Configuring RADIUS Server Support for Switch Services

Contents

Overview

This chapter provides information that applies to setting up a RADIUS server to configure the following switch features on ports supporting RADIUS-authenticated clients:

- CoS
- Rate-Limiting
- ACLS

Optional Network Management Applications. Per-port CoS and rate-limiting assignments through a RADIUS server are also supported in the ProCurve Manager (PCM) application. Per-port ACLs through a RADIUS server can also be augmented using the Identity-Driven Management (IDM) application available for use with PCM. However, the features described in this chapter can be used without PCM or IDM support, if desired.

For information on configuring client authentication on the switch, refer to the chapter 6, “RADIUS Authentication and Accounting”.

Optional PCM and IDM Applications. ProCurve Manager is a Windows-based network management solution for all manageable ProCurve devices. It provides network: mapping and polling capabilities, device auto-discovery and topology, tools for device configuration and management, monitoring network traffic, and alerts and troubleshooting information for ProCurve networks.

ProCurve Identity Driven Manager (IDM) is an add-on module to the ProCurve Manager plus (PCM+) application. IDM extends the functionality of PCM+ to include authorization control features for edge devices in networks using RADIUS servers and Web-Authentication, MAC-Authentication, or 802.1X security protocols.

For more information, including electronic copies of the PCM and IDM manuals, visit the ProCurve Web site at **www.procurve.com**. (The PCM and IDM documentation is available under **Network Management** on the **Product manuals page** of the **Technical Support** area.)

Configuring the RADIUS Server for Per-Port CoS and Rate-Limiting Services

This section provides general guidelines for configuring a RADIUS server to dynamically apply CoS (Class of Service) and Rate-Limiting for inbound traffic on ports supporting authenticated clients. To configure support for these services on a specific RADIUS server application, refer to the documentation provided with the application. (If multiple clients are authenticated on a port where inbound CoS and Rate-Limiting values have been imposed by a RADIUS server, the CoS and Rate-Limiting applied to all clients on the port are those that are assigned by RADIUS for the most recently authenticated client. Refer to the Note on page 7-7.)

Service	Control Method and Operating Notes:
802.1p (CoS) Priority Assignments on Inbound Traffic This feature assigns a RADIUS-specified 802.1p priority to all inbound packets received on a port supporting an authenticated client.	Vendor-Specific Attribute configured in the RADIUS server. ProCurve (HP) vendor-specific ID:11 VSA: 40 (string = HP) Setting: HP-COS = *xxxxxxxx* where: *x* = desired 802.1p priority **Note:** This is typically an eight-octet field. Enter the same *x*-value in all eight octets Requires a port-access (802.1X Web Auth, or MAC Auth) authentication method configured on the client's port on the ProCurve switch. For more on 802.1p priority levels, refer to the section titled "Overview" in the "Quality of Service (QoS)" chapter of the *Advanced Traffic Management Guide* for your switch.

Service	Control Method and Operating Notes:
Rate-Limiting on inbound traffic This feature assigns a bandwidth limit to all inbound packets received on a port supporting an authenticated client.	Vendor-Specific Attribute configured in the RADIUS server. ProCurve (HP) vendor-specific ID:11 VSA: 46 (integer = HP) Setting: HP-RATE-LIMIT = *< bandwidth-in-Kbps >* **Note:** The CLI command for configuring a rate-limit on a port uses a percentage value. However, using a VSA on a RADIUS server to specify a rate-limit requires the actual Kbps to which you want to limit inbound traffic volume. Thus, to limit in-bound traffic on a gigabit port to 50% of the port's bandwidth capacity requires a VSA setting of 500000 (1,000,000 x 0.5). Requires a port-access (802.1X, Web Auth, or MAC Auth) authentication method configured on the client's port on the ProCurve switch. For more on Rate-Limiting, refer to "Rate-Limiting" in the "Port Traffic Controls" chapter of the *Management and Configuration Guide* for your switch.

Viewing the Currently Active Per-Port CoS and Rate-Limiting Configuration Specified by a RADIUS Server

While a port-access authenticated client session is active, any RADIUS-imposed port settings override their counterparts in the port's configuration. For example, if the switch configuration allows port B1 a rate-limit of 80% of the port's available bandwidth, but the RADIUS server specifies a rate-limit of 50% for a given authenticated client, then the switch shows the RADIUS-imposed rate-limit for that port as long as the authenticated client session is active.

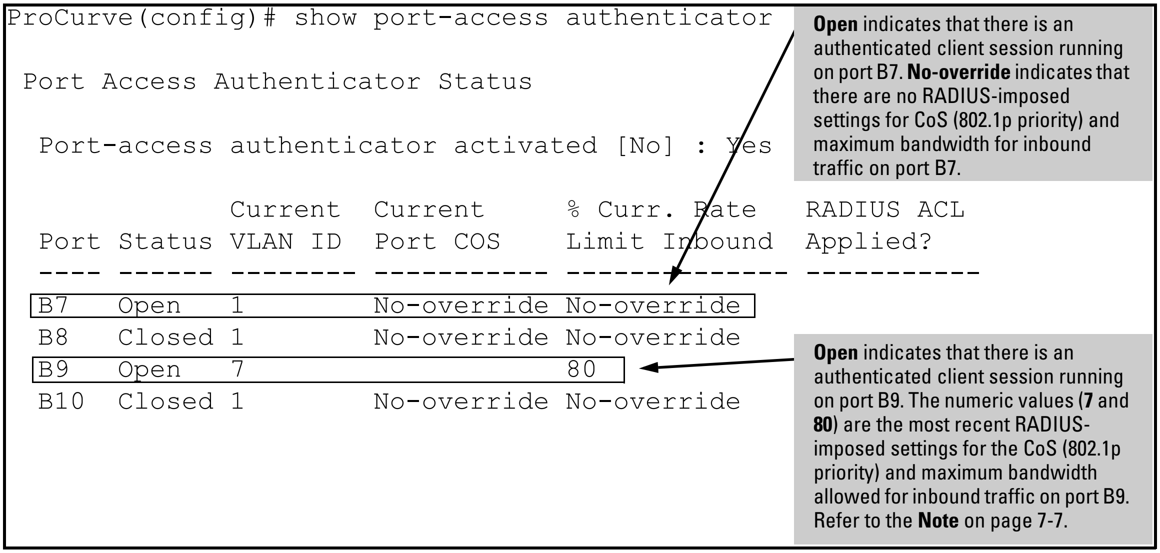
Syntax: show port-access authenticator [port-list]
show rate-limit all
show qos port-priority

These commands display the CoS and Rate-Limiting settings specified by the RADIUS server used to grant authentication for a given client on a given port. When the authenticated client session closes, the switch resets these fields to the values to which they are configured in the switch's running-config file.

show port-access authenticator [*port-list*] *displays, for 802.1X authentication, the status of RADIUS-imposed overrides of the switch's per-port CoS and Rate-Limiting configuration.*

show rate-limit all *displays, for all port-access authentication methods (802.1X, Web-Auth, and MAC-Auth), the status of RADIUS-imposed overrides of the switch's per-port Rate-Limiting configuration.*

show qos port-priority *displays, for all port-access authentication methods (802.1X, Web-Auth, and MAC-Auth), the status of RADIUS-imposed overrides of the switch's per-port CoS (802.1p) priority for inbound packets.*

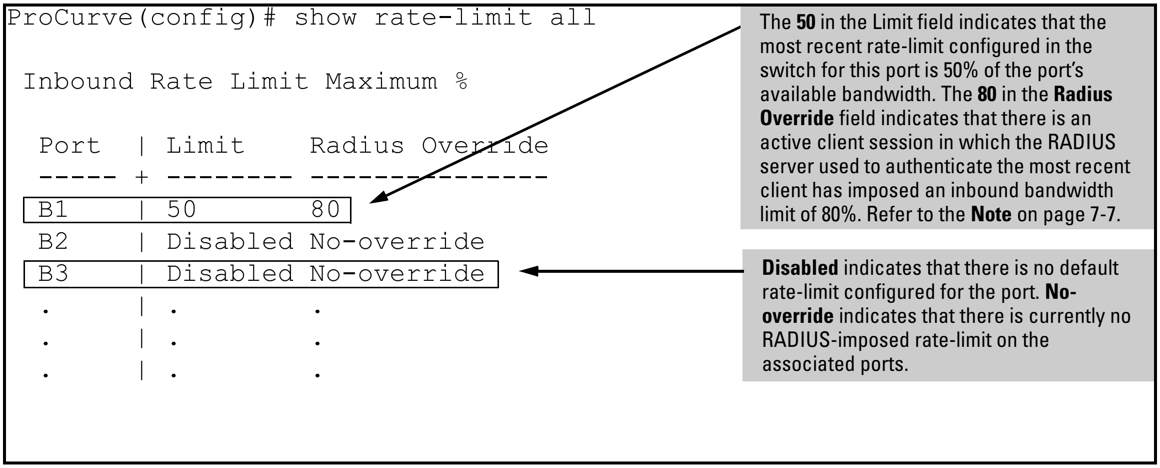


```
ProCurve(config)# show port-access authenticator

 Port Access Authenticator Status

  Port-access authenticator activated [No] : Yes

             Current  Current     % Curr. Rate   RADIUS ACL
  Port Status VLAN ID  Port COS    Limit Inbound  Applied?
  ---- ------ -------- ----------- -------------- -----------
  B7   Open   1        No-override No-override
  B8   Closed 1        No-override No-override
  B9   Open   7                    80
  B10  Closed 1        No-override No-override
```

Open indicates that there is an authenticated client session running on port B7. **No-override** indicates that there are no RADIUS-imposed settings for CoS (802.1p priority) and maximum bandwidth for inbound traffic on port B7.

Open indicates that there is an authenticated client session running on port B9. The numeric values (**7** and **80**) are the most recent RADIUS-imposed settings for the CoS (802.1p priority) and maximum bandwidth allowed for inbound traffic on port B9. Refer to the **Note** on page 7-7.

Figure 7-1. Example of Displaying Inbound CoS and Rate-Limiting Imposed by a RADIUS Session

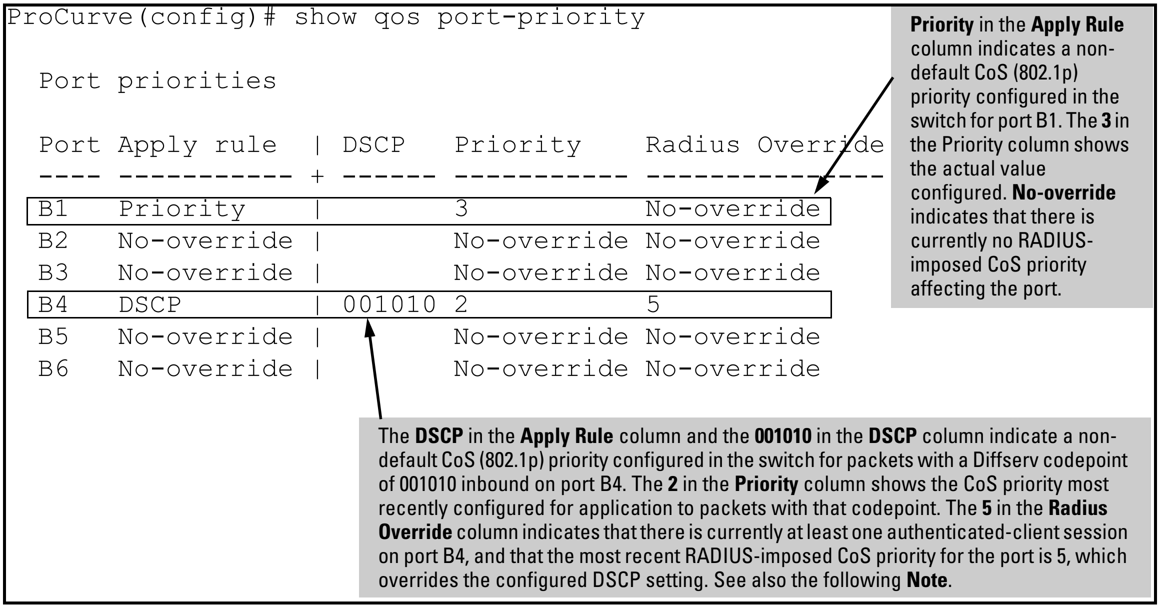


```
ProCurve(config)# show rate-limit all

 Inbound Rate Limit Maximum %

  Port   | Limit    Radius Override
  ----- + -------- ---------------
  B1     | 50       80
  B2     | Disabled No-override
  B3     | Disabled No-override
   .     | .        .
   .     | .        .
   .     | .        .
```

The **50** in the Limit field indicates that the most recent rate-limit configured in the switch for this port is 50% of the port's available bandwidth. The **80** in the **Radius Override** field indicates that there is an active client session in which the RADIUS server used to authenticate the most recent client has imposed an inbound bandwidth limit of 80%. Refer to the **Note** on page 7-7.

Disabled indicates that there is no default rate-limit configured for the port. **No-override** indicates that there is currently no RADIUS-imposed rate-limit on the associated ports.

Figure 7-2. Example of Displaying Inbound Rate-Limiting Imposed by a RADIUS Session



```
ProCurve(config)# show qos port-priority

  Port priorities

  Port Apply rule  | DSCP   Priority    Radius Override
  ---- ----------- + ------ ----------- ---------------
  B1   Priority    |        3           No-override
  B2   No-override |        No-override No-override
  B3   No-override |        No-override No-override
  B4   DSCP        | 001010 2           5
  B5   No-override |        No-override No-override
  B6   No-override |        No-override No-override
```

Priority in the **Apply Rule** column indicates a non-default CoS (802.1p) priority configured in the switch for port B1. The **3** in the Priority column shows the actual value configured. **No-override** indicates that there is currently no RADIUS-imposed CoS priority affecting the port.

The **DSCP** in the **Apply Rule** column and the **001010** in the **DSCP** column indicate a non-default CoS (802.1p) priority configured in the switch for packets with a Diffserv codepoint of 001010 inbound on port B4. The **2** in the **Priority** column shows the CoS priority most recently configured for application to packets with that codepoint. The **5** in the **Radius Override** column indicates that there is currently at least one authenticated-client session on port B4, and that the most recent RADIUS-imposed CoS priority for the port is 5, which overrides the configured DSCP setting. See also the following **Note**.

Figure 7-3. Example of Displaying Inbound CoS (802.1p) Priority Imposed by a RADIUS Session

Note

Where multiple clients are currently authenticated on a given port where inbound CoS and Rate-Limiting values have been imposed by a RADIUS server, the port operates with the inbound CoS priority and rate-limit assigned by RADIUS for the most recently authenticated client. Any earlier CoS or rate-limit values on the same port for authenticated client sessions that are still active are overwritten by the most recent RADIUS-imposed values. For example, if client "X" is authenticated with a CoS of 5 and a rate-limit of 75%, and client "Y" later becomes authenticated with a CoS of 3 and a rate-limit of 50% while the session for client "X" is still active, then the port will operate with a CoS of 3 and a rate-limit of 50% for both clients.

Configuring and Using RADIUS-Assigned Access Control Lists

Introduction

A RADIUS-assigned ACL is a *dynamic port ACL* configured on a RADIUS server and assigned by the server to filter traffic entering the switch through a specific port from an authenticated client. Note that client authentication can be enhanced by using ProCurve Manager with the optional IDM application. (Refer to "Optional PCM and IDM Applications" on page 7-2.)

The information in this section describes how to apply RADIUS-assigned, dynamic port ACLs on the switch, and assumes a general understanding of ACL structure and operation. If you need information on ACL filtering criteria, design, and operation, please refer to Chapter 10, "Access Control Lists (ACLs)".

Terminology

ACE: See Access Control Entry, below.

Access Control Entry (ACE): An ACE is a policy consisting of a packet-handling action and criteria to define the packets on which to apply the action. For dynamic port ACLs, the elements composing the ACE include:

- **permit** or **drop** (action)
- **in <** ***ip-packet-type*** **> from any** (source)
- **to < ip-address [/ mask] | any >** (destination)
- **[** ***port-#*** **]** (optional TCP or UDP application port numbers used when the packet type is TCP or UDP)

ACL: See Access Control List, below.

Access Control List (ACL): A list (or set) consisting of one or more explicitly configured Access Control Entries (ACEs) and terminating with an implicit "deny" default which drops any IP packets that do not have a match with any explicit ACE in the named ACL. An ACL can be "standard" or "extended". See "Standard ACL" and "Extended ACL". Both can be applied in any of the following ways:

- RACL: an ACL assigned to filter routed traffic entering or leaving the switch on a VLAN. (Separate assignments are required for inbound and outbound traffic.)
- VACL: an ACL assigned to filter inbound traffic on a specific VLAN configured on the switch
- Static Port ACL: an ACL assigned to filter inbound traffic on a specific switch port
- Dynamic Port ACL: dynamic ACL assigned to a port by a RADIUS server to filter inbound traffic from an authenticated client on that port

An ACL can be configured on an interface as an RACL, VACL, or static port ACL. (Dynamic port ACLs are configured on a RADIUS server.)

ACL Mask: Follows a destination IP address listed in an ACE. Defines which bits in a packet's corresponding IP addressing must exactly match the IP addressing in the ACE, and which bits need not match (wildcards).

DA: The acronym for *Destination IP Address*. In an IP packet, this is the destination IP address carried in the header, and identifies the destination intended by the packet's originator.

Deny: An ACE configured with this action causes the switch to drop a packet for which there is a match within an applicable ACL.

Deny Any Any: An abbreviated form of **deny in ip from any to any**, which denies any inbound IP traffic from any source to any destination.

Dynamic Port ACL: An ACL application type in which the ACL is assigned by a RADIUS server to a port to filter all inbound IP traffic from a client authenticated by the server for that port, regardless of whether the traffic is switched or routed. Filtering can be specified to include all IP traffic or specific IP applications or protocol types. Destination criteria can include a single destination IP address, a group of contiguous IP addresses, an IP subnet, or any IP destination. (Other, statically configured ACL application types are described in the chapter titled "Access Control Lists (ACLs)" in the *Advanced Traffic Management Guide* for your switch.

Implicit Deny: If the switch finds no matches between an inbound packet and the configured criteria in an applicable ACL, then the switch denies (drops) the packet with an implicit "deny IP any/any" operation. You can preempt the implicit "deny IP any/any" in a given ACL by configuring **permit in ip from any to any** as the last explicit ACE in the ACL. Doing so permits any inbound IP packet that is not explicitly permitted or denied by other ACEs configured sequentially earlier in the ACL. Unless otherwise noted, “implicit deny IP any” refers to the “deny” action enforced by both standard and extended ACLs.

Inbound Traffic: For the purpose of defining where the switch applies ACLs to filter traffic, inbound traffic is any IP packet that *enters the switch* from a given client on a given port.

NAS (Network Attached Server): In this context, refers to a ProCurve switch configured for RADIUS operation.

Outbound Traffic: For defining the points where the switch applies an ACL to filter traffic, outbound traffic is routed traffic *leaving the switch* through a VLAN interface (or a subnet in a multinetted VLAN). “Outbound traffic” can also apply to switched traffic leaving the switch on a VLAN interface, but VACLs do not filter outbound switched traffic.

Permit: An ACE configured with this action allows the switch to forward an inbound packet for which there is a match within an applicable ACL.

Permit Any Any: An abbreviated form of **permit in ip from any to any**, which permits any inbound IP traffic from any source to any destination.

RADIUS-Based ACL: See “Dynamic Port ACL”.

Routed ACL (RACL): An ACL applied to routed traffic that is entering or leaving the switch on a given VLAN. See also “Access Control List”.

Static Port ACL: An ACL statically configured on a specific port, group of ports, or trunk. A static port ACL filters all incoming traffic on the port, regardless of whether it is switched or routed.

VLAN ACL (VACL): An ACL applied to traffic entering the switch on a given VLAN interface. See also “Access Control List”.

VSA (Vendor-Specific-Attribute): A value used in a RADIUS-based configuration to uniquely identify a networking feature that can be applied to a port on a given vendor’s switch during an authenticated client session.

Wildcard: The part of a mask that indicates the bits in a packet’s IP addressing that do not need to match the corresponding bits specified in an ACL. See also **ACL Mask** on page 7-9.

Overview of RADIUS-Assigned, Dynamic Port ACLs

Dynamic port ACLs enhance network and switch management access security and traffic control by permitting or denying authenticated client access to specific network resources and to the switch management interface. This includes preventing clients from using TCP or UDP applications (such as Telnet, SSH, Web browser, and SNMP) if you do not want their access privileges to include these capabilities.

This feature is designed for use on the network edge to accept RADIUS-assigned, per-port ACLs (dynamic port ACLs) for Layer-3 filtering of IP traffic entering the switch from authenticated clients. A given dynamic port ACL is identified by a unique username/password pair or client MAC address, and applies only to IP traffic entering the switch from clients that authenticate with the unique credentials. The switch allows multiple dynamic port ACLs on a given port, up to the maximum number of authenticated clients allowed on the port. Also, dynamic port ACLs can be assigned regardless of whether other ACLs affecting the same port are statically configured on the switch. (For information on statically configured ACLs and application methods, refer to Chapter 10, “Access Control Lists (ACLs)”.)

A dynamic port ACL filters IP traffic entering the switch from the client whose authentication initiated the ACL assignment. Filtering criteria is based on destination and/or IP traffic type (such as TCP and UDP traffic) and traffic counter options. Implementing the feature requires:

- RADIUS authentication using the 802.1X, Web authentication, or MAC authentication services available on the switch to provide client authentication services
- configuring the ACLs on the RADIUS server (instead of the switch), and assigning each ACL to the username/password pair or MAC address of the clients you want the ACLs to support

Using RADIUS to dynamically apply per-port ACLs to edge ports enables the switch to filter IP traffic coming from outside the network, thus removing unwanted IP traffic as soon as possible and helping to improve system performance. Also, applying dynamic port ACLs to ports on the network edge is likely to be less complex than configuring static port and VLAN-based ACLs in the network core to filter unwanted IP traffic that could have been filtered at the edge.

Note

A dynamic port ACL can be applied to a port regardless of whether IP traffic on the port is already being filtered by a static port ACL and/or any VLAN-based ACLs configured on the switch. For more information, refer to “Multiple ACLs on an Interface” on page 10-20.

A dynamic port ACL assignment filters all inbound IP traffic from an authenticated client on a port, regardless of whether the client’s IP traffic is to be switched or routed.

Dynamic port ACLs can be used either with or without PCM and IDM support. (Refer to “Optional PCM and IDM Applications” on page 7-2.)

ACLs enhance network security by blocking selected IP traffic, and can serve as one aspect of network security. *However, because ACLs do not protect from malicious manipulation of data carried in IP packet transmissions, they should not be relied upon for a complete edge security solution.*

The ACLs described in this section do not screen non-IP traffic such as AppleTalk and IPX.

Contrasting Dynamic and Static ACLs

Table 7-1, below, highlights several key differences between the static ACLs configurable on switch VLANs and ports, and the dynamic port ACLs that can be assigned to individual ports by a RADIUS server.

Table 7-1. Contrasting Dynamic and Static ACLs

Dynamic Port ACLs	Static Port and VLAN ACLs
Configured in client accounts on a RADIUS server.	Configured on switch ports and VLANs.
Designed for use on the edge of the network where filtering of IP traffic entering the switch from individual, authenticated clients is most important and where clients with differing access requirements are likely to use the same port.	Designed for use where the filtering needs focus on static configurations covering: • selected routed IP traffic (RACLs) • switched or routed IP traffic entering the switch from multiple sources or from unauthenticated sources • IP traffic from multiple sources and having a destination on the switch itself
Implementation requires client authentication.	Client authentication not a factor.
Identified by the credentials (username/password pair or the MAC address) of the specific client the ACL is intended to service.	Identified by a number in the range of 1-199 or an alphanumeric name.
Supports dynamic assignment to filter only the IP traffic entering the switch from an authenticated client on the port to which the client is connected. (IP traffic can be routed or switched, and includes IP traffic having a DA on the switch itself.)	Supports static assignments to filter switched or routed IP traffic entering the switch, or routed IP traffic leaving the switch.
When the authenticated client session ends, the switch removes the RADIUS-assigned (dynamic port) ACL from the client port.	Remains statically assigned to the port or VLAN.
Allows one RADIUS-assigned (dynamic port) ACL per authenticated client on a port. (Each such ACL filters traffic from a different, authenticated client.) **Note:** The switch provides ample resources for supporting RADIUS-assigned ACLs and other features. However, the actual number of ACLs supported depends on the switch's current feature configuration and the related resource requirements. For more information, refer to the appendix titled "Monitoring Resources" in the *Management and Configuration Guide* for your switch.	Supports one each of the following: • inbound RACL • outbound RACL • VACL • static port ACL
Supports only extended ACLs. (Refer to Terminology.)	Supports standard, extended, and connection-rate ACLs. (Refer to "Configuring and Applying Connection-Rate ACLs" on page 3-19.)

Dynamic Port ACLs	Static Port and VLAN ACLs
A given dynamic port ACL filters only the IP traffic entering the switch from the authenticated client corresponding to that ACL, and does not filter IP traffic inbound from other authenticated clients.(The traffic source is not a configurable setting.)	**An RACL** applied to inbound traffic on a VLAN filters all routed IP traffic entering the switch through a port on that VLAN, as well as any inbound traffic having a DA on the switch itself. An RACL applied to outbound traffic on a VLAN filters all routed IP traffic leaving the switch through a port on that VLAN (and includes routed traffic generated by the switch itself). **A VACL** applied on a VLAN filters all IP traffic entering the switch through a port on that VLAN. **A static port ACL** applied on a port filters all traffic entering the switch through that port.
Requires client authentication by a RADIUS server configured to dynamically assign an ACL to the client port, based on client credentials.	No client authentication requirement.
ACEs allow a counter (**cnt**) option that causes a counter to increment when there is a packet match.	ACEs allow a **log** option that generates a log message whenever there is a packet match with a “deny” ACE.

Caution Regarding the Use of Source Routing

Source routing is enabled by default on the switch and can be used to override ACLs. For this reason, if you are using ACLs to enhance network security, the recommended action is to use the **no ip source-route** command to disable source routing on the switch. (If source routing is disabled in the running-config file, the **show running** command includes “**no ip source-route**” in the running-config file listing.)

How a RADIUS Server Applies a Dynamic Port ACL to a Switch Port

A dynamic port ACL configured on a RADIUS server is identified and invoked by the unique credentials (username/password pair or a client MAC address) of the specific client the ACL is designed to service. Where the username/ password pair is the selection criteria, the corresponding ACL can also be used for a group of clients that all require the same ACL policy and use the same username/password pair. Where the client MAC address is the selection criteria, only the client having that MAC address can use the corresponding ACL. When a RADIUS server authenticates a client, it also assigns the ACL configured with that client's credentials to the port. The ACL then filters the client's inbound IP traffic and denies (drops) any such traffic that is not explicitly permitted by the ACL. (Every ACL ends with an implicit **deny in ip from any to any** ("deny any any") ACE that denies IP traffic not specifically permitted by the ACL.) When the client session ends, the switch removes the dynamic port ACL from the client port.

Notes

Included in any dynamic port ACL, there is an implicit **deny in ip from any to any** ("deny any any") command that results in a default action to deny any inbound IP traffic that is not specifically permitted by the ACL. To override this default, use an explicit **permit in ip from any to any** ("permit any any") as the last ACE in the ACL.

On a given port, dynamic port ACL filtering occurs only for the traffic entering the switch from the client whose authentication configuration on the server includes a dynamic port ACL. Traffic entering the switch from another authenticated client (on the same port) whose authentication configuration on the server does not include a dynamic port ACL will *not* be filtered by an ACL assigned to the port for any other authenticated client.

Multiple Clients Sharing the Same Dynamic Port ACL. When multiple clients supported by the same RADIUS server use the same credentials, they will all be serviced by different instances of the same ACL. (The actual IP traffic inbound from any client on the switch carries a source MAC address unique to that client. The dynamic port ACL uses this MAC address to identify the traffic to be filtered.)

Multiple ACL Application Types on an Interface. The switch allows simultaneous use of all supported ACL application types on an interface. For more information, refer to "Multiple ACLs on an Interface" on page 10-20.

General ACL Features, Planning, and Configuration

These steps suggest a process for using dynamic port ACLs to establish access policies for client IP traffic.

1. Determine the polices you want to enforce for authenticated client traffic inbound on the switch.
2. Plan ACLs to execute traffic policies:
   - Apply ACLs on a per-client basis where individual clients need different traffic policies or where each client must have a different username/password pair or will authenticate using MAC authentication.
   - Apply ACLs on a client group basis where all clients in a given group can use the same traffic policy and the same username/password pair.
3. Configure the ACLs on a RADIUS server accessible to the intended clients.
4. Configure the switch to use the desired RADIUS server and to support the desired client authentication scheme. Options include 802.1X, Web authentication, or MAC authentication. (Note that the switch supports the option of simultaneously using 802.1X with either Web or MAC authentication.)
5. Test client access on the network to ensure that your RADIUS-based ACL application is properly enforcing your policies.

For further information common to all ACL applications, refer to the following sections in Chapter 10, “Access Control Lists (ACLs)”:

- “Features Common to All ACL Applications” on page 10-22
- “General Steps for Planning and Configuring ACLs” on page 10-24
- “Planning an ACL Application” on page 10-30

The Packet-filtering Process

Packet-Filtering in an applied ACL is sequential, from the first ACE in the ACL to the implicit “deny any” following the last explicit ACE. This operation is the same regardless of whether the ACL is applied dynamically from a RADIUS server or statically in the switch configuration. For details of this process, refer to “ACL Operation” in Chapter 10, “Access Control Lists (ACLs)”.

Note

If a dynamic port ACL permits an authenticated client's inbound IP packet, but the client port is also configured with a static port ACL and/or belongs to a VLAN for which there is an inbound, VLAN-based ACL configured on the switch, then the packet will also be filtered by these other ACLs. If there is a match with a deny ACE in any of these ACLs, the switch drops the packet. (If the packet is also subject to ACL mirroring, the mirroring action occurs regardless of whether a permit or deny match occurs with any other ACL.)

Caution

ACLs can enhance network security by blocking selected IP traffic, and can serve as one aspect of maintaining network security. *However, because ACLs do not provide user or device authentication, or protection from malicious manipulation of data carried in IP packet transmissions, they should not be relied upon for a complete security solution.*

Operating Rules for Dynamic Port ACLs

- **Relating a Client to a Dynamic Port ACL:** A dynamic port ACL for a particular client must be configured in the RADIUS server under the authentication credentials the server should expect for that client. (If the client must authenticate using 802.1X and/or Web Authentication, the username/password pair forms the credential set. If authentication is through MAC Authentication, then the client MAC address forms the credential set.) For more on this topic, refer to "Configuring an ACL in a RADIUS Server" on page 7-18.

- **Multiple Clients Using the Same Username/Password Pair:** Multiple clients using the same username\password pair will use duplicate instances of the same ACL.

- **Limits for ACEs in Dynamic Port ACLs:** The switch supports up to 80 characters in a single ACE. Exceeding this limit causes the related client authentication to fail.

- **Effect of Other, Statically Configured ACLs:** Suppose that port "X" belongs to VLAN "Y" and has a dynamic port ACL assignment from a RADIUS server to filter inbound traffic from an authenticated client. Port "X" is also configured with a static port ACL, and VLAN "Y" is statically configured with a VACL. Any IP traffic entering the switch on port "X" from the client and having a match with a **deny** ACE configured in *any* of these ACLs will be dropped. If an inbound RACL was also configured on VLAN "Y", then a **deny** match in the RACL would apply as well to any inbound, routed traffic from the client (and to any inbound, switched traffic having a destination on the switch itself). (If an outbound RACL was also configured on VLAN "Y", then any outbound, routed IP traffic leaving the switch through the subject port would be filtered by the outbound RACL as well.)

- **Effect of Dynamic Port ACLs on Inbound Traffic for Multiple Clients on the Same Port:** On a port configured for 802.1X *user-based* access where multiple clients are connected, if a given client's authentication results in a dynamic port ACL assignment, then the authentication of any other client concurrently using the port must also include a dynamic port ACL assignment. Thus, if a RADIUS server is configured to assign a dynamic port ACL when client "X" authenticates, but is not configured to do the same for client "Y", then traffic from client "Y" will be blocked whenever client "X" is authenticated on the port (and client "Y" will be deauthenticated). For this reason, if multiple clients are authenticated on a port, a separate dynamic port ACL must be assigned by a RADIUS server for each authenticated client. Inbound IP traffic from any client whose authentication does not result in a dynamic port ACL assignment will be blocked and the client will be deauthenticated. Also, if 802.1X *port-based* access is configured on the port, only one client can be authenticated on the port at any given time. In this case, no other inbound client traffic is allowed. For more on this topic, refer to "Static Port ACL and Dynamic Port ACL Applications" on page 10-19, and "Multiple ACLs on an Interface" on page 10-20.

Configuring an ACL in a RADIUS Server

This section provides general guidelines for configuring a RADIUS server to specify dynamic port ACLs. Also included is an example configuration for a FreeRADIUS server application. However, to configure support for these services on a specific RADIUS server application, please refer to the documentation provided with the application.

Elements in a Dynamic Port ACL Configuration. A dynamic port ACL configuration in a RADIUS server has the following elements:

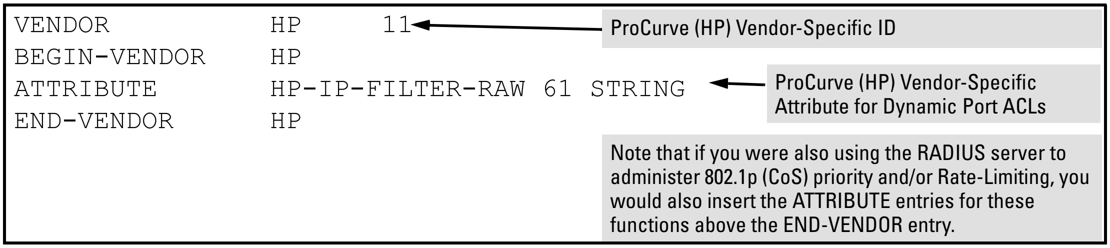
- vendor and ACL identifiers:
  - ProCurve (HP) Vendor-Specific ID: 11
  - Vendor-Specific Attribute for ACLs: 61 (string = HP-IP-FILTER-RAW)
  - Setting: HP-IP-FILTER-RAW = < "permit" or "deny" ACE >

(Note that the "string" value and the "Setting" specifier are identical.)

- ACL configuration, including:
  - one or more explicit "permit" and/or "deny" ACEs created by the system operator
  - implicit deny any any ACE automatically active after the last operator-created ACE

Example of Configuring a Dynamic Port ACL Using the FreeRADIUS Application. This example illustrates one method for configuring dynamic port ACL support for two different client identification methods (username/password and MAC address). For information on how to configure this functionality on other RADIUS server types, refer to the documentation provided with the server.

1. Enter the ProCurve vendor-specific ID and the ACL VSA in the FreeRADIUS dictionary file:



```
VENDOR          HP      11
BEGIN-VENDOR    HP
ATTRIBUTE       HP-IP-FILTER-RAW 61 STRING
END-VENDOR      HP
```

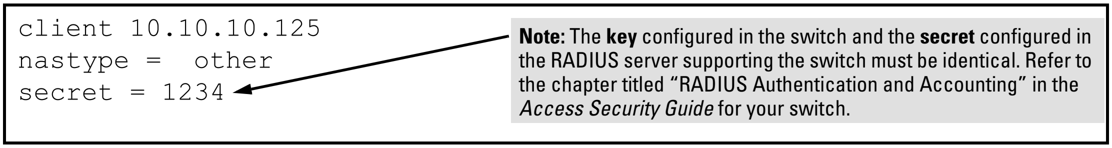
ProCurve (HP) Vendor-Specific ID

ProCurve (HP) Vendor-Specific Attribute for Dynamic Port ACLs

Note that if you were also using the RADIUS server to administer 802.1p (CoS) priority and/or Rate-Limiting, you would also insert the ATTRIBUTE entries for these functions above the END-VENDOR entry.

Figure 7-4. Example of Configuring the VSA for Dynamic Port ACLs in a FreeRADIUS Server

2. Enter the switch IP address, NAS (Network Attached Server) type, and the key in the FreeRADIUS **clients.conf** file. For example, if the switch IP address is 10.10.10.125 and the key is "1234", you would enter the following in the server's **clients.conf** file:



```
client 10.10.10.125
nastype =  other
secret = 1234
```

Note: The **key** configured in the switch and the **secret** configured in the RADIUS server supporting the switch must be identical. Refer to the chapter titled "RADIUS Authentication and Accounting" in the *Access Security Guide* for your switch.

Figure 7-5. Example of Configuring the Switch's Identity Information in a FreeRADIUS Server

3. For a given client username/password pair or MAC address, create an ACL by entering one or more ACEs in the FreeRADIUS "users" file. Enter the ACEs in an order that promotes optimum traffic management and conservation of system resources, and remember that every ACL you create

automatically includes an implicit **deny in ip from any to any** ACE. For example, suppose that you wanted to create identical ACL support for the following:

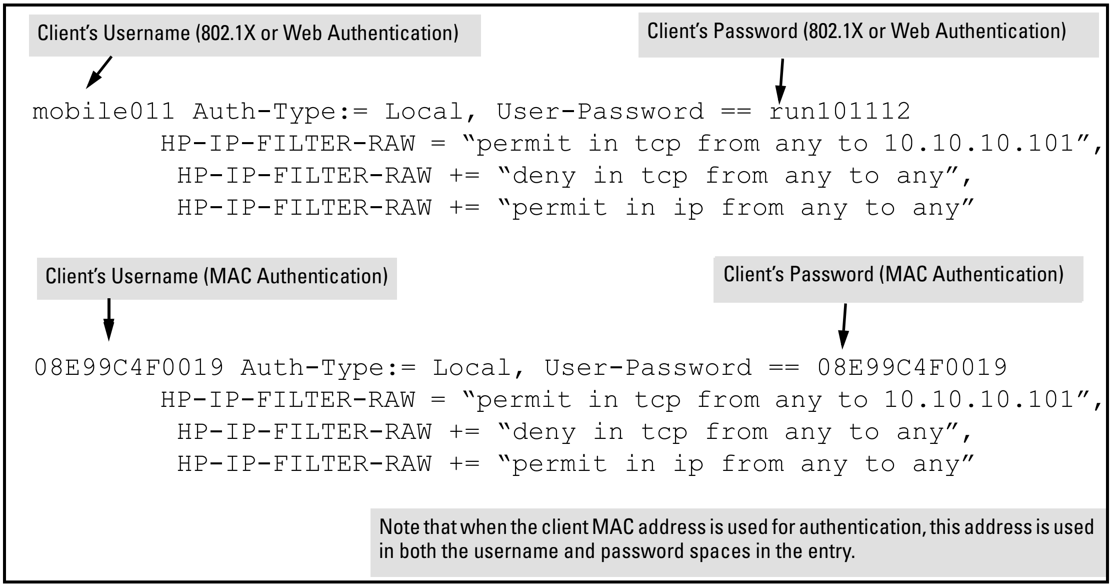
- a client having a username of “mobile011” and a password of “run101112”
- a client having a MAC address of 08 E9 9C 4F 00 19

The ACL in this example must achieve the following:

- permit http (TCP port 80) traffic from the client to the device at 10.10.10.101
- deny http (TCP port 80) traffic from the client to all other devices
- permit all other traffic from the client to all other devices

To configure the above ACL, you would enter the username/password and ACE information shown in figure7-6 into the FreeRADIUS **users** file.

Note For syntax details on dynamic port ACLs, refer to the next section, “Format Details for ACEs Configured in a Dynamic Port ACL”.


Client’s Username (802.1X or Web Authentication)
Client’s Password (802.1X or Web Authentication)
Client’s Username (MAC Authentication)
Client’s Password (MAC Authentication)

```
mobile011 Auth-Type:= Local, User-Password == run101112
        HP-IP-FILTER-RAW = “permit in tcp from any to 10.10.10.101”,
         HP-IP-FILTER-RAW += “deny in tcp from any to any”,
         HP-IP-FILTER-RAW += “permit in ip from any to any”

08E99C4F0019 Auth-Type:= Local, User-Password == 08E99C4F0019
        HP-IP-FILTER-RAW = “permit in tcp from any to 10.10.10.101”,
         HP-IP-FILTER-RAW += “deny in tcp from any to any”,
         HP-IP-FILTER-RAW += “permit in ip from any to any”
```

Note that when the client MAC address is used for authentication, this address is used in both the username and password spaces in the entry.

Figure 7-6. Example of Configuring the FreeRADIUS Server To Support ACLs for the Indicated Clients

Format Details for ACEs Configured in a Dynamic Port ACL.

Any instance of a dynamic port ACL is structured to filter authenticated client traffic as follows:

- Applies only to inbound client traffic on the switch port the authenticated client is using.
- Allows only the "any" source address (for any authenticated IP device connected to the port).
- Applies to all IP traffic from the authenticated client or to a specific type of IP traffic type from the client. Options include TCP, UDP, or any other type of IP traffic that is identified by an IP protocol number. (More information on protocol numbers is provided in the following ACL syntax description.) Has one of the following destination types:
  - A specific IP address
  - A contiguous series of IP address or an entire subnet
  - Any IP address
- Where the traffic type is either TCP or UDP, the ACE can optionally include one or more TCP or UDP port numbers.

Configuring ACE Syntax in RADIUS Servers

The following syntax and operating information applies to ACLs configured in a RADIUS server.

ACE Syntax: < permit | deny > in < ip | *ip-protocol-value* > from any to < *ip-addr* > [/< *mask* >] | > [*tcp/udp-ports*] [cnt]

< permit | deny >: *Specifies whether to forward or drop the identified IP traffic type from the authenticated client. (For information on explicitly permitting or denying all inbound IP traffic from an authenticated client, or for implicitly denying all such IP traffic not already permitted or denied, refer to "Configuration Notes" on page 7-22.)*

in: *Required keyword specifying that the ACL applies only to the traffic inbound from the authenticated client.*

< ip | *ip-protocol-value* >: *Options for specifying the type of traffic to filter.*

ip: *This option applies the ACL to all IP traffic from the authenticated client.*

ip-protocol-value: *This option applies the ACL to the type of IP traffic specified by either a protocol number or by* **tcp** *or* **udp**. *The range of protocol numbers is 0-255, and you can substitute 6 for TCP or 17 for UDP. (Protocol numbers are defined in RFC 2780. For a complete listing, refer to "Protocol Numbers" under "Protocol Number Assignment Services" on the Web site of the Internet Assigned Numbers Authority at www.iana.com.) Some examples of protocol numbers include:*

1 = ICMP
2 = IGMP
6 = TCP
17 = UDP
41 = IPv6

from any: *Required keywords specifying the (authenticated) client source. (Note that a dynamic port ACL assigned to a port filters only the inbound traffic having a source MAC address that matches the MAC address of the client whose authentication invoked the ACL assignment.)*

to: *Required destination keyword.*

< *ip-addr* >: *Specifies a single destination IP address.*

< *ip-addr* /< *mask* >: *Specifies a series of contiguous destination IP addresses or all destination IP addresses in a subnet. The < mask > is CIDR notation for the number of leftmost bits in a packet's destination IP address that must match the corresponding bits in the destination IP address listed in the ACE. For example, a destination of 10.100.17.1/24 in the ACE means that a match occurs when an inbound packet (of the designated IP type) from the authenticated client has a destination IP address where the first three octets are 10.100.17. (The fourth octet is a wildcard, and can be any value up to 255.)*

any: *Specifies any IP destination address. Use this option when you want the ACL action to apply to all traffic of the designated type, regardless of destination.*

[*tcp/udp-ports*]: *Optional TCP or UDP port specifier. Used when the ACL is intended to filter client TCP or UDP traffic with one or more specific TCP or UDP destination port numbers. You can specify port numbers as individual values and/or ranges. For example, the following ACE denies any UDP traffic from an authenticated client that has a DA of any IP address and a UDP destination port of 135, 137-139, or 445:*

```
     deny in udp from any to any 135, 137-139, 445.
```

[cnt]: *Optional counter specifier for a dynamic port ACL. When used in an ACL, the counter increments each time there is a "match" with a permit or deny ACE. This option requires that you configure the switch for RADIUS accounting.*

Configuration Notes

Explicitly Permitting Any IP Traffic. Entering a **permit in ip from any to any** (permit any any) ACE in an ACL permits all IP traffic not previously permitted or denied by that ACL. Any ACEs listed after that point do not have any effect.

Explicitly Denying Any IP Traffic. Entering a **deny in ip from any to any** ACE in an ACL denies all IP traffic not previously permitted or denied by that ACL. Any ACEs listed after that point have no effect.

Implicitly Denying Any IP Traffic. For any packet being filtered by a static port ACL, there will always be a match. That is, any packet that does not have a match with an explicit permit or deny ACE in the list will match with the implicit **deny in ip from any to any** that is automatically implied at the end of the list. Thus, the ACL denies any IP packet it filters that does not match any explicitly configured ACE. If you want an ACL to permit any packets that are not explicitly denied, you must configure **permit in ip from any to any** as the last explicit ACE in the ACL. This pre-empts the implicit **deny in ip from any to any** ACE and permits packets not explicitly permitted or denied by earlier ACEs in the list.

Configuring the Switch To Support Dynamic Port ACLs

An ACL configured in a RADIUS server is identified by the authentication credentials of the client or group of clients the ACL is designed to support. When a client authenticates with credentials associated with a particular ACL, the switch applies that ACL to the switch port the client is using. To enable the switch to forward a client's credentials to the RADIUS server, you must first configure RADIUS operation and an authentication method on the switch.

1. Configure RADIUS operation on the switch:

   Syntax: radius-server host < *ip-address* > key < *key-string* >

   This command configures the IP address and encryption key of a RADIUS server. The server should be accessible to the switch and configured to support authentication requests from clients using the switch to access the network. For more on RADIUS configuration, refer to chapter 6,"RADIUS Authentication and Accounting".

2. Configure RADIUS network accounting on the switch (optional). RADIUS network accounting is necessary to retrieve counter information if the **cnt** (counter) option is included in any of the ACEs configured on the RADIUS server.

   Syntax: aaa accounting network < start-stop | stop-only > radius

Note

Refer to the documentation provided with your RADIUS server for information on how the server receives and manages network accounting information, and how to perform any configuration steps necessary to enable the server to support network accounting data from the switch.

3. Configure an authentication method. Options include 802.1X, Web authentication, and MAC authentication. (You can configure 802.1X and either Web or MAC authentication to operate simultaneously on the same ports.)

   802.1X Option:

   Syntax: aaa port-access authenticator < *port-list* >
   aaa authentication port-access chap-radius
   aaa port-access authenticator active

These commands configure 802.1X port-based access control on the switch, and activates this feature on the specified ports. For more on 802.1X configuration and operation, refer to chapter 13, "Configuring Port-Based and User-Based Access Control (802.1X)" in this guide.

MAC Authentication Option:

Syntax: aaa port-access mac-based < *port-list* >

This command configures MAC authentication on the switch and activates this feature on the specified ports. For more on MAC authentication, refer to chapter 4, "Web and MAC Authentication".

Web Authentication Option:

Syntax: aaa port-access web-based < *port-list* >

This command configures Web authentication on the switch and activates this feature on the specified ports. For more on Web authentication, refer to chapter 4, "Web and MAC Authentication".

Displaying the Current Dynamic Port ACL Activity on the Switch

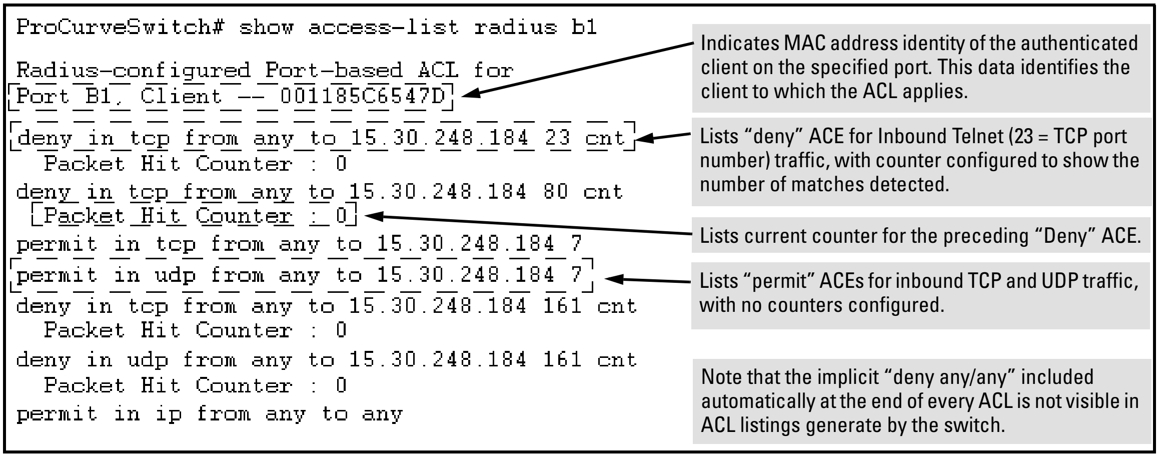
These commands output data indicating the current ACL activity imposed per-port by RADIUS server responses to client authentication.

Syntax: show access-list radius < *port-list* >

For the specified ports, this command lists the explicit ACEs, switch port, and client MAC address for each ACL dynamically assigned by a RADIUS server as a response to client authentication. If **cnt** *(counter) is included in an ACE, then the output includes the current number of inbound packet matches the switch has detected in the current session for that ACE.*

Note: *If there are no ACLs currently assigned to any port in* < port-list >, *executing this command returns only the system prompt. If a client authenticates but the server does not return a dynamic port ACL to the client port, then the server does not have a valid ACL configured and assigned to that client's authentication credentials.*

For example, the following output shows that a RADIUS server has assigned an ACL to port B1 to filter inbound traffic from an authenticated client identified by a MAC address of 00-11-85-C6-54-7D.



```
ProCurveSwitch# show access-list radius b1

Radius-configured Port-based ACL for
Port B1, Client -- 001185C6547D

deny in tcp from any to 15.30.248.184 23 cnt
  Packet Hit Counter : 0
deny in tcp from any to 15.30.248.184 80 cnt
  Packet Hit Counter : 0
permit in tcp from any to 15.30.248.184 7
permit in udp from any to 15.30.248.184 7
deny in tcp from any to 15.30.248.184 161 cnt
  Packet Hit Counter : 0
deny in udp from any to 15.30.248.184 161 cnt
  Packet Hit Counter : 0
permit in ip from any to any
```

Indicates MAC address identity of the authenticated client on the specified port. This data identifies the client to which the ACL applies.

Lists "deny" ACE for Inbound Telnet (23 = TCP port number) traffic, with counter configured to show the number of matches detected.

Lists current counter for the preceding "Deny" ACE.

Lists "permit" ACEs for inbound TCP and UDP traffic, with no counters configured.

Note that the implicit "deny any/any" included automatically at the end of every ACL is not visible in ACL listings generate by the switch.

Figure 7-7. Example Showing a Dynamic Port ACL Application to a Currently Active Client Session

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

For ports, in **< *port-list* >** *that are configured for authentication, this command indicates whether there are any RADIUS-assigned features active on the port(s). (Any ports in* **< *port-list* >** *that are not configured for authentication do not appear in this listing.)*

Port: *Port number of port configured for authentication.*

Status: *Port connection status:*

Open = *active connection with an external device*

Closed = *no active connection with an external device*

Current VLAN ID: *VLAN ID (VID) of the VLAN currently supporting the active connection.*

Current Port CoS: *Indicates the status of the current 802.1p priority setting for inbound traffic.*

No-override: *Indicates that no RADIUS-assigned 802.1p priority is currently active on the indicated port. (For more on traffic prioritization for the switches covered in this guide, refer to the chapter titled "Quality of Service (QoS): Managing Bandwidth More Effectively", in this guide.)*

0 - 7: *Indicates that the displayed 802.1p priority has been assigned by a RADIUS server to inbound traffic on the indicated port for a currently active, authenticated client session. This assignment remains active until the session ends.*

% Curr.Rate Limit Inbound: *Indicates the status of the current rate-limit setting for inbound traffic.*

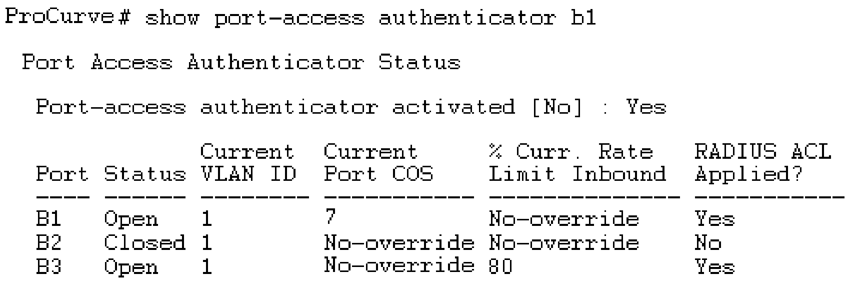
No-override: *No RADIUS-assigned rate-limit is currently active on the indicated port. (For more on rate-limiting, refer to the chapter titled "Port Traffic Controls" in the* Management and Configuration Guide *for your switch.)*

0 - 100: *Indicates that the displayed rate-limit has been assigned by a RADIUS server to inbound traffic on the indicated port for a currently active, authenticated client session. This assignment remains active until the session ends.*

RADIUS ACL Applied?: *Indicates whether a dynamic port ACL is currently active on the port.*

Yes: *An ACL has been assigned by a RADIUS server to inbound traffic on the indicated port for a currently active, authenticated client session. This assignment remains active until the session ends.*

No: *There is no dynamic port ACL currently active on the indicated port.*



```
ProCurve# show port-access authenticator b1

 Port Access Authenticator Status

  Port-access authenticator activated [No] : Yes

              Current  Current     % Curr. Rate   RADIUS ACL
  Port Status VLAN ID  Port COS    Limit Inbound  Applied?
  ---- ------ -------- ----------- -------------- -----------
  B1   Open   1        7           No-override    Yes
  B2   Closed 1        No-override No-override    No
  B3   Open   1        No-override 80             Yes
```

Figure 7-8. Example of Output Showing Current RADIUS-Applied Features

Event Log Messages

Message	Meaning
`ACE parsing error, permit/deny keyword` <*ace-#*> `client` <*mac-address*> `port` <*port-#*>.	Notifies of a problem with the `permit/deny` keyword in the indicated ACE included in the access list for the indicated client on the indicated switch port.
`Could not add ACL entry.`	Notifies that the ACE entry could not be added to the internal ACL storage.
`Could not create ACL entry.`	Notifies that the ACL could not be added to the internal ACL storage.
`Could not add ACL, client mac`<*mac-address*>`port` <*port-#*>`, at max per-port ACL quantity.`	Notifies that the ACL could not be added because the per-port ACL quantity would be exceeded.
`ACE parsing error, IN keyword,` <*ace-#*> `client` <*mac-address*> `port` <*port-#*>.	Notifies of a problem with the `IN` keyword in the indicated ACE of the access list for the indicated client on the indicated switch port.
`ACE parsing error, protocol field,` <*ace-#*> `client` <*mac-address*> `port` <*port-#*>.	Notifies of a problem with the protocol field in the indicated ACE of the access list for the indicated client on the indicated switch port.
`ACE parsing error, FROM keyword,` <*ace-#*> `client` <*mac-address*> `port` <*port-#*>.	Notifies of a problem with the `FROM` keyword in the indicated ACE of the access list for the indicated client on the indicated switch port.
`ACE parsing error, ANY keyword,` <*ace-#*> `client` <*mac-address*> `port` <*port-#*>.	Notifies of a problem with the `ANY` keyword in the indicated ACE of the access list for the indicated client on the indicated switch port.
`ACE parsing error, TO keyword,` <*ace-#*> `client` <*mac-address*> `port` <*port-#*>.	Notifies of a problem with the `TO` keyword in the indicated ACE of the access list for the indicated client on the indicated switch port.
`ACE parsing error, destination IP,` <*ace-#*> `client` <*mac-address*> `port` <*port-#*>.	Notifies of a problem with the destination IP field in the indicated ACE of the access list for the indicated client on the indicated switch port.
`ACE parsing error, tcp/udp ports,` <*ace-#*> `client` <*mac-address*> `port` <*port-#*>.	Notifies of a problem with the TCP/UDP port field in the indicated ACE of the access list for the indicated client on the indicated switch port.
`Rule limit per ACL exceeded.` <*ace-#*> `client` <*mac-address*> `port` <*port-#*>.	Notifies that an ACL has too many rules.
`Duplicate mac. An ACl exists for client. Deauthenticating second. client` <*mac-address*> `port` <*port-#*>.	Notifies that an ACL for this mac on this port already exists.

Message	Meaning
`Invalid Access-list entry length, client <`*mac-address*`> port <`*port-#*`>.`	Notifies that the string configured for an ACE entry on the Radius server exceeds 80 characters.
`Memory allocation failure for IDM ACL.`	Notifies of a memory allocation failure for a dynamic port ACL assigned by a RADIUS server performing client authentication. (This message is used in IDM and non-IDM environments.)

Causes of Client Deauthentication Immediately After Authenticating

- ACE formatted incorrectly in the RADIUS server
  - "from", "any", or "to" keyword missing
  - An IP protocol number in the ACE exceeds 255.
  - An optional UDP or TCP port number is invalid, or a UDP/TCP port number is specified when the protocol is neither UDP or TCP.
- A dynamic port ACL limit has been exceeded.
  - An ACE in the ACL for a given authenticated client exceeds 80 characters.
  - The TCP/UDP port-range quantity of 14 per slot or port group has been exceeded.
  - The rule limit of 3048 per slot or port group has been exceeded.

Monitoring Shared Resources

Currently active, RADIUS-based authentication sessions (including ProCurve IDM client sessions) using dynamic port ACLs share internal routing switch resources with several other features. The routing switch provides ample resources for all features. However, if the internal resources do become fully subscribed, new RADIUS-based sessions using dynamic port ACLs cannot be authenticated until the necessary resources are released from other applications. For information on determining the current resource availability and usage, refer to the appendix titled "Monitoring Resources" in the *Management and Configuration Guide* for your switch.