Configuring RADIUS

- Finding Feature Information, page 1
- Prerequisites for Controlling Switch Access with RADIUS, page 1
- Restrictions for Controlling Switch Access with RADIUS, page 2
- Information about RADIUS, page 3
- How to Configure RADIUS, page 15
- Monitoring CoA Functionality, page 29
- Configuration Examples for Controlling Switch Access with RADIUS, page 29

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Related Topics
- Feature History and Information for Troubleshooting Software Configuration

Prerequisites for Controlling Switch Access with RADIUS

This section lists the prerequisites for controlling Catalyst 3850 switch access with RADIUS.

General:

- RADIUS and AAA must be enabled to use any of the configuration commands in this chapter.
- RADIUS is facilitated through AAA and can be enabled only through AAA commands.
- At a minimum, you must identify the host or hosts that run the RADIUS server software and define the method lists for RADIUS authentication. You can optionally define method lists for RADIUS authorization and accounting.
• You should have access to and should configure a RADIUS server before configuring RADIUS features on your switch.

• The RADIUS host is normally a multiuser system running RADIUS server software from Cisco (Cisco Secure Access Control Server Version 3.0), Livingston, Merit, Microsoft, or another software provider. For more information, see the RADIUS server documentation.

• To use the Change-of-Authorization (CoA) interface, a session must already exist on the switch. CoA can be used to identify a session and enforce a disconnect request. The update affects only the specified session.

• A redundant connection between a switch stack and the RADIUS server is recommended. This is to help ensure that the RADIUS server remains accessible in case one of the connected stack members is removed from the switch stack.

For RADIUS operation:

• Users must first successfully complete RADIUS authentication before proceeding to RADIUS authorization, if it is enabled.

Related Topics

RADIUS and Switch Access, on page 3
RADIUS Operation, on page 4

Restrictions for Controlling Switch Access with RADIUS

This topic covers restrictions for controlling switch access with RADIUS.

General:

• To prevent a lapse in security, you cannot configure RADIUS through a network management application.

RADIUS is not suitable in the following network security situations:

• Multiprotocol access environments. RADIUS does not support AppleTalk Remote Access (ARA), NetBIOS Frame Control Protocol (NBFCP), NetWare Asynchronous Services Interface (NASI), or X.25 PAD connections.

• Switch-to-switch or router-to-router situations. RADIUS does not provide two-way authentication. RADIUS can be used to authenticate from one device to a non-Cisco device if the non-Cisco device requires authentication.

• Networks using a variety of services. RADIUS generally binds a user to one service model.

Related Topics

RADIUS Overview, on page 3
Information about RADIUS

RADIUS and Switch Access

This section describes how to enable and configure RADIUS. RADIUS provides detailed accounting information and flexible administrative control over the authentication and authorization processes.


Note

For complete syntax and usage information for the commands used in this section, see the Cisco IOS Security Command Reference, Release 12.4 and the Cisco IOS IPv6 Command Reference.

Related Topics

Prerequisites for Controlling Switch Access with RADIUS, on page 1
Configuring the Switch for Local Authentication and Authorization
SSH Servers, Integrated Clients, and Supported Versions

RADIUS Overview

RADIUS is a distributed client/server system that secures networks against unauthorized access. RADIUS clients run on supported Cisco routers and switches. Clients send authentication requests to a central RADIUS server, which contains all user authentication and network service access information.

Use RADIUS in these network environments that require access security:

• Networks with multiple-vendor access servers, each supporting RADIUS. For example, access servers from several vendors use a single RADIUS server-based security database. In an IP-based network with multiple vendors’ access servers, dial-in users are authenticated through a RADIUS server that has been customized to work with the Kerberos security system.

• Turnkey network security environments in which applications support the RADIUS protocol, such as in an access environment that uses a smart card access control system. In one case, RADIUS has been used with Enigma’s security cards to validates users and to grant access to network resources.

• Networks already using RADIUS. You can add a Cisco switch containing a RADIUS client to the network. This might be the first step when you make a transition to a TACACS+ server. See Figure 2: Transitioning from RADIUS to TACACS+ Services below.

• Network in which the user must only access a single service. Using RADIUS, you can control user access to a single host, to a single utility such as Telnet, or to the network through a protocol such as IEEE 802.1x. For more information about this protocol, see Chapter 11, “Configuring IEEE 802.1x Port-Based Authentication.”
Networks that require resource accounting. You can use RADIUS accounting independently of RADIUS authentication or authorization. The RADIUS accounting functions allow data to be sent at the start and end of services, showing the amount of resources (such as time, packets, bytes, and so forth) used during the session. An Internet service provider might use a freeware-based version of RADIUS access control and accounting software to meet special security and billing needs.

**Figure 1: Transitioning from RADIUS to TACACS+ Services**

---

**RADIUS Operation**

When a user attempts to log in and authenticate to a switch that is access controlled by a RADIUS server, these events occur:

1. The user is prompted to enter a username and password.
2. The username and encrypted password are sent over the network to the RADIUS server.
3. The user receives one of the following responses from the RADIUS server:
   - ACCEPT—The user is authenticated.
   - REJECT—The user is either not authenticated and is prompted to re-enter the username and password, or access is denied.
   - CHALLENGE—A challenge requires additional data from the user.
   - CHALLENGE PASSWORD—A response requests the user to select a new password.

The ACCEPT or REJECT response is bundled with additional data that is used for privileged EXEC or network authorization. The additional data included with the ACCEPT or REJECT packets includes these items:
• Telnet, SSH, rlogin, or privileged EXEC services
• Connection parameters, including the host or client IP address, access list, and user timeouts

Related Topics
Prerequisites for Controlling Switch Access with RADIUS, on page 1

RADIUS Change of Authorization

This section provides an overview of the RADIUS interface including available primitives and how they are used during a Change of Authorization (CoA).

• Change-of-Authorization Requests
• CoA Request Response Code
• CoA Request Commands
• Session Reauthentication
• Stacking Guidelines for Session Termination

A standard RADIUS interface is typically used in a pulled model where the request originates from a network attached device and the response come from the queried servers. Catalyst switches support the RADIUS Change of Authorization (CoA) extensions defined in RFC 5176 that are typically used in a pushed model and allow for the dynamic reconfiguring of sessions from external authentication, authorization, and accounting (AAA) or policy servers.

The switch supports these per-session CoA requests:

• Session reauthentication
• Session termination
• Session termination with port shutdown
• Session termination with port bounce

This feature is integrated with the Cisco Secure Access Control Server (ACS) 5.1.

The RADIUS interface is enabled by default on Catalyst switches. However, some basic configuration is required for the following attributes:

• Security and Password—refer to the “Preventing Unauthorized Access to Your Switch” section in the Configuring Switch-Based Authentication chapter in the Catalyst 3750 Switch Software Configuration Guide, 12.2(50)SE.

• Accounting—refer to the “Starting RADIUS Accounting” section in the Configuring Switch-Based Authentication chapter in the Catalyst 3750 Switch Software Configuration Guide, 12.2(50)SE.

Change-of-Authorization Requests

Change of Authorization (CoA) requests, as described in RFC 5176, are used in a push model to allow for session identification, host reauthentication, and session termination. The model is comprised of one request (CoA-Request) and two possible response codes:
• CoA acknowledgment (ACK) [CoA-ACK]
• CoA non-acknowledgment (NAK) [CoA-NAK]

The request is initiated from a CoA client (typically a RADIUS or policy server) and directed to the switch that acts as a listener.

**RFC 5176 Compliance**

The Disconnect Request message, which is also referred to as Packet of Disconnect (POD), is supported by the switch for session termination.

This table shows the IETF attributes supported for this feature.

*Table 1: Supported IETF Attributes*

<table>
<thead>
<tr>
<th>Attribute Number</th>
<th>Attribute Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>24</td>
<td>State</td>
</tr>
<tr>
<td>31</td>
<td>Calling-Station-ID</td>
</tr>
<tr>
<td>44</td>
<td>Acct-Session-ID</td>
</tr>
<tr>
<td>80</td>
<td>Message-Authenticator</td>
</tr>
<tr>
<td>101</td>
<td>Error-Cause</td>
</tr>
</tbody>
</table>

This table shows the possible values for the Error-Cause attribute.

*Table 2: Error-Cause Values*

<table>
<thead>
<tr>
<th>Value</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>201</td>
<td>Residual Session Context Removed</td>
</tr>
<tr>
<td>202</td>
<td>Invalid EAP Packet (Ignored)</td>
</tr>
<tr>
<td>401</td>
<td>Unsupported Attribute</td>
</tr>
<tr>
<td>402</td>
<td>Missing Attribute</td>
</tr>
<tr>
<td>403</td>
<td>NAS Identification Mismatch</td>
</tr>
<tr>
<td>404</td>
<td>Invalid Request</td>
</tr>
<tr>
<td>405</td>
<td>Unsupported Service</td>
</tr>
<tr>
<td>406</td>
<td>Unsupported Extension</td>
</tr>
<tr>
<td>407</td>
<td>Invalid Attribute Value</td>
</tr>
</tbody>
</table>
### CoA Request Response Code

The CoA Request response code can be used to convey a command to the switch.

**Related Topics**

CoA Request Commands, on page 8

#### Session Identification

For disconnect and CoA requests targeted at a particular session, the switch locates the session based on one or more of the following attributes:

- Calling-Station-Id (IETF attribute #31 which contains the host MAC address)
- Audit-Session-Id (Cisco VSA)
- Acct-Session-Id (IETF attribute #44)

Unless all session identification attributes included in the CoA message match the session, the switch returns a Disconnect-NAK or CoA-NAK with the "Invalid Attribute Value" error-code attribute.

If more than one session identification attribute is included in the message, all the attributes must match the session or the switch returns a Disconnect-negative acknowledgment (NAK) or CoA-NAK with the error code "Invalid Attribute Value."

The packet format for a CoA Request code as defined in RFC 5176 consists of the fields: Code, Identifier, Length, Authenticator, and Attributes in Type:Length:Value (TLV) format.

<table>
<thead>
<tr>
<th>Value</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>501</td>
<td>Administratively Prohibited</td>
</tr>
<tr>
<td>502</td>
<td>Request Not Routable (Proxy)</td>
</tr>
<tr>
<td>503</td>
<td>Session Context Not Found</td>
</tr>
<tr>
<td>504</td>
<td>Session Context Not Removable</td>
</tr>
<tr>
<td>505</td>
<td>Other Proxy Processing Error</td>
</tr>
<tr>
<td>506</td>
<td>Resources Unavailable</td>
</tr>
<tr>
<td>507</td>
<td>Request Initiated</td>
</tr>
<tr>
<td>508</td>
<td>Multiple Session Selection Unsupported</td>
</tr>
</tbody>
</table>
The attributes field is used to carry Cisco vendor-specific attributes (VSAs).

**Related Topics**

- CoA Disconnect-Request, on page 10
- CoA Request: Disable Host Port, on page 10
- CoA Request: Bounce-Port, on page 10

**CoA ACK Response Code**

If the authorization state is changed successfully, a positive acknowledgment (ACK) is sent. The attributes returned within CoA ACK will vary based on the CoA Request and are discussed in individual CoA Commands.

**CoA NAK Response Code**

A negative acknowledgment (NAK) indicates a failure to change the authorization state and can include attributes that indicate the reason for the failure. Use `show` commands to verify a successful CoA.

**CoA Request Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Cisco VSA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reauthenticate host</td>
<td>Cisco:Avpair=&quot;subscriber:command=reauthenticate&quot;</td>
</tr>
<tr>
<td>Terminate session</td>
<td>This is a standard disconnect request that does not require a VSA.</td>
</tr>
<tr>
<td>Bounce host port</td>
<td>Cisco:Avpair=&quot;subscriber:command=bounce-host-port&quot;</td>
</tr>
<tr>
<td>Disable host port</td>
<td>Cisco:Avpair=&quot;subscriber:command=disable-host-port&quot;</td>
</tr>
</tbody>
</table>

1 All CoA commands must include the session identifier between the switch and the CoA client.

**Related Topics**

- CoA Request Response Code, on page 7

**Session Reauthentication**

The AAA server typically generates a session reauthentication request when a host with an unknown identity or posture joins the network and is associated with a restricted access authorization profile (such as a guest...
A reauthentication request allows the host to be placed in the appropriate authorization group when its credentials are known.

To initiate session authentication, the AAA server sends a standard CoA-Request message which contains a Cisco VSA in this form: *Cisco:Avpair="subscriber:command=reauthenticate"* and one or more session identification attributes.

The current session state determines the switch response to the message. If the session is currently authenticated by IEEE 802.1x, the switch responds by sending an EAPoL (Extensible Authentication Protocol over Lan) -RequestId message to the server.

If the session is currently authenticated by MAC authentication bypass (MAB), the switch sends an access-request to the server, passing the same identity attributes used for the initial successful authentication.

If session authentication is in progress when the switch receives the command, the switch terminates the process, and restarts the authentication sequence, starting with the method configured to be attempted first. If the session is not yet authorized, or is authorized via guest VLAN, or critical VLAN, or similar policies, the reauthentication message restarts the access control methods, beginning with the method configured to be attempted first. The current authorization of the session is maintained until the reauthentication leads to a different authorization result.

### Session Reauthentication in a Switch Stack

When a switch stack receives a session reauthentication message:

- It checkpoints the need for a re-authentication before returning an acknowledgment (ACK).
- It initiates reauthentication for the appropriate session.
- If authentication completes with either success or failure, the signal that triggered the reauthentication is removed from the stack member.
- If the stack master fails before authentication completes, reauthentication is initiated after stack master switch-over based on the original command (which is subsequently removed).
- If the stack master fails before sending an ACK, the new stack master treats the re-transmitted command as a new command.

### Session Termination

There are three types of CoA requests that can trigger session termination. A CoA Disconnect-Request terminates the session, without disabling the host port. This command causes re-initialization of the authenticator state machine for the specified host, but does not restrict that host’s access to the network.

To restrict a host’s access to the network, use a CoA Request with the Cisco:Avpair="subscriber:command=disable-host-port" VSA. This command is useful when a host is known to be causing problems on the network, and you need to immediately block network access for the host. When you want to restore network access on the port, re-enable it using a non-RADIUS mechanism.

When a device with no supplicant, such as a printer, needs to acquire a new IP address (for example, after a VLAN change), terminate the session on the host port with port-bounce (temporarily disable and then re-enable the port).
**CoA Disconnect-Request**

This command is a standard Disconnect-Request. Because this command is session-oriented, it must be accompanied by one or more of the session identification attributes. If the session cannot be located, the switch returns a Disconnect-NAK message with the "Session Context Not Found" error-code attribute. If the session is located, the switch terminates the session. After the session has been completely removed, the switch returns a Disconnect-ACK.

If the switch fails-over to a standby switch before returning a Disconnect-ACK to the client, the process is repeated on the new active switch when the request is re-sent from the client. If the session is not found following re-sending, a Disconnect-ACK is sent with the "Session Context Not Found" error-code attribute.

**Related Topics**

  - [Session Identification, on page 7](#)

**CoA Request: Disable Host Port**

This command is carried in a standard CoA-Request message that has this new VSA:

`Cisco:Avpair="subscriber:command=disable-host-port"

Because this command is session-oriented, it must be accompanied by one or more of the session identification attributes. If the session cannot be located, the switch returns a CoA-NAK message with the "Session Context Not Found" error-code attribute. If the session is located, the switch disables the hosting port and returns a CoA-ACK message.

If the switch fails before returning a CoA-ACK to the client, the process is repeated on the new active switch when the request is re-sent from the client. If the switch fails after returning a CoA-ACK message to the client but before the operation has completed, the operation is restarted on the new active switch.

**Note**

A Disconnect-Request failure following command re-sending could be the result of either a successful session termination before change-over (if the Disconnect-ACK was not sent) or a session termination by other means (for example, a link failure) that occurred after the original command was issued and before the standby switch became active.

**Related Topics**

  - [Session Identification, on page 7](#)

**CoA Request: Bounce-Port**

This command is carried in a standard CoA-Request message that contains the following VSA:

`Cisco:Avpair="subscriber:command=bounce-host-port"

Because this command is session-oriented, it must be accompanied by one or more of the session identification attributes. If the session cannot be located, the switch returns a CoA-NAK message with the "Session Context Not Found" error-code attribute. If the session is located, the switch disables the hosting port for a period of 10 seconds, re-enables it (port-bounce), and returns a CoA-ACK.
If the switch fails before returning a CoA-ACK to the client, the process is repeated on the new active switch when the request is re-sent from the client. If the switch fails after returning a CoA-ACK message to the client but before the operation has completed, the operation is re-started on the new active switch.

Related Topics
   Session Identification, on page 7

Stacking Guidelines for Session Termination

No special handling is required for CoA Disconnect-Request messages in a switch stack.

Stacking Guidelines for CoA-Request Bounce-Port

Because the bounce-port command is targeted at a session, not a port, if the session is not found, the command cannot be executed.

When the Auth Manager command handler on the stack master receives a valid bounce-port command, it checkpoints the following information before returning a CoA-ACK message:

- the need for a port-bounce
- the port-id (found in the local session context)

The switch initiates a port-bounce (disables the port for 10 seconds, then re-enables it).

If the port-bounce is successful, the signal that triggered the port-bounce is removed from the standby stack master.

If the stack master fails before the port-bounce completes, a port-bounce is initiated after stack master change-over based on the original command (which is subsequently removed).

If the stack master fails before sending a CoA-ACK message, the new stack master treats the re-sent command as a new command.

Stacking Guidelines for CoA-Request Disable-Port

Because the disable-port command is targeted at a session, not a port, if the session is not found, the command cannot be executed.

When the Auth Manager command handler on the stack master receives a valid disable-port command, it verifies this information before returning a CoA-ACK message:

- the need for a port-disable
- the port-id (found in the local session context)

The switch attempts to disable the port.

If the port-disable operation is successful, the signal that triggered the port-disable is removed from the standby stack master.

If the stack master fails before the port-disable operation completes, the port is disabled after stack master change-over based on the original command (which is subsequently removed).

If the stack master fails before sending a CoA-ACK message, the new stack master treats the re-sent command as a new command.
Default RADIUS Configuration

RADIUS and AAA are disabled by default.
To prevent a lapse in security, you cannot configure RADIUS through a network management application.
When enabled, RADIUS can authenticate users accessing the switch through the CLI.

RADIUS Server Host

Switch-to-RADIUS-server communication involves several components:

- Hostname or IP address
- Authentication destination port
- Accounting destination port
- Key string
- Timeout period
- Retransmission value

You identify RADIUS security servers by their hostname or IP address, hostname and specific UDP port numbers, or their IP address and specific UDP port numbers. The combination of the IP address and the UDP port number creates a unique identifier, allowing different ports to be individually defined as RADIUS hosts providing a specific AAA service. This unique identifier enables RADIUS requests to be sent to multiple UDP ports on a server at the same IP address.

If two different host entries on the same RADIUS server are configured for the same service—for example, accounting—the second host entry configured acts as a fail-over backup to the first one. Using this example, if the first host entry fails to provide accounting services, the %RADIUS-4-RADIUS_DEAD message appears, and then the switch tries the second host entry configured on the same device for accounting services. (The RADIUS host entries are tried in the order that they are configured.)

A RADIUS server and the switch use a shared secret text string to encrypt passwords and exchange responses. To configure RADIUS to use the AAA security commands, you must specify the host running the RADIUS server daemon and a secret text (key) string that it shares with the switch.

The timeout, retransmission, and encryption key values can be configured globally for all RADIUS servers, on a per-server basis, or in some combination of global and per-server settings.

Related Topics

- Identifying the RADIUS Server Host, on page 15
- Defining AAA Server Groups, on page 18
- Configuring Settings for All RADIUS Servers, on page 23
- Configuring RADIUS Login Authentication, on page 16

RADIUS Login Authentication

To configure AAA authentication, you define a named list of authentication methods and then apply that list to various ports. The method list defines the types of authentication to be performed and the sequence in which
they are performed; it must be applied to a specific port before any of the defined authentication methods are performed. The only exception is the default method list. The default method list is automatically applied to all ports except those that have a named method list explicitly defined.

A method list describes the sequence and authentication methods to be queried to authenticate a user. You can designate one or more security protocols to be used for authentication, thus ensuring a backup system for authentication in case the initial method fails. The software uses the first method listed to authenticate users; if that method fails to respond, the software selects the next authentication method in the method list. This process continues until there is successful communication with a listed authentication method or until all defined methods are exhausted. If authentication fails at any point in this cycle—meaning that the security server or local username database responds by denying the user access—the authentication process stops, and no other authentication methods are attempted.

Related Topics
Configuring RADIUS Login Authentication, on page 16

AAA Server Groups

You can configure the switch to use AAA server groups to group existing server hosts for authentication. You select a subset of the configured server hosts and use them for a particular service. The server group is used with a global server-host list, which lists the IP addresses of the selected server hosts.

Server groups also can include multiple host entries for the same server if each entry has a unique identifier (the combination of the IP address and UDP port number), allowing different ports to be individually defined as RADIUS hosts providing a specific AAA service. If you configure two different host entries on the same RADIUS server for the same service, (for example, accounting), the second configured host entry acts as a fail-over backup to the first one.

Related Topics
Defining AAA Server Groups, on page 18

AAA Authorization

AAA authorization limits the services available to a user. When AAA authorization is enabled, the switch uses information retrieved from the user’s profile, which is in the local user database or on the security server, to configure the user’s session. The user is granted access to a requested service only if the information in the user profile allows it.

Related Topics
Configuring RADIUS Authorization for User Privileged Access and Network Services, on page 21

RADIUS Accounting

The AAA accounting feature tracks the services that users are using and the amount of network resources that they are consuming. When you enable AAA accounting, the switch reports user activity to the RADIUS security server in the form of accounting records. Each accounting record contains accounting attribute-value (AV) pairs and is stored on the security server. You can then analyze the data for network management, client billing, or auditing.
Vendor-Specific RADIUS Attributes

The Internet Engineering Task Force (IETF) draft standard specifies a method for communicating vendor-specific information between the switch and the RADIUS server by using the vendor-specific attribute (attribute 26). Vendor-specific attributes (VSAs) allow vendors to support their own extended attributes not suitable for general use. The Cisco RADIUS implementation supports one vendor-specific option by using the format recommended in the specification. Cisco's vendor-ID is 9, and the supported option has vendor-type 1, which is named cisco-avpair. The value is a string with this format:

```
protocol : attribute sep value *
```

Protocol is a value of the Cisco protocol attribute for a particular type of authorization. Attribute and value are an appropriate attribute-value (AV) pair defined in the Cisco TACACS+ specification, and sep is = for mandatory attributes and is * for optional attributes. The full set of features available for TACACS+ authorization can then be used for RADIUS.

Other vendors have their own unique vendor-IDs, options, and associated VSAs. For more information about vendor-IDs and VSAs, see RFC 2138, "Remote Authentication Dial-In User Service (RADIUS)."

For a complete list of RADIUS attributes or more information about vendor-specific attribute 26, see the "RADIUS Attributes" appendix in the Cisco IOS Security Configuration Guide.

Vendor-Proprietary RADIUS Server Communication

Although an IETF draft standard for RADIUS specifies a method for communicating vendor-proprietary information between the switch and the RADIUS server, some vendors have extended the RADIUS attribute set in a unique way. Cisco IOS software supports a subset of vendor-proprietary RADIUS attributes.

As mentioned earlier, to configure RADIUS (whether vendor-proprietary or IETF draft-compliant), you must specify the host running the RADIUS server daemon and the secret text string it shares with the switch. You specify the RADIUS host and secret text string by using the `radius-server` global configuration commands.

Related Topics

- Starting RADIUS Accounting, on page 22
- Configuring the Switch to Use Vendor-Specific RADIUS Attributes, on page 25
- Configuring the Switch for Vendor-Proprietary RADIUS Server Communication, on page 25
How to Configure RADIUS

Identifying the RADIUS Server Host

To apply these settings globally to all RADIUS servers communicating with the switch, use the three unique global configuration commands: `radius-server timeout`, `radius-server retransmit`, and `radius-server key`. To apply these values on a specific RADIUS server, use the `radius-server host` global configuration command.

You can configure the switch to use AAA server groups to group existing server hosts for authentication. For more information, see Related Topics below.

You also need to configure some settings on the RADIUS server. These settings include the IP address of the switch and the key string to be shared by both the server and the switch. For more information, see the RADIUS server documentation.

Before You Begin

If you configure both global and per-server functions (timeout, retransmission, and key commands) on the switch, the per-server timer, retransmission, and key value commands override global timer, retransmission, and key value commands. For information on configuring these settings on all RADIUS servers, see Related Topics below.

SUMMARY STEPS

1. configure terminal
2. radius-server host {hostname | ip-address} [auth-port port-number] [acct-port port-number] [timeout seconds] [retransmit retries] [key string]
3. end

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enters the global configuration mode.</td>
</tr>
</tbody>
</table>

Example:

Switch# configure terminal

Step 2 radius-server host {hostname | ip-address} [auth-port port-number] [acct-port port-number] [timeout seconds] [retransmit retries] [key string]

Specifies the IP address or hostname of the remote RADIUS server host.

- (Optional) For `auth-port port-number`, specify the UDP destination port for authentication requests.

- (Optional) For `acct-port port-number`, specify the UDP destination port for accounting requests.

- (Optional) For `timeout seconds`, specify the time interval that the switch waits for the RADIUS server to reply before resending. The range is 1 to 1000. This setting overrides the `radius-server timeout` global configuration command setting. If no
Before You Begin

To secure the switch for HTTP access by using AAA methods, you must configure the switch with the `ip http authentication aaa` global configuration command. Configuring AAA authentication does not secure the switch for HTTP access by using AAA methods.

For more information about the `ip http authentication` command, see the Cisco IOS Security Command Reference, Release 12.4.
## SUMMARY STEPS

1. configure terminal
2. aaa new-model
3. aaa authentication login \{default | list-name\} method1 [method2...]
4. line [console | tty | vty] line-number [ending-line-number]
5. login authentication \{default | list-name\}
6. end

## DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>aaa new-model</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# aaa new-model</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>aaa authentication login {default</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# aaa authentication login default local</td>
</tr>
<tr>
<td>- To create a default list that is used when a named list is <em>not</em> specified in the login authentication command, use the default keyword followed by the methods that are to be used in default situations. The default method list is automatically applied to all ports.</td>
<td></td>
</tr>
<tr>
<td>- For list-name, specify a character string to name the list you are creating.</td>
<td></td>
</tr>
<tr>
<td>- For method1..., specify the actual method the authentication algorithm tries. The additional methods of authentication are used only if the previous method returns an error, not if it fails.</td>
<td></td>
</tr>
<tr>
<td>Select one of these methods:</td>
<td></td>
</tr>
<tr>
<td>- <em>enable</em>—Use the enable password for authentication. Before you can use this authentication method, you must define an enable password by using the enable password global configuration command.</td>
<td></td>
</tr>
<tr>
<td>- <em>group radius</em>—Use RADIUS authentication. Before you can use this authentication method, you must configure the RADIUS server.</td>
<td></td>
</tr>
<tr>
<td>- <em>line</em>—Use the line password for authentication. Before you can use this authentication method, you must define a line password. Use the password password line configuration command.</td>
<td></td>
</tr>
</tbody>
</table>
### Defining AAA Server Groups

You use the `server` group server configuration command to associate a particular server with a defined group server. You can either identify the server by its IP address or identify multiple host instances or entries by using the optional `auth-port` and `acct-port` keywords.

Beginning in privileged EXEC mode, follow these steps to define AAA server groups:
SUMMARY STEPS

1. configure terminal
2. radius-server host {hostname | ip-address} [auth-port port-number] [acct-port port-number] [timeout seconds] [retransmit retries] [key string]
3. aaa new-model
4. aaa group server radius group-name
5. server ip-address
6. end

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enters the global configuration mode.</td>
</tr>
<tr>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 2 radius-server host {hostname</td>
<td>ip-address} [auth-port port-number] [acct-port port-number] [timeout seconds] [retransmit retries] [key string]</td>
</tr>
<tr>
<td>Example: Switch(config)# radius-server host 172.29.36.49 auth-port 1612 acct-port 1613 timeout 10 retransmit 10 key rad1</td>
<td></td>
</tr>
</tbody>
</table>

- (Optional) For auth-port port-number, specify the UDP destination port for authentication requests.
- (Optional) For acct-port port-number, specify the UDP destination port for accounting requests.
- (Optional) For timeout seconds, specify the time interval that the switch waits for the RADIUS server to reply before resending. The range is 1 to 1000. This setting overrides the radius-server timeout global configuration command setting. If no timeout is set with the radius-server host command, the setting of the radius-server timeout command is used.
- (Optional) For retransmit retries, specify the number of times a RADIUS request is resent to a server if that server is not responding or responding slowly. The range is 1 to 1000. If no retransmit value is set with the radius-server host command, the setting of the radius-server retransmit global configuration command is used.
- (Optional) For key string, specify the authentication and encryption key used between the switch and the RADIUS daemon running on the RADIUS server.

**Note** The key is a text string that must match the encryption key used on the RADIUS server. Always configure the key as the last item in the radius-server host command. Leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks are part of the key.
### Configuring RADIUS

#### Defining AAA Server Groups

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>To configure the switch to recognize more than one host entry associated with a single IP address, enter this command as many times as necessary, making sure that each UDP port number is different. The switch software searches for hosts in the order in which you specify them. Set the timeout, retransmit, and encryption key values to use with the specific RADIUS host.</td>
<td></td>
</tr>
</tbody>
</table>

**Step 3**

<table>
<thead>
<tr>
<th>aaa new-model</th>
</tr>
</thead>
</table>

**Example:**

```bash
Switch(config)# aaa new-model
```

Enables AAA.

**Step 4**

<table>
<thead>
<tr>
<th>aaa group server radius group-name</th>
</tr>
</thead>
</table>

**Example:**

```bash
Switch(config)# aaa group server radius group1
```

Defines the AAA server-group with a group name. This command puts the switch in a server group configuration mode.

**Step 5**

<table>
<thead>
<tr>
<th>server ip-address</th>
</tr>
</thead>
</table>

**Example:**

```bash
Switch(config-sg-radius)# server 172.20.0.1 auth-port 1000 acct-port 1001
```

Associates a particular RADIUS server with the defined server group. Repeat this step for each RADIUS server in the AAA server group. Each server in the group must be previously defined in Step 2.

**Step 6**

<table>
<thead>
<tr>
<th>end</th>
</tr>
</thead>
</table>

**Example:**

```bash
Switch(config)# end
```

Returns to privileged EXEC mode.

### Using Two Different RADIUS Group Servers

In this example, the switch is configured to recognize two different RADIUS group servers (group1 and group2). Group1 has two different host entries on the same RADIUS server configured for the same services. The second host entry acts as a fail-over backup to the first entry.

```bash
Switch(config)# radius-server host 172.20.0.1 auth-port 1000 acct-port 1001
Switch(config)# radius-server host 172.10.0.1 auth-port 1000 acct-port 1001
Switch(config)# aaa new-model
Switch(config)# aaa group server radius group1
Switch(config-sg-radius)# server 172.20.0.1 auth-port 1000 acct-port 1001
Switch(config-sg-radius)# exit
Switch(config)# aaa group server radius group2
Switch(config-sg-radius)# server 172.20.0.1 auth-port 2000 acct-port 2001
Switch(config-sg-radius)# exit
```
Related Topics
- Identifying the RADIUS Server Host, on page 15
- RADIUS Server Host, on page 12
- AAA Server Groups, on page 13

Configuring RADIUS Authorization for User Privileged Access and Network Services

Note
Authorization is bypassed for authenticated users who log in through the CLI even if authorization has been configured.

Beginning in privileged EXEC mode, follow these steps to configure RADIUS authorization for user privileged access and network services:

SUMMARY STEPS

1. configure terminal
2. aaa authorization network radius
3. aaa authorization exec radius
4. end

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters the global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>aaa authorization network radius</td>
<td>Configures the switch for user RADIUS authorization for all network-related service requests.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# aaa authorization network radius</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>aaa authorization exec radius</td>
<td>Configures the switch for user RADIUS authorization if the user has privileged EXEC access.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Switch(config)# aaa authorization exec radius</td>
<td></td>
</tr>
<tr>
<td>The exec keyword might return user profile information (such as autocmd information).</td>
<td></td>
</tr>
</tbody>
</table>
### What to Do Next

You can use the `aaa authorization` global configuration command with the `radius` keyword to set parameters that restrict a user’s network access to privileged EXEC mode.

The `aaa authorization exec radius local` command sets these authorization parameters:

- Use RADIUS for privileged EXEC access authorization if authentication was performed by using RADIUS.
- Use the local database if authentication was not performed by using RADIUS.

### Related Topics

- AAA Authorization, on page 13

### Starting RADIUS Accounting

Beginning in privileged EXEC mode, follow these steps to start RADIUS accounting:

#### SUMMARY STEPS

1. `configure terminal`
2. `aaa accounting network start-stop radius`
3. `aaa accounting exec start-stop radius`
4. `end`

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code></td>
<td>Enters the global configuration mode.</td>
</tr>
</tbody>
</table>

Example:

```
Switch# configure terminal
```

---

### Configuring RADIUS

### Starting RADIUS Accounting
### Configuring Settings for All RADIUS Servers

Beginning in privileged EXEC mode, follow these steps to configure settings for all RADIUS servers:

**SUMMARY STEPS**

1. `configure terminal`
2. `radius-server key string`
3. `radius-server retransmit retries`
4. `radius-server timeout seconds`
5. `radius-server deadline minutes`
6. `end`

#### What to Do Next

To establishing a session with a router if the AAA server is unreachable, use the `aaa accounting system guarantee-first` command. This command guarantees system accounting as the first record, which is the default condition. In some situations, users might be prevented from starting a session on the console or terminal connection until after the system reloads, which can take more than 3 minutes. To establish a console or Telnet session with the router if the AAA server is unreachable when the router reloads, use the `no aaa accounting system guarantee-first` command.

**Related Topics**

- [RADIUS Accounting](#) on page 13
## DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters the global configuration mode.</td>
</tr>
<tr>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> radius-server key string</td>
<td>Specifies the shared secret text string used between the switch and all RADIUS servers.</td>
</tr>
<tr>
<td>Example: Switch(config)# radius-server key your_server_key</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> radius-server retransmit retries</td>
<td>Specifies the number of times the switch sends each RADIUS request to the server before giving up. The default is 3; the range 1 to 1000.</td>
</tr>
<tr>
<td>Example: Switch(config)# radius-server retransmit 5</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> radius-server timeout seconds</td>
<td>Specifies the number of seconds a switch waits for a reply to a RADIUS request before resending the request. The default is 5 seconds; the range is 1 to 1000.</td>
</tr>
<tr>
<td>Example: Switch(config)# radius-server timeout 3</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> radius-server deadtime minutes</td>
<td>When a RADIUS server is not responding to authentication requests, this command specifies a time to stop the request on that server. This avoids the wait for the request to timeout before trying the next configured server. The default is 0; the range is 1 to 1440 minutes.</td>
</tr>
<tr>
<td>Example: Switch(config)# radius-server deadtime 0</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Switch(config)# end</td>
<td></td>
</tr>
</tbody>
</table>

### Related Topics
- [Identifying the RADIUS Server Host](#), on page 15
- [RADIUS Server Host](#), on page 12
### Configuring the Switch to Use Vendor-Specific RADIUS Attributes

Beginning in privileged EXEC mode, follow these steps to configure the switch to use vendor-specific RADIUS attributes:

#### SUMMARY STEPS

1. configure terminal
2. radius-server vsa send [accounting | authentication]
3. end

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters the global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch# configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enables the switch to recognize and use VSAs as defined by RADIUS IETF attribute 26.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config)# radius-server vsa send [accounting</td>
</tr>
<tr>
<td></td>
<td>• (Optional) Use the <strong>accounting</strong> keyword to limit the set of recognized vendor-specific attributes to only accounting attributes.</td>
</tr>
<tr>
<td></td>
<td>• (Optional) Use the <strong>authentication</strong> keyword to limit the set of recognized vendor-specific attributes to only authentication attributes.</td>
</tr>
<tr>
<td></td>
<td>If you enter this command without keywords, both accounting and authentication vendor-specific attributes are used.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Switch(config)# end</td>
</tr>
</tbody>
</table>

**Related Topics**

- Vendor-Specific RADIUS Attributes, on page 14

### Configuring the Switch for Vendor-Proprietary RADIUS Server Communication

Beginning in privileged EXEC mode, follow these steps to configure the switch to use vendor-proprietary RADIUS server communication:
SUMMARY STEPS

1. configure terminal
2. radius-server host \{hostname | ip-address\} non-standard
3. radius-server key string
4. end

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch# configure terminal</td>
</tr>
<tr>
<td></td>
<td>Enters the global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>radius-server host {hostname</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# radius-server host 172.20.30.15 nonstandard</td>
</tr>
<tr>
<td></td>
<td>Specifies the IP address or hostname of the remote RADIUS server host and identifies that it is using a vendor-proprietary implementation of RADIUS.</td>
</tr>
<tr>
<td>Step 3</td>
<td>radius-server key string</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# radius-server key radi124</td>
</tr>
<tr>
<td></td>
<td>Specifies the shared secret text string used between the switch and the vendor-proprietary RADIUS server. The switch and the RADIUS server use this text string to encrypt passwords and exchange responses.</td>
</tr>
<tr>
<td>Note</td>
<td>The key is a text string that must match the encryption key used on the RADIUS server. Leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks are part of the key.</td>
</tr>
<tr>
<td>Step 4</td>
<td>end</td>
</tr>
<tr>
<td>Example:</td>
<td>Switch(config)# end</td>
</tr>
<tr>
<td></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
</tbody>
</table>

What to Do Next

This feature allows access and authentication requests to be evenly across all RADIUS servers in a server group. For more information, see the "RADIUS Server Load Balancing" chapter of the Cisco IOS Security Configuration Guide, Release 12.4.

Related Topics

Vendor-Proprietary RADIUS Server Communication, on page 14
Configuring CoA on the Switch

Beginning in privileged EXEC mode, follow these steps to configure CoA on a switch. This procedure is required.

SUMMARY STEPS

1. configure terminal
2. aaa new-model
3. aaa server radius dynamic-author
4. client {ip-address | name} [vrf vrfname] [server-key string]
5. server-key [0 | 7] string
6. port port-number
7. auth-type {any | all | session-key}
8. ignore session-key
9. ignore server-key
10. authentication command bounce-port ignore
11. authentication command disable-port ignore
12. end

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters the global configuration mode.</td>
</tr>
<tr>
<td>Example: Switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> aaa new-model</td>
<td>Enables AAA.</td>
</tr>
<tr>
<td>Example: Switch(config)# aaa new-model</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> aaa server radius dynamic-author</td>
<td>Configures the switch as an authentication, authorization, and accounting (AAA) server to facilitate interaction with an external policy server.</td>
</tr>
<tr>
<td>Example: Switch(config)# aaa server radius dynamic-author</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> client {ip-address</td>
<td>name} [vrf vrfname] [server-key string]</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Configures the RADIUS key to be shared between a device and RADIUS clients.</td>
</tr>
<tr>
<td>server-key [0</td>
<td>7] string</td>
</tr>
<tr>
<td></td>
<td>Switch(config-sg-radius)# server-key your_server_key</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Specifies the port on which a device listens for RADIUS requests from configured RADIUS clients.</td>
</tr>
<tr>
<td>port port-number</td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Switch(config-sg-radius)# port 25</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>Specifies the type of authorization the switch uses for RADIUS clients.</td>
</tr>
<tr>
<td>auth-type {any</td>
<td>all</td>
</tr>
<tr>
<td></td>
<td>Switch(config-sg-radius)# auth-type any</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>(Optional) Configures the switch to ignore the session-key. For more information about the <code>ignore</code> command, see the Cisco IOS Intelligent Services Gateway Command Reference on Cisco.com.</td>
</tr>
<tr>
<td>ignore session-key</td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td>(Optional) Configures the switch to ignore the server-key. For more information about the <code>ignore</code> command, see the Cisco IOS Intelligent Services Gateway Command Reference on Cisco.com.</td>
</tr>
<tr>
<td>ignore server-key</td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Switch(config-sg-radius)# ignore server-key</td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td>(Optional) Configures the switch to ignore a CoA request to temporarily disable the port hosting a session. The purpose of temporarily disabling the port is to trigger a DHCP renegotiation from the host when a VLAN change occurs and there is no supplicant on the endpoint to detect the change.</td>
</tr>
<tr>
<td>authentication command bounce-port ignore</td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Switch(config-sg-radius)# authentication command bounce-port ignore</td>
</tr>
<tr>
<td><strong>Step 11</strong></td>
<td>(Optional) Configures the switch to ignore a nonstandard command requesting that the port hosting a session be administratively shut down. Shutting down the port results in termination of the session. Use standard CLI or SNMP commands to re-enable the port.</td>
</tr>
<tr>
<td>authentication command disable-port ignore</td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Switch(config-sg-radius)# authentication command disable-port ignore</td>
</tr>
<tr>
<td><strong>Step 12</strong></td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>end</td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Switch(config-sg-radius)# end</td>
</tr>
</tbody>
</table>
Monitoring CoA Functionality

Table 4: Privileged EXEC show Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show aaa attributes protocol radius</td>
<td>Displays AAA attributes of RADIUS commands.</td>
</tr>
</tbody>
</table>

Table 5: Global Troubleshooting Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug radius</td>
<td>Displays information for troubleshooting RADIUS.</td>
</tr>
<tr>
<td>debug aaa coa</td>
<td>Displays information for troubleshooting CoA</td>
</tr>
<tr>
<td>processing.</td>
<td></td>
</tr>
<tr>
<td>debug aaa pod</td>
<td>Displays information for troubleshooting POD</td>
</tr>
<tr>
<td>packets.</td>
<td></td>
</tr>
<tr>
<td>debug aaa subsys</td>
<td>Displays information for troubleshooting POD</td>
</tr>
<tr>
<td>packets.</td>
<td></td>
</tr>
<tr>
<td>debug cmdhd [detail</td>
<td>Displays information for troubleshooting command</td>
</tr>
<tr>
<td>error</td>
<td>events]</td>
</tr>
</tbody>
</table>

For detailed information about the fields in these displays, see the command reference for this release.

Configuration Examples for Controlling Switch Access with RADIUS

Examples: Identifying the RADIUS Server Host

This example shows how to configure one RADIUS server to be used for authentication and another to be used for accounting:

Switch(config)# radius-server host 172.29.36.49 auth-port 1612 key rad1
Switch(config)# radius-server host 172.20.36.50 acct-port 1618 key rad2
This example shows how to configure host1 as the RADIUS server and to use the default ports for both authentication and accounting:

```plaintext
Switch(config)# radius-server host host1
```

### Examples: Configuring the Switch to Use Vendor-Specific RADIUS Attributes

For example, this AV pair activates Cisco’s multiple named ip address pools feature during IP authorization (during PPP IPCP address assignment):

```plaintext
cisco-avpair= "ip:addr-pool=first"
```

This example shows how to provide a user logging in from a switch with immediate access to privileged EXEC commands:

```plaintext
cisco-avpair= "shell:priv-lvl=15"
```

This example shows how to specify an authorized VLAN in the RADIUS server database:

```plaintext
cisco-avpair= "tunnel-type(#64)=VLAN(13)"
cisco-avpair= "tunnel-medium-type(#65)=802 media(6)"
cisco-avpair= "tunnel-private-group-id(#81)=vlanid"
```

This example shows how to apply an input ACL in ASCII format to an interface for the duration of this connection:

```plaintext
cisco-avpair= "ip:inacl#1=deny ip 10.10.10.10 0.0.255.255 20.20.20.20 255.255.0.0"
cisco-avpair= "ip:inacl#2=deny ip 10.10.10.10 0.0.255.255 any"
cisco-avpair= "mac:inacl#3=deny any any decnet-iv"
```

This example shows how to apply an output ACL in ASCII format to an interface for the duration of this connection:

```plaintext
cisco-avpair= "ip:outacl#2=deny ip 10.10.10.10 0.0.255.255 any"
```

### Example: Configuring the Switch for Vendor-Proprietary RADIUS Server Communication

This example shows how to specify a vendor-proprietary RADIUS host and to use a secret key of rad124 between the switch and the server:

```plaintext
Switch(config)# radius-server host 172.20.30.15 nonstandard
Switch(config)# radius-server key rad124
```