1 or 2, above, apply, but the port is an untagged member of a statically configured, port-based VLAN, then the port remains in this VLAN.
 4. If neither 1, 2, or 3, above, apply, then the client session does not have access to any statically configured, untagged VLANs and client access is blocked.
 - After an authorized client session begins on a given port, the port's VLAN membership does not change. If other clients on the same port become authenticated with a different VLAN assignment than the first client, the port blocks access to these other clients until the first client session ends.
 - The optional "authorized" VLAN (**auth-vid**) and "unauthorized" VLAN (**unauth-vid**) you can configure for Web- or MAC-based authentication must be statically configured VLANs on the switch. Also, if you configure one or both of these options, any services you want clients in either category to access must be available on those VLANs.
- Where a given port's configuration includes an unauthorized client VLAN assignment, the port will allow an unauthenticated client session only while there are no requests for an authenticated client session on that port. In this case, if there is a successful request for authentication from an authorized client, the switch terminates the unauthorized-client session and begins the authorized-client session.
 - When a port on the switch is configured for Web or MAC Authentication and is supporting a current session with another device, rebooting the switch invokes a re-authentication of the connection.
 - When a port on the switch is configured as a Web- or MAC-based authenticator, it blocks access to a client that does not provide the proper authentication credentials. If the port configuration includes an optional, unauthorized VLAN (**unauth-vid**), the port is temporarily placed in the unauthorized VLAN if there are no other authorized clients currently using the port with a different VLAN assignment. If an authorized client is using the port with a different VLAN or if there is no unauthorized VLAN configured, the unauthorized client does not receive access to the network.

- Web- or MAC-based authentication and LACP cannot both be enabled on the same port.

**Web/MAC
Authentication
and LACP**

Web or MAC authentication and LACP are not supported at the same time on a port. The switch automatically disables LACP on ports configured for Web or MAC authentication.

- Use the **show port-access web-based** commands to display session status, port-access configuration settings, and statistics for Web-Auth sessions.

Setup Procedure for Web/MAC Authentication

Before You Configure Web/MAC Authentication

1. Configure a local username and password on the switch for both the Operator (login) and Manager (enable) access levels. (While this is not required for a Web- or MAC-based configuration, ProCurve recommends that you use a local user name and password pair, at least until your other security measures are in place, to protect the switch configuration from unauthorized access.)
2. Determine the switch ports that you want to configure as authenticators. Note that before you configure Web- or MAC-based authentication on a port operating in an LACP trunk, you must remove the port from the trunk. (For more information, refer to the “Web/MAC Authentication and LACP” on page 4-12.)

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

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

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

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

```

Figure 4-4. Example of show port-access config Command Output

3. Determine whether any VLAN assignments are needed for authenticated clients.
 - a. If you configure the RADIUS server to assign a VLAN for an authenticated client, this assignment overrides any VLAN assignments configured on the switch while the authenticated client session remains active. Note that the VLAN must be statically configured on the switch.
 - b. If there is no RADIUS-assigned VLAN, the port can join an “Authorized VLAN” for the duration of the client session, if you choose to configure one. This must be a port-based, statically configured VLAN on the switch.
 - c. If there is neither a RADIUS-assigned VLAN or an “Authorized VLAN” for an authenticated client session on a port, then the port’s VLAN membership remains unchanged during authenticated client sessions. In this case, configure the port for the VLAN in which you want it to operate during client sessions.

Note that when configuring a RADIUS server to assign a VLAN, you can use either the VLAN's name or VID. For example, if a VLAN configured in the switch has a VID of 100 and is named **vlan100**, you could configure the RADIUS server to use either "100" or "vlan100" to specify the VLAN.

4. Determine whether to use the optional "Unauthorized VLAN" mode for clients that the RADIUS server does not authenticate. This VLAN must be statically configured on the switch. If you do not configure an "Unauthorized VLAN", the switch simply blocks access to unauthenticated clients trying to use the port.
5. Determine the authentication policy you want on the RADIUS server and configure the server. Refer to the documentation provided with your RADIUS application and include the following in the policy for each client or client device:
 - The CHAP-RADIUS authentication method.
 - An encryption key
 - One of the following:
 - If you are configuring Web-based authentication, include the user name and password for each authorized client.
 - If you are configuring MAC-based authentication, enter the device MAC address in both the username and password fields of the RADIUS policy configuration for that device. Also, if you want to allow a particular device to receive authentication only through a designated port and switch, include this in your policy.
6. Determine the IP address of the RADIUS server(s) you will use to support Web- or MAC-based authentication. (For information on configuring the switch to access RADIUS servers, refer to "Configuring the Switch To Access a RADIUS Server" on page 4-15.)

Configuring the RADIUS Server To Support MAC Authentication

On the RADIUS server, configure the client device authentication in the same way that you would any other client, except:

- Configure the client device's (hexadecimal) MAC address as both username and password. Be careful to configure the switch to use the same format that the RADIUS server uses. Otherwise, the server will deny access. The switch provides four format options:

aabbccddeeff (the default format)

aabbcc-ddeeff

aa-bb-cc-dd-ee-ff

aa:bb:cc:dd:ee:ff

**Note on MAC
Addresses**

You must enter the letters in a MAC address in lowercase.

- If the device is a switch or other VLAN-capable device, use the base MAC address assigned to the device, and not the MAC address assigned to the VLAN through which the device communicates with the authenticator switch. Note that the switch applies a single MAC address to all VLANs configured in the switch. Thus, for a given switch, the MAC address is the same for all VLANs configured on the switch. (Refer to the chapter titled “Static Virtual LANs (VLANs)” in the *Advanced Traffic Management Guide* for your switch.)

Configuring the Switch To Access a RADIUS Server

RADIUS Server Configuration Commands

radius-server	
[host <ip-address>]	below
[key <global-key-string >]	below
radius-server host <ip-address> key <server-specific key-string>	4-16

This section describes the minimal commands for configuring a RADIUS server to support Web-Auth and MAC Auth. For information on other RADIUS command options, refer to chapter 6, “RADIUS Authentication and Accounting” .

Syntax: [no] radius-server

[host < ip-address >]

*Adds a server to the RADIUS configuration or (with **no**) deletes a server from the configuration. You can configure up to three RADIUS server addresses. The switch uses the first server it successfully accesses. (Refer to “RADIUS Authentication and Accounting” on page 6-1.)*

[key < global-key-string >]

Specifies the global encryption key the switch uses with servers for which the switch does not have a server-specific key assignment (below). This key is optional if all RADIUS server addresses configured in the switch include a server-specific encryption key. (Default: Null.)

Syntax: radius-server host < ip-address > key <server-specific key-string>
[no] radius-server host < ip-address > key

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

*The **no** form of the command removes the key configured for a specific server.*

For example, to configure the switch to access a RADIUS server at IP address 192.168.32.11 using a server specific shared secret key of ‘1A7rd’

```
ProCurve(config)# radius-server host 192.168.32 11
ProCurve(config)# radius-server host 192.168.32.11 key 1A7rd

ProCurve(config)# show radius

Status and Counters - General RADIUS Information

Deadtime(min) : 0
Timeout(secs) : 5
Retransmit Attempts : 3
Global Encryption Key :

Server IP Addr      Auth  Acct
                  Port  Port  Encryption Key
-----
192.168.32.11      1812  1813  1A7rd
```

Figure 4-5. Example of Configuring a Switch To Access a RADIUS Server

Configuring Web Authentication

Overview

1. If you have not already done so, configure a local username and password pair on the switch.
2. Identify or create a redirect URL for use by authenticated clients. ProCurve recommends that you provide a redirect URL when using Web Authentication. If a redirect URL is not specified, web browser behavior following authentication may not be acceptable.
3. If you plan to use multiple VLANs with Web Authentication, ensure that these VLANs are configured on the switch and that the appropriate port assignments have been made. Also, confirm that the VLAN used by authorized clients can access the redirect URL.
4. Use the **ping** command in the switch console interface to ensure that the switch can communicate with the RADIUS server you have configured to support Web-Auth on the switch.
5. Configure the switch with the correct IP address and encryption key to access the RADIUS server.
6. (Optional) To use SSL encryption for web authentication login, configure and enable SSL on the switch.
7. Enable web authentication on the switch ports you want to use.
8. Configure the optional settings that you want to use for web authentication; for example:
 - To avoid address conflicts in a secure network, configure the base IP address and mask to be used by the switch for temporary DHCP addresses. You can also set the lease length for these temporary IP addresses.
 - To use SSL encryption for web authentication login, configure the SSL option.
 - To redirect authorized clients to a specified URL, configure the Redirect URL option.
9. Configure how web-authenticator ports transmit traffic before they successfully authenticate a client and enter the authenticated state:
 - You can block incoming and outgoing traffic on a port before authentication occurs.

- You can block only incoming traffic on a port before authentication occurs. Outgoing traffic with unknown destination addresses is flooded on unauthenticated ports configured for web authentication. For example, Wake-on-LAN traffic is transmitted on a web-authenticated egress port that has not yet transitioned to the authenticated state;
10. Test both authorized and unauthorized access to your system to ensure that Web Authentication works properly on the ports you have configured for port-access using Web Authentication.

Note

Client web browsers may not use a proxy server to access the network.

Configuration Commands for Web Authentication

Command	Page
Configuration Level	
aaa port-access <port-list> controlled-directions <both in>	4-20
[no] aaa port-access web-based <port-list>	4-22
[auth-vid]	4-22
[clear-statistics]	4-22
[client-limit]	4-22
[client-moves]	4-23
[dhcp-addr]	4-23
[dhcp-lease]	4-23
[ewa-server]	4-23
[logoff-period]	4-23
[max-requests]	4-23
[max-retries]	4-24
[quiet-period]	4-24
[reauth-period]	4-24
[reauthenticate]	4-24
[redirect-url]	4-25
[server-timeout]	4-25
[unauth-vid]	4-36

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

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

both (default): *Incoming and outgoing traffic is blocked on a port configured for web authentication before authentication occurs.*

in: *Incoming traffic is blocked on a port configured for web authentication before authentication occurs. Outgoing traffic with unknown destination addresses is flooded on unauthenticated ports configured for web authentication.*

Prerequisites: *As implemented in 802.1X authentication, the disabling of incoming traffic and transmission of outgoing traffic on a web-authenticated egress port in an unauthenticated state (using the **aaa port-access controlled-directions in** command) is supported only if:*

- *The 802.1s Multiple Spanning Tree Protocol (MSTP) or 802.1w Rapid Spanning Tree Protocol (RSTP) is enabled on the switch. MSTP and RSTP improve resource utilization while maintaining a loop-free network.*

*The port is configured as an edge port in the network using the **spanning-tree edge-port** command.*

Syntax: `aaa port-access <port-list> controlled-directions <both | in>`
— Continued —

Notes:

- For information on how to configure the prerequisites for using the **aaa port-access controlled-directions in** command, see Chapter 4, “Multiple Instance Spanning-Tree Operation” in the Advanced Traffic Management Guide.
- To display the currently configured *Controlled Directions* value for web-authenticated ports, enter the **show port-access web-based config** command as shown in Figure 4-4.
- The **aaa port-access controlled-direction in** command allows Wake-on-LAN traffic to be transmitted on a web-authenticated egress port that has not yet transitioned to the authenticated state; the **controlled-direction both** setting prevents Wake-on-LAN traffic to be transmitted on a web-authenticated egress port until authentication occurs.

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

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

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

For information about how to configure and use 802.1X authentication, refer to Chapter 13, “Configuring Port-Based and User-Based Access Control (802.1X)”.

- When a web-authenticated port is configured with the **controlled-directions in** setting, eavesdrop prevention is not supported on the port.

Syntax: [no] aaa port-access web-based <port-list>

*Enables web-based authentication on the specified ports. Use the **no** form of the command to disable web-based authentication on the specified ports.*

Syntax: aaa port-access web-based <port-list> [auth-vid <vid>]]

no aaa port-access web-based <port-list> [auth-vid]

*Specifies the VLAN to use for an authorized client. The RADIUS server can override the value (accept-response includes a vid). If **auth-vid** is **0**, no VLAN changes occur unless the RADIUS server supplies one.*

*Use the **no** form of the command to set the **auth-vid** to **0**. (Default: 0).*

Syntax: aaa port-access web-based [clear-statistics]

*Clears (resets to 0) all counters used to monitor the CEI, HTTP, Web-Auth control traffic generated in web authentication session. (To display Web-Auth traffic statistics, enter the **show port-access web-based statistics** command.)*

Syntax: aaa port-access web-based <port-list> [client-limit <1-32>]

Specifies the maximum number of authenticated clients to allow on the port. (Default: 1)

Note: *On switches where Web Auth and 802.1X can operate concurrently, this limit includes the total number of clients authenticated through both methods.*

Syntax: [no] aaa port-access web-based <port-list> [client-moves]

Allows client moves between the specified ports under Web Auth control. When enabled, the switch allows clients to move without requiring a re-authentication. When disabled, the switch does not allow moves and when one does occur, the user will be forced to re-authenticate. At least two ports (from port(s) and to port(s)) must be specified.

*Use the **no** form of the command to disable client moves between ports under Web Auth control.
(Default: disabled – no moves allowed)*

Syntax: aaa port-access web-based [dhcp-addr <ip-address/mask>]

*Specifies the base address/mask for the temporary IP pool used by DHCP. The base address can be any valid ip address (not a multicast address). Valid mask range value is <255.255.240.0 - 255.255.255.0>.
(Default: 192.168.0.0/255.255.255.0)*

Syntax: aaa port-access web-based [dhcp-lease <5 - 25>]

*Specifies the lease length, in seconds, of the temporary IP address issued for Web Auth login purposes.
(Default: 10 seconds)*

Syntax: aaa port-access web-based <port-list> [logoff-period] <60-9999999>]

Specifies the period, in seconds, that the switch enforces for an implicit logoff. This parameter is equivalent to the MAC age interval in a traditional switch sense. If the switch does not see activity after a logoff-period interval, the client is returned to its pre-authentication state. (Default: 300 seconds)

Syntax: aaa port-access web-based <port-list> [max-requests <1-10>]

*Specifies the number of authentication attempts that must time-out before authentication fails.
(Default: 2)*

Syntax: aaa port-access web-based <port-list> [max-retries <1-10>]

*Specifies the number of the number of times a client can enter their user name and password before authentication fails. This allows the reentry of the user name and password if necessary.
(Default: 3)*

Syntax: aaa port-access web-based <port-list> [quiet-period <1 - 65535>]

Specifies the time period (in seconds) the switch uses before sending an authentication request for a client that failed authentication. (Default: 60 seconds)

Syntax: aaa port-access web-based <port-list> [reauth-period <0 - 9999999>]

*Specifies the time period, in seconds, the switch enforces on a client to re-authenticate. When set to **0**, reauthentication is disabled. (Default: 300 seconds)*

Syntax: aaa port-access web-based <port-list> [reauthenticate]

Forces a reauthentication of all attached clients on the port.

Syntax: aaa port-access web-based <port-list> [redirect-url <url>]
no aaa port-access web-based <port-list> [redirect-url]

Specifies the URL that a user is redirected to after a successful login. Any valid, fully-formed URL may be used, for example, `http://welcome-server/welcome.htm` or `http://192.22.17.5`. ProCurve recommends that you provide a redirect URL when using Web Authentication.

Note: *The `redirect-url` command accepts only the first 103 characters of the allowed 127 characters.*

*Use the **no** form of the command to remove a specified redirect URL.*

(Default: There is no default URL. Browser behavior for authenticated clients may not be acceptable.)

Syntax: aaa port-access web-based [e] <port-list> [server-timeout <1 - 300>]

*Specifies the period, in seconds, the switch waits for a server response to an authentication request. Depending on the current **max-requests** value, the switch sends a new attempt or ends the authentication session.
(Default: 30 seconds)*

Show Commands for Web Authentication

Command	Page
show port-access web-based [<i>port-list</i>]	4-26
show port-access web-based clients [<i>port-list</i>]	4-27
show port-access web-based clients < <i>port-list</i> > detailed	4-28
show port-access web-based config [<i>port-list</i>]	4-29
show port-access web-based config < <i>port-list</i> > detailed	4-30
show port-access web-based config [<i>port-list</i>] auth-server	4-31
show port-access web-based config [<i>port-list</i>] web-server	4-31

Syntax: show port-access web-based [*port-list*]

Displays the status of all ports or specified ports that are enabled for Web authentication. The information displayed for each port includes:

- *Number of authorized and unauthorized clients*
- *VLAN ID number of the untagged VLAN used. If the switch supports MAC-based (untagged) VLANs, **MACbased** is displayed to show that multiple untagged VLANs are configured for authentication sessions.*
- *If tagged VLANs (statically configured or RADIUS-assigned) are used (**Yes** or **No**)*
- *If client-specific per-port CoS (Class of Service) values are configured (**Yes** or **No**) or the numerical value of the CoS (802.1p priority) applied to all inbound traffic. For client-specific per-port CoS values, enter the **show port-access web-based clients detailed** command.*
- *If per-port rate-limiting for inbound traffic is applied (**Yes** or **No**) or the percentage value of the port's available bandwidth applied as a rate-limit value.*
- *If RADIUS-assigned ACLs are applied*

Information on ports not enabled for Web Authentication is not displayed.

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

Port Access Web-Based Status

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

Figure 5. Example of show port-access web-based Command Output

Syntax: show port-access web-based clients [*port-list*]

Displays the session status, name, and address for each web-authenticated client on the switch. The IP address displayed is taken from the DHCP binding table (learned through the DHCP Snooping feature).

If DHCP snooping is not enabled on the switch, n/a (not available) is displayed for a client's IP address.

If a web-authenticated client uses an IPv6 address, n/a - IPv6 is displayed.

If DHCP snooping is enabled but no MAC-to-IP address binding for a client is found in the DHCP binding table, n/a - no info is displayed.

```
ProCurve (config)# show port-access web-based clients

Port Access Web-Based Client Status

Port    Client Name    MAC Address    IP Address    Session Status
-----
1       webuser1      0010b5-891a9e  192.192.192.192  Authenticated
1       webuser2      001560-b3ea48  n/a - no info   Authenticating
1       webuser3      000000-111111  n/a - IPv6      Authenticating
3       webuser4      000000-111112  n/a             Authenticating
```

Figure 6. Example of show port-access web-based clients Command Output

Syntax: show port-access web-based clients <port-list> detailed

Displays detailed information on the status of web-authenticated client sessions on specified switch ports.

```
ProCurve (config)# show port-access web-based clients 1 detailed

Port Access Web-Based Client Status Detailed

Client Base Details :
Port           : 1
Session Status : authenticated      Session Time(sec) : 6
Username       : webuser1          MAC Address       : 0010b5-891a9e
IP             : n/a

Access Policy Details :
COS Map        : 12345678           In Limit %       : 98
Untagged VLAN : 4006               Out Limit %      : 100
Tagged VLANs  : 1, 3, 5, 6, 334, 2566

RADIUS-ACL List :
deny in udp from any to 10.2.8.233 CNT
Hit Count: 0
permit in udp from any to 10.2.8.233 CNT
Hit Count: 0
deny in tcp from any to 10.2.8.233 CNT
Hit Count: 0
permit in tcp from any to 10.2.8.233 CNT
Hit Count: 0
permit in tcp from any to 0.0.0.0/0 CNT
Hit Count: 0
```

Figure 7. Example of show port-access web-based clients detailed Command Output

Syntax: show port-access web-based config [*port-list*]

Displays the currently configured Web Authentication settings for all switch ports or specified ports, including:

- *Temporary DHCP base address and mask*
- *Support for RADIUS-assigned dynamic VLANs (**Yes** or **No**)*
- *Controlled directions setting for transmitting Wake-on-LAN traffic on egress ports*
- *Authorized and unauthorized VLAN IDs*

*If the authorized or unauthorized VLAN ID value is **0**, the default VLAN ID is used unless overridden by a RADIUS-assigned value.*

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

Port Access Web-Based Configuration

DHCP Base Address : 192.168.0.0
DHCP Subnet Mask  : 255.255.255.0
DHCP Lease Length : 10
Allow RADIUS-assigned dynamic (GVRP) VLANs [No] : No

Port  Enabled  Client  Client  Logoff  Re-Auth  Unauth  Auth  Cntrl
-----  -
1     Yes       1      No      300    0        0       0     both
2     Yes       1      No      300    0        0       0     in
...
```

Figure 8. Example of show port-access web-based config Command Output

Syntax: show port-access web-based config <port-list> detailed

Displays more detailed information on the currently configured Web Authentication settings for specified ports.

```
ProCurve (config)# show port-access web-based config 1 detailed

Port Access Web-Based Detailed Configuration

Port          : 1          Web-based enabled : Yes
Client Limit  : 1          Client Moves       : No
Logoff Period : 300         Re-Auth Period    : 0

Unauth VLAN ID : 0          Auth VLAN ID      : 0

Max Requests  : 3          Quiet Period      : 60
Server Timeout : 30

Max Retries   : 3          SSL Enabled       : No
Redirect URL  :
...
```

Figure 9. Example of show port-access web-based config detail Command Output

Syntax: show port-access web-based config [*port-list*] auth-server

Displays the currently configured Web Authentication settings for all switch ports or specified ports and includes RADIUS server-specific settings, such as:

- *Timeout waiting period*
- *Number of timeouts supported before authentication login fails*
- *Length of time (quiet period) supported between authentication login attempts*

```
ProCurve (config)# show port-access web-based config auth-server
```

Port Access Web-Based Configuration

Port	Enabled	Client Limit	Client Moves	Logoff Period	Re-Auth Period	Max Req	Quiet Period	Server Timeout
1	Yes	1	No	300	0	3	60	30
2	No	1	No	300	0	3	60	30
...								

Figure 10. Example of show port-access web-based config auth-server Command Output

Syntax: show port-access web-based config [*port-list*] web-server

Displays the currently configured Web Authentication settings for all ports or specified ports, including web-specific settings for password retries, SSL login status, and a redirect URL, if specified.

Configuring MAC Authentication on the Switch

Overview

1. If you have not already done so, configure a local username and password pair on the switch.
2. If you plan to use multiple VLANs with MAC Authentication, ensure that these VLANs are configured on the switch and that the appropriate port assignments have been made.
3. Use the **ping** command in the switch console interface to ensure that the switch can communicate with the RADIUS server you have configured to support MAC-Auth on the switch.
4. Configure the switch with the correct IP address and encryption key to access the RADIUS server.
5. Configure the switch for MAC-Auth:
 - a. Configure MAC Authentication on the switch ports you want to use.
6. Test both the authorized and unauthorized access to your system to ensure that MAC Authentication works properly on the ports you have configured for port-access.

Configuration Commands for MAC Authentication

Command	Page
Configuration Level	
aaa port-access mac-based addr-format	4-33
[no] aaa port-access mac-based [e] < port-list >	4-34
[addr-limit]	4-34
[addr-moves]	4-34
[auth-vid]	4-34
[logoff-period]	4-35
[max-requests]	4-35
[quiet-period]	4-35
[reauth-period]	4-35
[reauthenticate]	4-35
[server-timeout]	4-35
[unauth-vid]	4-36

Syntax: aaa port-access mac-based addr-format <no-delimiter | single-dash | multi-dash | multi-colon | no-delimiter-uppercase | single-dash-uppercase | multi-dash-uppercase | multi-colon-uppercase>

Specifies the MAC address format to be used in the RADIUS request message. This format must match the format used to store the MAC addresses in the RADIUS server. (Default: no-delimiter)

no-delimiter — *specifies an aabbccddeeff format.*

single-dash — *specifies an aabbcc-ddeeff format.*

multi-dash — *specifies an aa-bb-cc-dd-ee-ff format.*

multi-colon — *specifies an aa:bb:cc:dd:ee:ff format.*

no-delimiter-uppercase — *specifies an AABCCDDEEFF format.*

single-dash-uppercase — *specifies an AABCC-DDEEFF format*

multi-dash-uppercase — *specifies an AA-BB-CC-DD-EE-FF format*

multi-colon-uppercase — *specifies an AA:BB:CC:DD:EE:FF format.*

Syntax: [no] aaa port-access mac-based < port-list >

*Enables MAC-based authentication on the specified ports. Use the **no** form of the command to disable MAC-based authentication on the specified ports.*

Syntax: aaa port-access mac-based [e] < port-list > [addr-limit <1-32>]

Specifies the maximum number of authenticated MACs to allow on the port. (Default: 1)

Note: *On switches where MAC Auth and 802.1X can operate concurrently, this limit includes the total number of clients authenticated through both methods.*

Syntax: [no] aaa port-access mac-based [e] < port-list > [addr-moves]

*Allows client moves between the specified ports under MAC Auth control. When enabled, the switch allows addresses to move without requiring a re-authentication. When disabled, the switch does not allow moves and when one does occur, the user will be forced to re-authenticate. At least two ports (from port(s) and to port(s)) must be specified. Use the **no** form of the command to disable MAC address moves between ports under MAC Auth control. (Default: disabled – no moves allowed)*

Syntax: aaa port-access mac-based [e] < port-list > [auth-vid <vid>]

no aaa port-access mac-based [e] < port-list > [auth-vid]

*Specifies the VLAN to use for an authorized client. The Radius server can override the value (accept-response includes a vid). If **auth-vid** is 0, no VLAN changes occur unless the RADIUS server supplies one. Use the **no** form of the command to set the **auth-vid** to 0. (Default: 0).*

Syntax: aaa port-access mac-based [e] < port-list >
[logoff-period] <60-9999999>

Specifies the period, in seconds, that the switch enforces for an implicit logoff. This parameter is equivalent to the MAC age interval in a traditional switch sense. If the switch does not see activity after a logoff-period interval, the client is returned to its pre-authentication state. (Default: 300 seconds)

Syntax: aaa port-access mac-based [e] < port-list > [max-requests <1-10>]

Specifies the number of authentication attempts that must time-out before authentication fails. (Default: 2)

Syntax: aaa port-access mac-based [e] < port-list > [quiet-period <1 - 65535>]

Specifies the time period (in seconds) that the switch waits before processing an authentication request from a MAC address that failed authentication. (Default: 60 seconds)

Syntax: aaa port-access mac-based [e] < port-list > [reauth-period <0 - 9999999>]

Specifies the time period (in seconds) that the switch enforces on a client to re-authenticate. The client remains authenticated while the reauthentication occurs.

When set to 0, reauthentication is disabled. (Default: 300 seconds)

Syntax: aaa port-access mac-based [e] < port-list > [reauthenticate]

Forces a reauthentication of all attached clients on the port.

Syntax: aaa port-access mac-based [e] < port-list > [server-timeout <1 - 300>]

*Specifies the period, in seconds, the switch waits for a server response to an authentication request. Depending on the current **max-requests** value, the switch sends a new attempt or ends the authentication session. (Default: 30seconds)*

Syntax: aaa port-access mac-based [e] <port-list> [unauth-vid <vid>]
 no aaa port-access mac-based [e] <port-list> [unauth-vid]

*Specifies the VLAN to use for a client that fails authentication. If **unauth-vid** is **0**, no VLAN changes occur. Use the **no** form of the command to set the **unauth-vid** to **0**. (Default: 0)*

Show Commands for MAC-Based Authentication

Command	Page
show port-access mac-based [port-list]	4-37
show port-access mac-based clients [port-list]	4-37
show port-access mac-based clients <port-list> detailed	4-38
show port-access mac-based config [port-list]	4-39
show port-access mac-based config <port-list> detailed	4-40
show port-access mac-based config [port-list] auth-server	4-41

Syntax: show port-access mac-based [port-list]

Displays the status of all ports or specified ports that are enabled for MAC authentication. The information displayed for each port includes:

- *Number of authorized and unauthorized clients*
- *VLAN ID number of the untagged VLAN used. If the switch supports MAC-based (untagged) VLANs, **MACbased** is displayed to show that multiple untagged VLANs are configured for authentication sessions.*
- *If tagged VLANs (statically configured or RADIUS-assigned) are used (**Yes** or **No**)*
- *If client-specific per-port CoS (Class of Service) values are configured (**Yes** or **No**) or the numerical value of the CoS (802.1p priority) applied to all inbound traffic. For client-specific per-port CoS values, enter the **show port-access web-based clients detailed** command.*
- *If per-port rate-limiting for inbound traffic is applied (**Yes** or **No**) or the percentage value of the port's available bandwidth applied as a rate-limit value.*
- *If RADIUS-assigned ACLs are applied*

Information on ports not enabled for MAC authentication is not displayed.

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

Port Access MAC-Based Status

Auth    Unauth  Untagged  Tagged   Port    % In   RADIUS
Port  Clients Clients VLAN     VLANs   COS     Limit  ACL
-----
1     1       1       2003    Yes     70000000 100    Yes
2     2       0       MACbased No      Yes     Yes    Yes
3     4       0       1       Yes     No       No     No
```

Figure 4-6. Example of show port-access mac-based Command Output

Syntax: show port-access mac-based clients [*port-list*]

Displays the session status, name, and address for each MAC-authenticated client on the switch. The IP address displayed is taken from the DHCP binding table (learned through the DHCP Snooping feature).

If DHCP snooping is not enabled on the switch, n/a (not available) is displayed for a client's IP address.

If a MAC-authenticated client uses an IPv6 address, n/a - IPv6 is displayed.

If DHCP snooping is enabled but no MAC-to-IP address binding for a client is found in the DHCP binding table, n/a - no info is displayed.

```
ProCurve (config)# show port-access mac-based clients

Port Access MAC-Based Client Status

Port  MAC Address  IP Address                               Session Status
-----
1     001321-eb8063 2001:fe cd:ba23:cd1f:dcb1:1010:9234:4088 unauthenticated
1     000000-111111 192.192.192.192                          authenticated
2     000000-111111 n/a                                        authenticating
```

Figure 5. Example of show port-access mac-based clients Command Output

Syntax: show port-access mac-based clients <port-list> detailed
Displays detailed information on the status of MAC-authenticated client sessions on specified ports.

```
ProCurve (config)# show port-access mac-based clients 1 detailed

Port Access MAC-Based Client Status Detailed

Client Base Details :
  Port          : 1
  Session Status : authenticated      Session Time(sec) : 6
  Username      : client1            MAC Address       : 0010b5-891a9e
  IP            : n/a

Access Policy Details :
  COS Map       : 12345678           In Limit %       : 98
  Untagged VLAN : 4006               Out Limit %      : 100
  Tagged VLANs  : 1, 3, 5, 6, 334, 4001

RADIUS-ACL List :
  deny in udp from any to 10.2.8.233 CNT
    Hit Count: 0
  permit in udp from any to 10.2.8.233 CNT
    Hit Count: 0
  deny in tcp from any to 10.2.8.233 CNT
    Hit Count: 0
  permit in tcp from any to 10.2.8.233 CNT
    Hit Count: 0
  permit in tcp from any to 0.0.0.0/0 CNT
    Hit Count: 0
```

Figure 6. Example of show port-access mac-based clients detail Command Output

Syntax: show port-access mac-based config [*port-list*]

Displays the currently configured MAC Authentication settings for all switch ports or specified ports, including:

- *MAC address format*
- *Support for RADIUS-assigned dynamic VLANs (Yes or No)*
- *Controlled directions setting for transmitting Wake-on-LAN traffic on egress ports*
- *Authorized and unauthorized VLAN IDs*

If the authorized or unauthorized VLAN ID value is 0, the default VLAN ID is used unless overridden by a RADIUS-assigned value.

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

Port Access MAC-Based Configuration

MAC Address Format : no-delimiter
Allow RADIUS-assigned dynamic (GVRP) VLANs [No] : No

      Client Client Logoff  Re-Auth  Unauth   Auth      Cntrl
Port  Enabled  Limit  Moves  Period  Period  VLAN ID  VLAN ID  Dir
-----
1     No      1      No     300    0       0        0        both
2     Yes     1      No     300    0       0        0        in
...
```

Figure 7. Example of show port-access mac-based config Command Output

Syntax: show port-access mac-based config <port-list> detailed

Displays more detailed information on the currently configured MAC Authentication settings for specified ports.

```
ProCurve (config)# show port-access mac-based config 1 detailed

Port Access MAC-Based Detailed Configuration

Port          : 1          Web-based enabled : Yes
Client Limit  : 1          Client Moves      : No
Logoff Period : 300         Re-Auth Period   : 0

Unauth VLAN ID : 0          Auth VLAN ID     : 0

Max Requests  : 3          Quiet Period     : 60
Server Timeout : 30
```

Figure 8. Example of show port-access mac-based config detail Command Output

Syntax: show port-access mac-based config [*port-list*] auth-server

Displays the currently configured Web Authentication settings for all switch ports or specified ports and includes RADIUS server-specific settings, such as:

- *Timeout waiting period*
- *Number of timeouts supported before authentication login fails*
- *Length of time (quiet period) supported between authentication login attempts*

```
ProCurve (config)# show port-access mac-based config auth-server
```

Port Access MAC-Based Configuration

Port	Enabled	Client Limit	Client Moves	Logoff Period	Re-Auth Period	Max Req	Quiet Period	Server Timeout
1	No	1	No	300	0	3	60	30
2	No	1	No	300	0	3	60	30
3	Yes	1	No	300	0	3	60	30
...								

Figure 9. Example of show port-access mac-based config auth-server Command Output

Client Status

The table below shows the possible client status information that may be reported by a Web-based or MAC-based **'show... clients'** command.

Reported Status	Available Network Connection	Possible Explanations
authenticated	Authorized VLAN	Client authenticated. Remains connected until logoff-period or reauth-period expires.
authenticating	Switch only	Pending RADIUS request.
rejected-no vlan	No network access	<ol style="list-style-type: none">1. Invalid credentials supplied.2. RADIUS Server difficulties. See log file.3. If unauth-vid is specified it cannot be successfully applied to the port. An authorized client on the port has precedence.
rejected-unauth vlan	Unauthorized VLAN only	<ol style="list-style-type: none">1. Invalid credentials supplied.2. RADIUS Server difficulties. See log file.
timed out-no vlan	No network access	RADIUS request timed out. If unauth-vid is specified it cannot be successfully applied to the port. An authorized client on the port has precedence. Credentials resubmitted after quiet-period expires.
timed out-unauth vlan	Unauthorized VLAN only	RADIUS request timed out. After the quiet-period expires credentials are resubmitted when client generates traffic.
unauthenticated	Switch only	Waiting for user credentials.
