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

Per-port CoS and rate-limiting assignments through a RADIUS server are also supported in this ProCurve Manager (PCM) application. Similarly, per-port ACLs are supported in the Identity-Driven Management application used with PCM.

For information on configuring client authentication on the switch, refer to the chapter titled “RADIUS Authentication and Accounting” in the *Access Security Guide* for your switch.

Configuring a RADIUS Server To Specify Per-Port CoS and Rate-Limiting Services

Configuring the RADIUS Server

This section provides general guidelines for configuring a RADIUS server to specify 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. (Where 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 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 fields 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 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 percent-age 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
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 (not available on 4200vl switches) *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.*

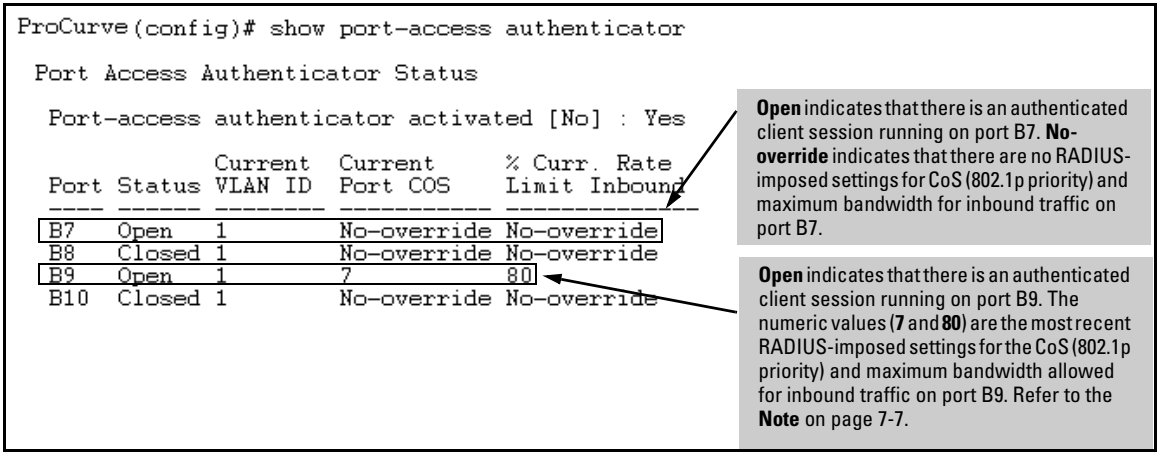

Figure 7-1. Example of Displaying Inbound CoS and Rate-Limiting Imposed by a RADIUS Session

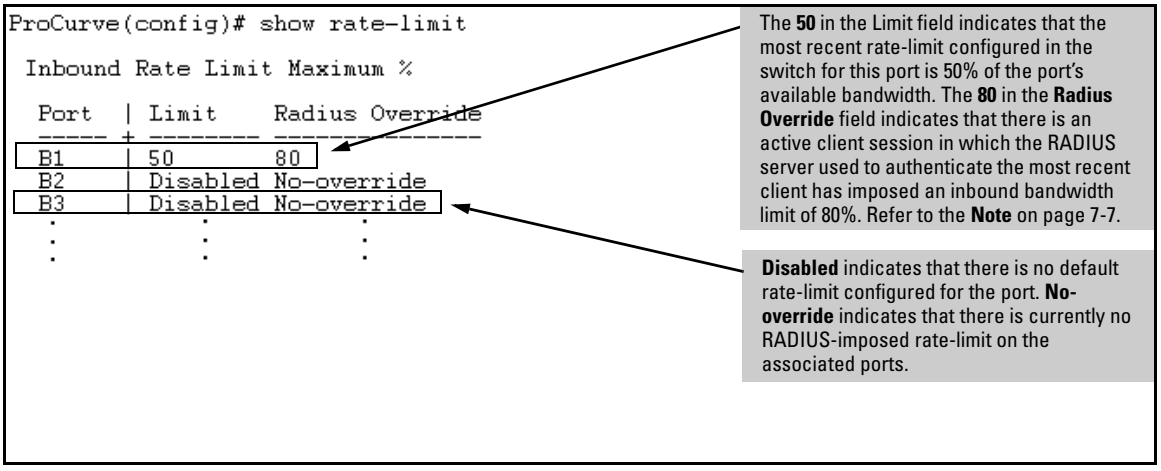

Figure 7-2. Example of Displaying Inbound Rate-Limiting Imposed by a RADIUS Session

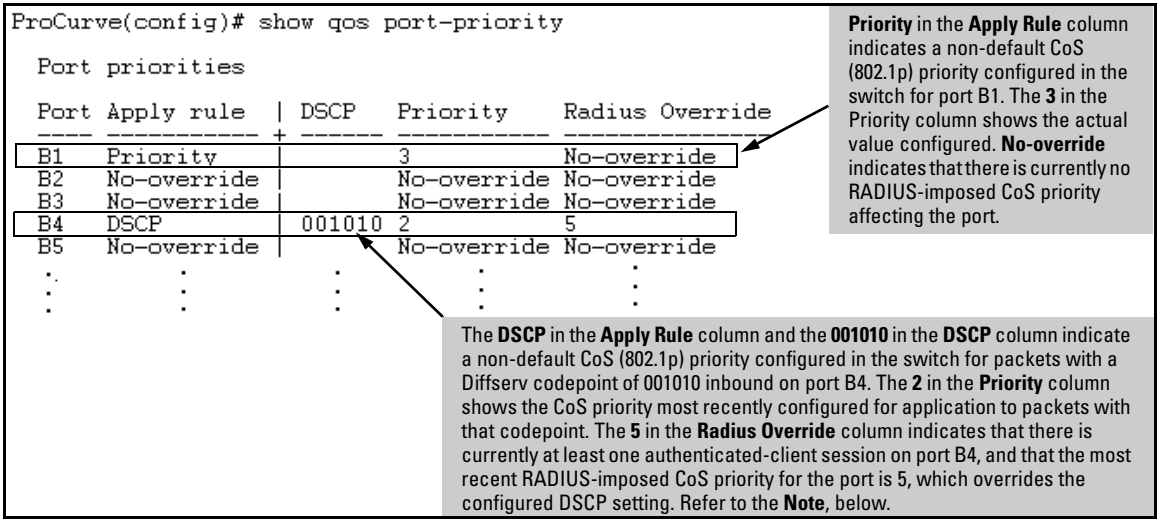

Figure 7-3. Example of Displaying Inbound CoS (802.1p) Priority Imposed by a RADIUS Session

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

This feature uses RADIUS-assigned, per-port ACLs for Layer-3 filtering of inbound IP traffic from authenticated clients. A given RADIUS-assigned ACL is identified by a unique username/password pair or client MAC address, and applies only to traffic from clients that authenticate with the same unique credentials. ACL services for an authenticated client include filtering inbound IP traffic 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

A RADIUS-assigned ACL is a type of extended ACL that filters IP traffic inbound on a port from any source (and, optionally, of any specific IP application or protocol type) to a single destination IP address, a group of contiguous IP addresses, an IP subnet, or any IP destination.

This feature is designed to accept dynamic configuration of a RADIUS-based ACL on an individual port on the network edge to filter traffic from an authenticated end-node client. Using RADIUS to apply per-port ACLs to edge

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

This feature enhances network and switch management access security 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.

Note

A RADIUS-assigned ACL filters all inbound IP traffic from an authenticated client on a port, regardless of whether the traffic is to be switched or routed. (VLAN-based ACLs configurable on 5300xl switches filter only routed traffic and traffic with a destination address—DA—on the switch itself.)

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.

Table 7-1, below, highlights several key differences between the static ACLs configurable on 5300xl switch VLANs and the dynamic ACLs that can be assigned to individual ports by a RADIUS server.

Table 7-1. Contrasting Dynamic and Static ACLs

RADIUS-Based (Dynamic) ACLs	VLAN-Based (Static) ACLs
Configured in client accounts on a RADIUS server.	Configured in the switch itself.
Designed for use on the edge of the network where filtering of inbound traffic is most important and where clients with differing access requirements are likely to use the same port at different times.	Designed for general use where the filtering needs for traffic to or from connected devices are predictable and largely static.
Implementation requires client authentication.	Client authentication not a factor.

RADIUS-Based (Dynamic) ACLs	VLAN-Based (Static) ACLs
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 inbound IP traffic from an authenticated client on the port to which the client is connected. (Traffic can be routed or switched, and includes traffic having a DA on the switch itself.)	Supports static assignments to filter either inbound or outbound for all ports in the assigned VLAN, routed IP traffic, and inbound IP traffic having a DA on the switch itself.
When the authenticated client session ends, the switch removes the RADIUS-assigned ACL from the client port.	Remains statically assigned to the VLAN unless removed by a **no vlan < *vid* > ip access-group** CLI command.
Supports a maximum of two RADIUS-based ACLs on a port. (Each ACL supports one authenticated client.)	Supports one inbound ACL and one outbound ACL per-VLAN.
Supports only extended ACLs. (Refer to Terminology.)	Supports standard, extended, and connection-rate ACLs, and applies these ACLs to traffic on all ports belonging to the VLAN.
The ACL filters only the IP traffic it receives inbound from the authenticated client corresponding to that ACL, and does not filter traffic inbound from other authenticated clients.(The traffic source is not a configurable setting.)	An ACL applied inbound on a VLAN filters all IP traffic received on any member port from any source in the same VLAN, as long as the traffic is either routed by the switch to another VLAN or subnet, or has a DA on the switch itself. An ACL applied outbound on a VLAN filters all routed IP traffic leaving the switch on any member port.
Can contain up to 30 ACEs.	Can contain up to 1024 ACEs per 5300xl switch.
Requires client authentication by a RADIUS server configured to dynamically assign an ACL to the client port, based on client credentials.	Configured in the switch and statically applied to filter IP traffic on all ports in the specified VLAN, regardless of other factors.
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.

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 RADIUS-based 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 packets that do not have a match with any explicit ACE in the named ACL.

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.

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.

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.

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 7-10.

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.)

General Operation

An ACL is a list of one or more Access Control Entries (ACEs), where each ACE consists of a matching criteria and an action (permit or deny). These ACEs are designed to control the network access privileges of an authenticated client. A RADIUS-based ACL applies only to the inbound traffic from the client whose authentication triggers the ACL assignment to the client port.

How a RADIUS Server Applies a RADIUS-Based ACL to a Switch Port

A RADIUS-based 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 from the client 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 RADIUS-based ACL from the client port.

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 traffic inbound from any client on the switch carries a source MAC address unique to that client. The RADIUS-based ACL uses this MAC address to identify the traffic to be filtered.)

Notes

On any ACL assigned to a port, 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 reverse this default, use an explicit "permit any" as the last ACE in the ACL.

On a given port, RADIUS-based ACL filtering occurs only for the inbound traffic from the client whose authentication configuration on the server includes a RADIUS-based ACL. Inbound traffic from another authenticated client (on the same port) whose authentication configuration on the server does not include a RADIUS-based ACL will not be filtered by a RADIUS-based ACL assigned to the port for any other authenticated client.

The Packet-filtering Process

Sequential Comparison and Action. When an ACL filters a packet, it sequentially compares each ACE's filtering criteria to the corresponding data in the packet until it finds a match. The action indicated by the matching ACE (deny or permit) is then performed on the packet.

Implicit Deny. If a packet does not have a match with the criteria in any of the ACEs in the ACL, the ACL denies (drops) the packet. If you need to override the implicit deny so that a packet that does not have a match will be permitted, then you can use the "permit any" option as the last ACE in the ACL. This directs the ACL to permit (forward) packets that do not have a match with any earlier ACE listed in the ACL, and prevents these packets from being filtered by the implicit "deny any".

Example. Suppose the ACL in figure 7-4 is assigned to filter the traffic from an authenticated client on a given port in the switch:

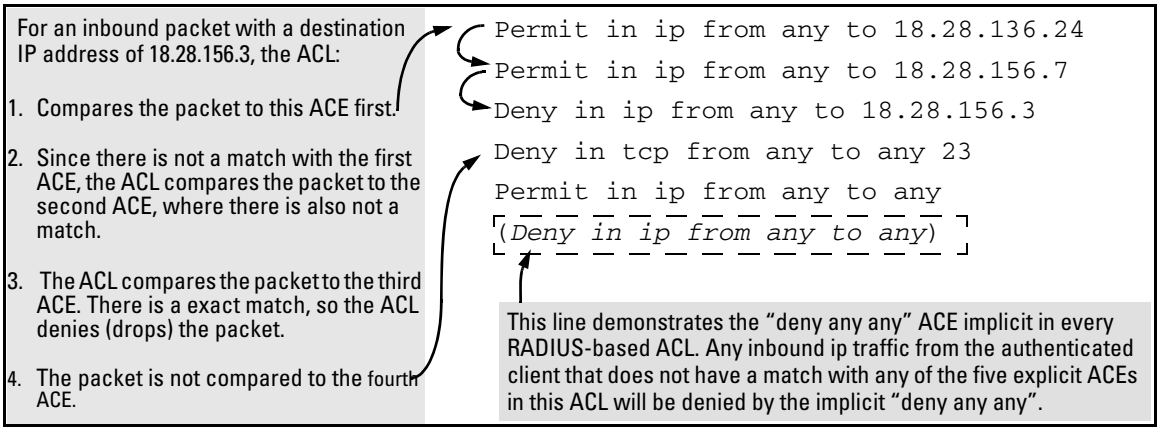

Figure 7-4. Example of Sequential Comparison

As shown above, the ACL tries to apply the first ACE in the list. If there is not a match, it tries the second ACE, and so on. When a match is found, the ACL invokes the configured action for that entry (permit or drop the packet) and no further comparisons of the packet are made with the remaining ACEs in the list. This means that when an ACE whose criteria matches a packet is found, the action configured for that ACE is invoked, and any remaining ACEs in the ACL are ignored. *Because of this sequential processing, successfully implementing an ACL depends in part on configuring ACEs in the correct order for the overall policy you want the ACL to enforce.*

Note

If a RADIUS-based ACL permits an authenticated client's inbound IP packet, but the client port 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 the VLAN-based ACL.

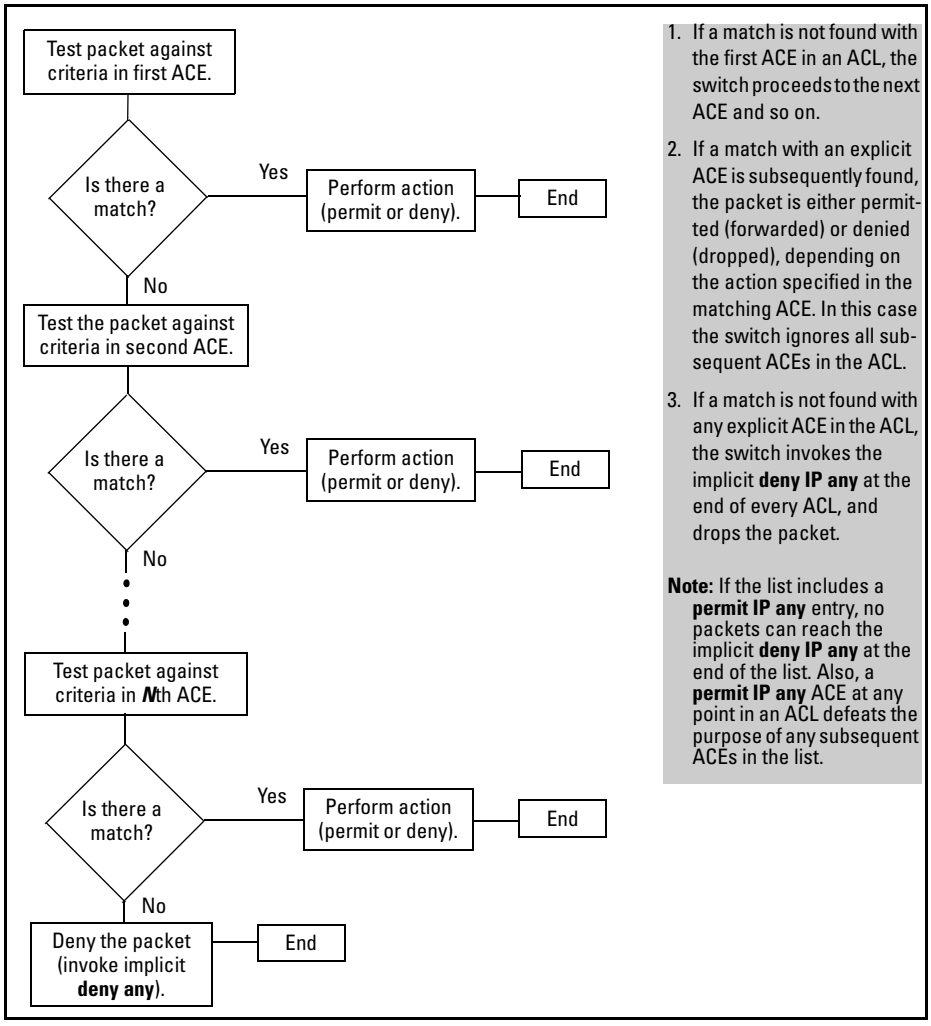

Figure 7-5. The Packet-Filtering Process in an ACL with *N* Entries (ACEs)

Note

The order in which an ACE occurs in an ACL is significant. For example, if an ACL contains six ACEs, but the first ACE is a “permit IP any”, then the ACL permits all IP traffic, and the remaining ACEs in the list do not apply, even if they specify criteria that would make a match with any of the traffic permitted by the first ACE.

For example, suppose you want to configure a RADIUS-based ACL to invoke these policies in the 11.11.11.0 network:

1. Permit inbound client traffic with a DA of 11.11.11.42.
2. Permit inbound Telnet traffic for DA 11.11.11.101.
3. Deny inbound Telnet traffic for all other IP addresses in the 11.11.11.0 network.
4. Permit inbound HTTP traffic for any IP address in the 11.11.11.0 network.
5. Deny all other inbound traffic.

The following ACL model, when invoked by a client authenticating with the credentials configured in the RADIUS server for this ACL, supports the above case:

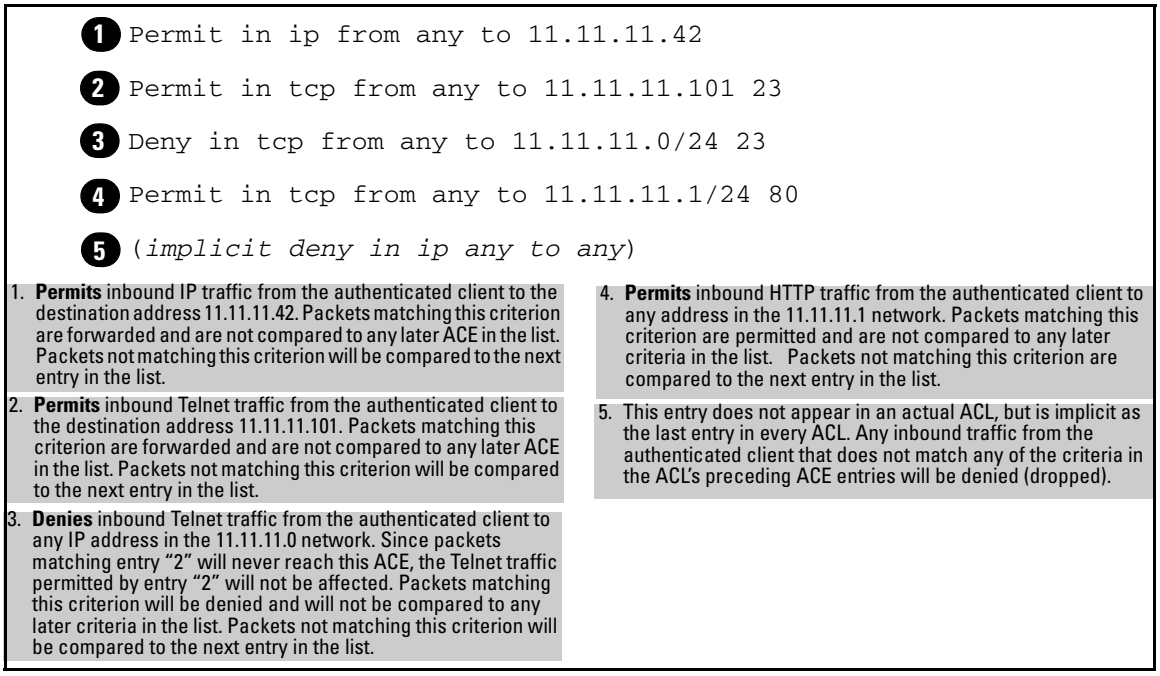

Figure 7-6. Example of How a RADIUS-Based ACL Filters Packets

It is important to remember that RADIUS-based ACLs include an implicit "deny IP any any". That is, packets received inbound from an authenticated client that the ACL does not *explicitly* permit or deny will be *implicitly* denied, and therefore dropped instead of forwarded. If you want the port to permit all inbound IP traffic (from the authenticated client) that the ACL does not explicitly permit or deny, insert a **permit in ip from any to any** ("permit any any") as the last explicit entry in the ACL.

Overriding the Implicit "deny IP any any". If you want an ACL to permit any routed packets that are not explicitly denied by other entries in the ACL, you can do so by configuring a **permit any** entry as the last entry in the ACL. Doing so permits any packet not explicitly denied by earlier entries.

General Steps

These steps suggest a process for using ACLs to establish client access policies. The topics following this section provide details.

1. Determine the polices you want to enforce for 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.

Determining Traffic Policies

This section assumes that the RADIUS server needed by a client for authentication and ACL assignments is accessible from any switch that authorized clients may use.

Begin by defining the policies you want an ACL to enforce for a given client or group of clients. This includes the type of IP traffic permitted or not permitted from the client(s) and the areas of the network the client(s) are authorized or not authorized to use.

- What traffic should you permit for the client or group? In some cases you will need to explicitly identify permitted traffic. In other cases, depending on your policies, you can insert a **permit any/any** entry at the end of the ACL so that all IP traffic not specifically matched by

earlier entries in the list will be permitted. This may be the best choice for an ACL that begins by defining the inbound client IP traffic that should be dropped.

- What traffic must be explicitly blocked for the client or group? This can include requests to access to "off-limits" subnets, unauthorized access to the internet, access to sensitive data storage or restricted equipment, and preventing the use of specific TCP or UDP applications such as Telnet, SSH, and web browser access to the switch.
- What traffic can be blocked simply by relying on the implicit **deny any/any** that is automatically included at the end of every ACL? This can reduce the number of entries needed in an ACL.
- Is it important to keep track of the number of matches for a particular client or ACE? If so, you can use the optional **cnt** (counter) feature in ACEs where you want to know this information. This is especially useful if you want to verify that the switch is denying unwanted client packets. (Note that configuring a high number of counters can exhaust the counter resources.)

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.*

Planning the ACLs Needed To Enforce Designated Traffic Policies

This section can help in understanding how to order the ACEs in a RADIUS-based ACL and in understanding how clients and the switch operate in this dynamic environment.

Guidelines for Structuring a RADIUS-Based ACL.

- The sequence of ACEs is significant. When the switch uses an ACL to determine whether to permit or deny a packet on a particular VLAN, it compares the packet to the criteria specified in the individual Access Control Entries (ACEs) in the ACL, beginning with the first ACE in the list and proceeding sequentially until a match is found. When a match is found, the switch applies the indicated action (permit or deny) to the packet. This is significant because, when a match is found for a packet, subsequent ACEs in the same ACL will not be used for that packet, regardless of whether they match the packet.
- **Inbound Traffic Only:** RADIUS-based ACLs filter only the inbound IP traffic from an authenticated client for which an ACL has been configured on the appropriate RADIUS server.
- **Result of an ACE/Packet Match:** The first match of a given packet to an ACE dictates the action for that packet. Any subsequent match possibilities are ignored.
- **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 an ACL, there will always be a match. Included in every ACL is an implicit **deny in ip from any to any**. This means that the ACL denies any IP packet it filters that does not have a match with an explicitly configured ACE. Thus, 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. Because, for a given packet, the switch sequentially applies the ACEs in an ACL until it finds a

match, any packet that reaches the **permit in ip from any to any** entry will be permitted, and will not reach the implicit **deny in ip from any to any** ACE that is included at the end of the ACL.

- Determine the order in which you want the individual ACEs in the ACL to filter inbound traffic from a client. A general guideline is to arrange the ACEs in the expected order of decreasing application frequency. This will result in the most prevalent traffic types finding a match earlier in the ACL than traffic types that are more infrequent, thus saving processing cycles.

Operating Rules for RADIUS-Based ACLs

- **Relating a Client to a RADIUS-Based ACL:** A RADIUS-based 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 7-22.

- **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 RADIUS-Based ACLs, Associated ACEs, and Counters:**

  The table below describes limits the switch supports in ACLs applied by a RADIUS server. Exceeding a limit causes the related client authentication to fail.

Table 7-2. Limits Affecting RADIUS-Based ACL Applications

Item	Limit	Notes
Maximum Number of Authenticated Sessions Per-Port Using RADIUS-based ACLs	2	A port supports a maximum of two ACLs (or two instances of the same ACL) on a given port at the same time. *This rule does not affect the number of authenticated clients a port supports (32); only the number of authenticated clients using RADIUS-based ACLs.* If two authenticated clients are already using RADIUS-based ACLs on a port and a third client on the same port attempts to authenticate with a RADIUS server account that includes an ACL assignment, the attempt will fail.
Maximum Number of (internal) ACEs Per-Port, and Maximum Number of (internal) ACEs Per-ACL	30	Depending on how a RADIUS-assigned ACE is formed, it can consume multiple internal ACEs. A RADIUS-assigned ACE that does not specify TCP or UDP port numbers uses one internal ACE. However, an ACE that includes TCP or UDP port numbers uses one or more internal ACE resources, depending on the port number groupings. A single TCP or UDP port number or a series of contiguous port numbers comprise one group. For example, "80" and "137-146" each form one group. "135, 137-140, 143" in a given ACE form three groups. The following ACE examples illustrate how the switch applies internal ACE usage. **Examples of Single and Multiple (Internal) ACEs Per-Port** — **Internal ACEs** deny in ip from any to any — 1 deny in tcp from any to any — 1 deny in tcp from any to any 80 — 1 permit in tcp from any to any 135, 137-146, 445 — 3 permit in tcp from any to any 135-137, 139, 141, 143, 146, 445 — 6 permit in tcp from any to any 135-146, 445 — 2 Where two authenticated clients are using RADIUS-based ACLs on the same port, the total number of ACEs in both active sessions cannot exceed the maximum.
Maximum Number of Characters in a single ACE	80	—
Maximum Number of (optional) Internal Counters Used Per-Module	100	Depending on how an ACE is formed, using the **cnt** (counter) option consumes one or more internal counters. Using a counter in an ACE that does not specify TCP or UDP port numbers uses one counter. Using a counter in an ACE that includes TCP or UDP port numbers uses one or more counters, depending on the port number groupings. A single TCP or UDP port number or a series of contiguous port numbers comprise one group. For example, "80" and "137-146" each form one group. "135, 137-140, 143" in a given ACE form three groups. The following ACE examples illustrate how the switch calculates internal counter groups. **Examples of ACEs Employing Counters** — **Internal Counters** deny in ip from any to any cnt — 1 deny in tcp from any to any cnt — 1 deny in tcp from any to any 80 cnt — 1 permit in tcp from any to any 135, 137-146, 445 cnt — 3 permit in tcp from any to any 135-137, 139, 141, 143, 146, 445 cnt — 6 permit in tcp from any to any 135-146, 445 cnt — 2

- **Effect of VLAN-Based ACLs Configured on the Switch:** A port receiving a dynamic, RADIUS-based ACL assignment can also belong to a VLAN for which there is an inbound ACL statically configured (on the switch). In this case, an IP packet permitted by the RADIUS-based ACL will also be filtered by the VLAN-based ACL if the inbound client packets are routed or have a DA on the switch itself. If the RADIUS-based ACL permits the packet, but the VLAN-based, inbound ACL denies the packet, then the packet is dropped. If the RADIUS-based ACL denies the packet, then the packet is dropped and does not reach the VLAN-based, inbound ACL. (RADIUS-based ACLs operate only on inbound IP traffic, and are not a factor for the traffic filtered by VLAN-based, outbound ACLs.)

- **A RADIUS-Based ACL Affects Only the Inbound Traffic from a Specific, Authenticated Client:** A RADIUS-based ACL assigned to a port as the result of a client authenticating on that port applies only to the inbound traffic received on that port from that client. It does not affect the traffic received from any other authenticated clients on that port, and does not affect any outbound traffic on that port.

Configuring an ACL in a RADIUS Server

This section provides general guidelines for configuring a RADIUS server to specify RADIUS-based 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 RADIUS-Based ACL Configuration. A RADIUS-based ACL configuration in a RADIUS server has the following elements:

- vendor and ACL identifiers:
  - ProCurve 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 RADIUS-based ACL Using the FreeRADIUS Application. This example illustrates one method for configuring RADIUS-based 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:

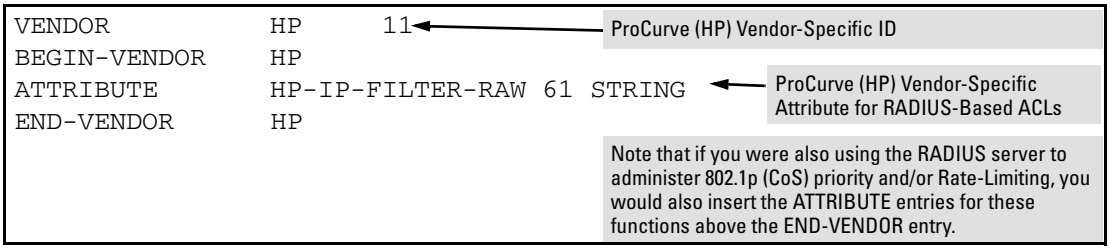

Figure 7-7. Example of Configuring the VSA for RADIUS-Based ACLs in a FreeRADIUS Server

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:

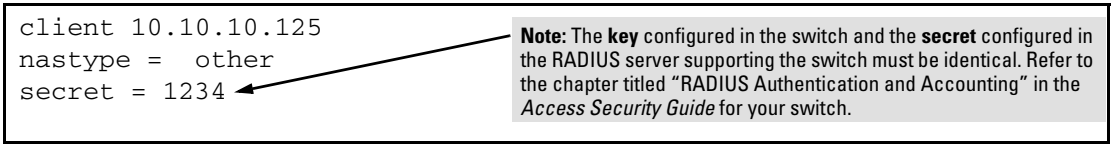

Figure 7-8. Example of Configuring the Switch's Identity Information in a FreeRADIUS Server

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. (Refer to "Guidelines for Structuring a RADIUS-Based ACL" on page 7-19.) 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 figure7-9 into the FreeRADIUS **users** file.

Note For syntax details on RADIUS-based ACLs, refer to "Format Details for ACEs Configured in a RADIUS-Based ACL" on page 7-24.

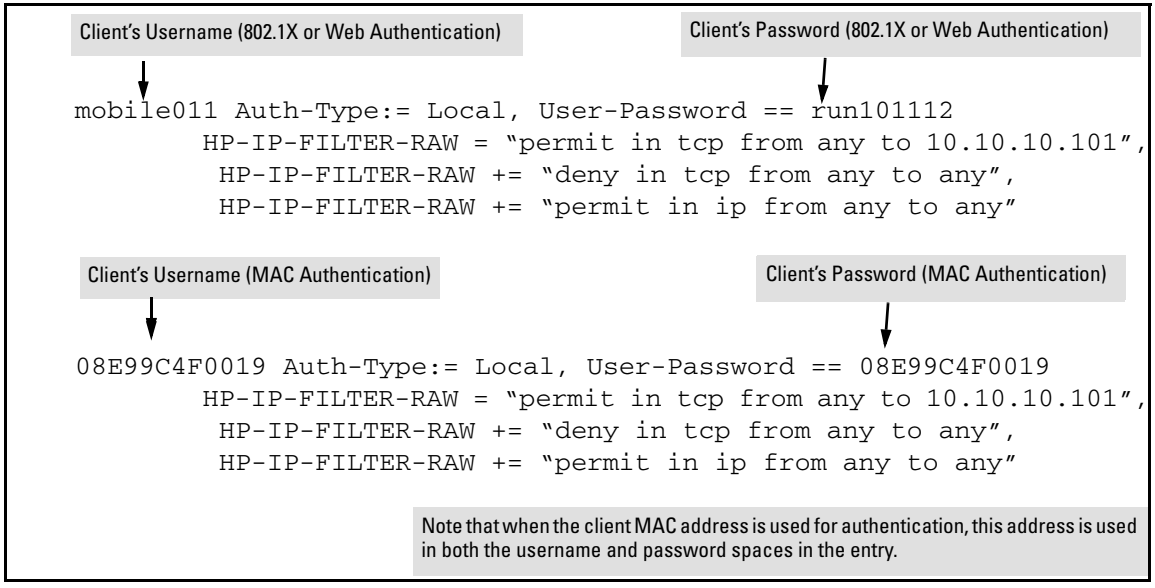

Figure 7-9. Example of Configuring the FreeRADIUS Server To Support ACLs for the Indicated Clients

Format Details for ACEs Configured in a RADIUS-Based ACL.

Any instance of a RADIUS-Based 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.

The following syntax and operating information refers 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.*

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

from any: *Required keywords specifying the (authenticated) client source. (Note that a RADIUS-Based 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 RADIUS-based 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. (Refer to the entry describing the maximum number of (optional) internal counters in Table 6-1 on page 6-7.)*

Configuring the Switch To Support RADIUS-Based 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 the chapter titled "RADIUS Authentication and Accounting" in the *Access Security Guide* for your switch.

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 the chapter titled “Configuring Port-Based and Client-Based Access Control” in the *Access Security Guide* for your switch.

   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 the chapter titled “Web and MAC Authentication” in the *Access Security Guide* for your switch.

   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 the chapter titled “Web and MAC Authentication” in the *Access Security Guide* for your switch.

Displaying the Current RADIUS-Based 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 RADIUS-based 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.

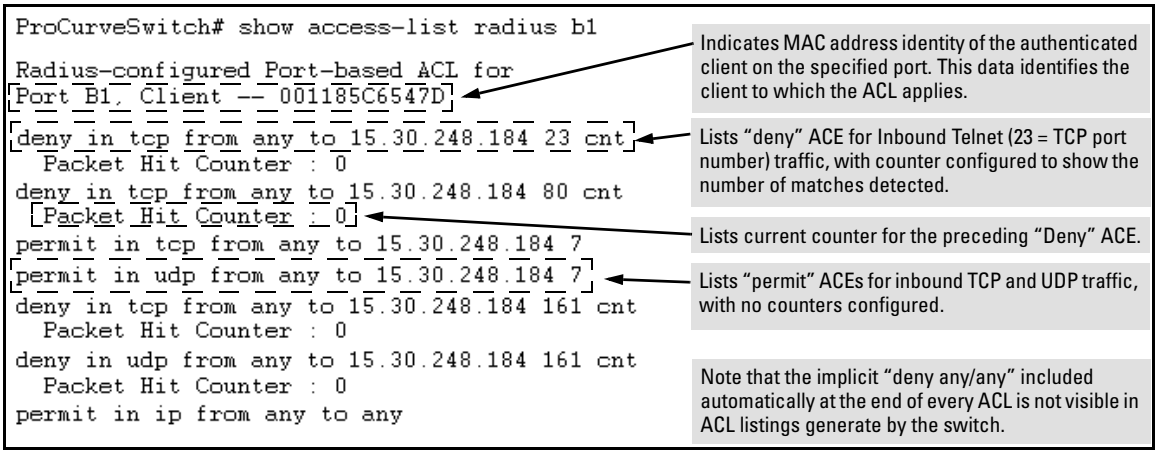

Figure 7-10. Example Showing a RADIUS-Based ACL Application to a Currently Active Client Session

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 5300xl switches, refer to the chapter titled "Quality of Service (QoS): Managing Bandwidth More Effectively" in the Advanced Traffic Management Guide for your switch.)*

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 RADIUS-assigned 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 RADIUS-assigned ACL currently active on the indicated port.*

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.

Message	Meaning
`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. A maximum of 30 (internal) ACEs are allowed per ACL. Refer to Table 7-2 on page 21.
`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.
`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 RADIUS-based ACL. User Action?
`ACE limit per port exceeded. client <mac-address> port <port-#>.`	Notifies that the maximum number of ACEs (30) allowed on the port was exceeded.
`Exceeded counter per slot limit. client <mac-address> port <port-#>.`	Notifies that the internal counter (cnt) limit of 100 per module was exceeded on port *<port-#>*. Refer to Table 7-2 on page 21.

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.

- A RADIUS-Based ACL limit has been exceeded. (Refer to table 7-2, "Limits Affecting RADIUS-Based ACL Applications" on page 7-21.)
  - The allowed maximum of two RADIUS-assigned ACLs has already been reached on the port through which the deauthenticated client is trying to access the network. (Each client requiring a RADIUS-assigned ACL is a separate instance, even if multiple clients are assigned the same ACL.)
  - For a given port on a given module, the latest client authentication includes a RADIUS-Based ACL assignment exceeding the maximum number of ACEs allowed on the module.
  - An ACE in the ACL for a given authenticated client exceeds 80 characters.
  - An ACL assigned to an authenticated client causes the number of optional counters needed on the module supporting the client's port to exceed the per-module maximum (100).