CHAPTER 1

Configuring RADIUS

This chapter describes how to configure Remote Access Dial-In User Service (RADIUS) protocol on the Nexus 5000 Series switch.

This chapter includes the following sections:

Information About RADIUS

The RADIUS distributed client/server system allows you to secure networks against unauthorized access. In the Cisco implementation, RADIUS clients run on the Nexus 5000 Series of switches and send authentication and accounting requests to a central RADIUS server that contains all user authentication and network service access information.

This section includes the following topics:

RADIUS Network Environments

RADIUS can be implemented in a variety of network environments that require high levels of security while maintaining network access for remote users.

You can use RADIUS in the following network environments that require access security:

- Networks with multiple-vendor network devices, each supporting RADIUS.

  For example, network devices from several vendors can use a single RADIUS server-based security database.

- Networks already using RADIUS.

  You can add a Nexus 5000 Series switch with RADIUS to the network. This action might be the first step when you make a transition to a AAA server.

- Networks that require resource accounting.

  You can use RADIUS accounting independent of RADIUS authentication or authorization. The RADIUS accounting functions allow data to be sent at the start and end of services, indicating the amount of resources (such as time, packets, bytes, and so on) used during the session. An Internet service provider (ISP) might use a freeware-based version of the RADIUS access control and accounting software to meet special security and billing needs.

- Networks that support authentication profiles.

  Using the RADIUS server in your network, you can configure AAA authentication and set up per-user profiles. Per-user profiles enable the Nexus 5000 Series switch to better manage ports using their existing RADIUS solutions and to efficiently manage shared resources to offer different service-level agreements.

RADIUS Operation

When a user attempts to log in and authenticate to a Nexus 5000 Series switch using RADIUS, the following process occurs:

1. The user is prompted for and enters 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 not authenticated and is prompted to reenter the username and password, or access is denied.
   - CHALLENGE—A challenge is issued by the RADIUS server. The challenge collects additional data from the user.
   - CHANGE PASSWORD—A request is issued by the RADIUS server, asking the user to select a new password.

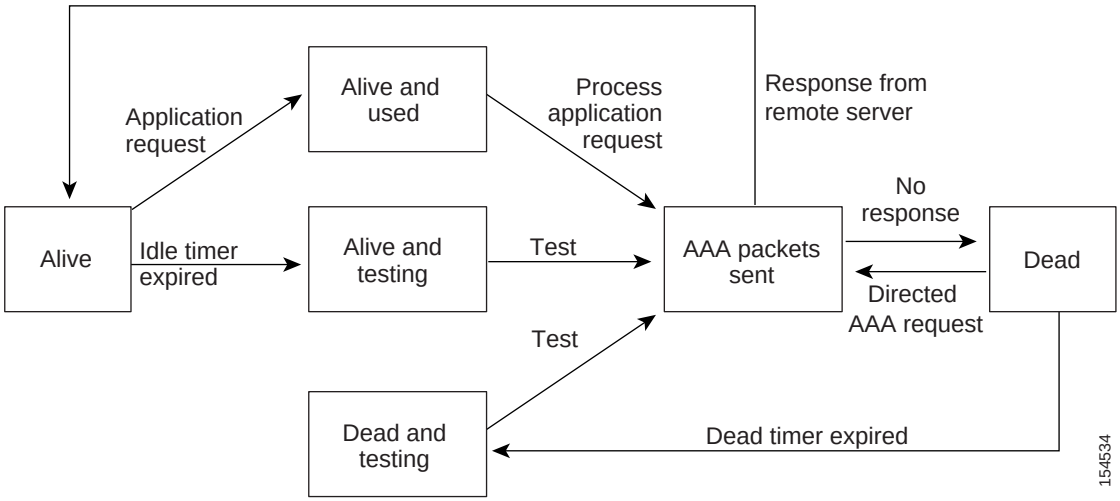
The ACCEPT or REJECT response is bundled with additional data that is used for EXEC or network authorization. You must first complete RADIUS authentication before using RADIUS authorization. The additional data included with the ACCEPT or REJECT packets consists of the following:

- Services that the user can access, including Telnet, rlogin, or local-area transport (LAT) connections, and Point-to-Point Protocol (PPP), Serial Line Internet Protocol (SLIP), or EXEC services.
- Connection parameters, including the host or client IPv4 or IPv6 address, access list, and user timeouts.

RADIUS Server Monitoring

An unresponsive RADIUS server can cause delay in processing of AAA requests. You can configure the Nexus 5000 Series switch to periodically monitor a RADIUS server to check whether it is responding (or alive) to save time in processing AAA requests. The Nexus 5000 Series switch marks unresponsive RADIUS servers as dead and does not send AAA requests to any dead RADIUS servers. The switch periodically monitors the dead RADIUS servers and brings them to the alive state once they respond. This monitoring process verifies that a RADIUS server is in a working state before real AAA requests are sent its way. Whenever a RADIUS server changes to the dead or alive state, a Simple Network Management Protocol (SNMP) trap is generated and the Nexus 5000 Series switch displays an error message that a failure is taking place. See Figure 1-1.

Figure 1-1 RADIUS Server States



Note The monitoring interval for alive servers and dead servers are different and can be configured by the user. The RADIUS server monitoring is performed by sending a test authentication request to the RADIUS server.

Vendor-Specific Attributes

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

```
protocol : attribute separator value *
```

The protocol is a Cisco attribute for a particular type of authorization, the separator is an equal sign (=) for mandatory attributes, and an asterisk (*) indicates optional attributes.

When you use RADIUS servers for authentication on a Nexus 5000 Series switch, the RADIUS protocol directs the RADIUS server to return user attributes, such as authorization information, along with authentication results. This authorization information is specified through VSAs.

The following VSA protocol options are supported by the Nexus 5000 Series switch:

- Shell— Used in access-accept packets to provide user profile information.
- Accounting— Used in accounting-request packets. If a value contains any white spaces, you should enclose the value within double quotation marks.

The Nexus 5000 Series switch supports the following attributes:

- roles—Lists all the roles to which the user belongs. The value field is a string that lists the role names delimited by white space.
- accountinginfo—Stores accounting information in addition to the attributes covered by a standard RADIUS accounting protocol. This attribute is sent only in the VSA portion of the Account-Request frames from the RADIUS client on the switch. It can be used only with the accounting protocol data units (PDUs).

Prerequisites for RADIUS

RADIUS has the following prerequisites:

- Obtain IPv4 or IPv6 addresses or host names for the RADIUS servers.
- Obtain preshared keys from the RADIUS servers.
- Ensure that the Nexus 5000 Series switch is configured as a RADIUS client of the AAA servers.

Guidelines and Limitations

RADIUS has the following guidelines and limitations:

- You can configure a maximum of 64 RADIUS servers on the Nexus 5000 Series switch.

Configuring RADIUS Servers

To configure RADIUS servers, perform this task:

Step 1 Establish the RADIUS server connections to the Nexus 5000 Series switch.

See the "Configuring RADIUS Server Hosts" section on page 1-5.

Step 2 Configure the preshared secret keys for the RADIUS servers.

See the "Configuring Global Preshared Keys" section on page 1-6.

Step 3 If needed, configure RADIUS server groups with subsets of the RADIUS servers for AAA authentication methods.

See the "Allowing Users to Specify a RADIUS Server at Login" section on page 1-9 and the "Configuring AAA" section on page 1-6.

Step 4 If needed, configure any of the following optional parameters:

- Dead-time interval

  See the "The following example shows how to configure periodic RADIUS server monitoring:" section on page 1-13.

- Allow specification of a RADIUS server at login

  See the "Allowing Users to Specify a RADIUS Server at Login" section on page 1-9).

- Transmission retry count and timeout interval

  See the "Configuring the Global RADIUS Transmission Retry Count and Timeout Interval" section on page 1-9.

- Accounting and authentication attributes

  See the "Configuring Accounting and Authentication Attributes for RADIUS Servers" section on page 1-11.

Step 5 If needed, configure periodic RADIUS server monitoring.
See the "Configuring Periodic RADIUS Server Monitoring" section on page 1-12.

The following topics describe the RADIUS configuration procedure in more details:

Note If you are familiar with the Cisco IOS CLI, be aware that the Cisco NX-OS commands for this feature might differ from the Cisco IOS commands that you would use.

Configuring RADIUS Server Hosts

You must configure the IPv4 or IPv6 address or the host name for each RADIUS server that you want to use for authentication. All RADIUS server hosts are added to the default RADIUS server group. You can configure up to 64 RADIUS servers.

To configure a RADIUS server host, perform this task:

	Command	Purpose
Step 1	`switch# configure terminal`	Enters configuration mode.
Step 2	`switch(config) #radius-server host {ipv4-address | ipv6-address | host-name}`	Specifies the IPv4 or IPv6 address or hostname for a RADIUS server.
Step 3	`switch(config)# exit`	Exits configuration mode.
Step 4	`switch# show radius-server`	(Optional) Displays the RADIUS server configuration.
Step 5	`switch# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

The following example shows how to configure a RADIUS server host:

```
switch# configure terminal
switch(config)# radius-server host 10.10.1.1
switch(config)# exit
switch# show radius-server
switch# copy running-config startup-config
```

Configuring Global Preshared Keys

You can configure preshared keys at the global level for all servers used by the Nexus 5000 Series switch. A preshared key is a shared secret text string between the Nexus 5000 Series switch and the RADIUS server hosts.

To configure global preshared keys, obtain the preshared key values for the remote RADIUS servers and perform this task:

:

	Command	Purpose
Step 1	`switch# configure terminal`	Enters configuration mode.
Step 2	`switch(config)# radius-server key [0 | 7] key-value`	Specifies a preshared key for all RADIUS servers. You can specify a clear text (**0**) or encrypted (**7**) preshared key. The default format is clear text. The maximum length is 63 characters. By default, no preshared key is configured.
Step 3	`switch(config)# exit`	Exits configuration mode.

	Command	Purpose
Step 4	`switch# show radius-server`	(Optional) Displays the RADIUS server configuration. **Note** The preshared keys are saved in encrypted form in the running configuration. Use the **show running-config** command to display the encrypted preshared keys.
Step 5	`switch# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

The following example shows how to obtain the preshared key values for a remote RADIUS server:

```
switch# configure terminal
switch(config)# radius-server key 0 QsEfThUkO
switch(config)# exit
switch# show radius-server
switch# copy running-config startup-config
```

Configuring RADIUS Server Preshared Keys

You can configure preshared keys for a RADIUS server. A preshared key is a shared secret text string between the Nexus 5000 Series switch and the RADIUS server host.

To configure radius server preshared keys, obtain the preshared key values for the remote RADIUS servers and perform this task:

:

	Command	Purpose
Step 1	`switch# configure terminal`	Enters configuration mode.
Step 2	`switch(config)# radius-server host {`*ipv4-address* `|` *ipv6-address* `|` *host-name*`} key [0	7]` *key-value*	Specifies a preshared key for a specific RADIUS server. You can specify a clear text (**0**) or encrypted (**7**) preshared key. The default format is clear text. The maximum length is 63 characters. This preshared key is used instead of the global preshared key.
Step 3	`switch(config)# exit`	Exits configuration mode.
Step 4	`switch# show radius-server`	(Optional) Displays the RADIUS server configuration. **Note** The preshared keys are saved in encrypted form in the running configuration. Use the **show running-config** command to display the encrypted preshared keys.
Step 5	`switch# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

The following example shows how to configure a preshared keys for a RADIUS server:

```
switch# configure terminal
switch(config)# radius-server host 10.10.1.1 key 0 PlIjUhYg
switch(config)# exit
switch# show radius-server
switch# copy running-config startup-config
```

Configuring RADIUS Server Groups

You can specify one or more remote AAA servers for authentication using server groups. All members of a group must belong to the RADIUS protocol. The servers are tried in the same order in which you configure them.

You can configure these server groups at any time but they only take effect when you apply them to an AAA service. For information on AAA services, see the "Remote AAA Services" section on page 1-3.

To configure radius server groups, perform this task:

:

	Command	Purpose
Step 1	`switch# configure terminal`	Enters configuration mode.
Step 2	`switch(config)# aaa group server radius` *group-name*	Creates a RADIUS server group and enters the RADIUS server group configuration submode for that group. The *group-name* argument is a case-sensitive alphanumeric string with a maximum length of 127 characters.
Step 3	`switch(config-radius)# server` {*ipv4-address* |*ipv6-address* | *server-name*}	Configures the RADIUS server as a member of the RADIUS server group. **Tip** If the specified RADIUS server is not found, configure it using the **radius-server host** command and retry this command.
Step 4	`switch(config-radius)# deadtime` *minutes*	(Optional) Configures the monitoring dead time. The default is 0 minutes. The range is from 1 through 1440. **Note** If the dead-time interval for a RADIUS server group is greater than zero (0), that value takes precedence over the global dead-time value. See the example that shows how to configure periodic RADIUS server monitoring.
Step 5	`switch(config-radius)# exit`	Exits configuration mode.
Step 6	`switch(config) #show radius-server group [GROUP-NAME]`	(Optional) Displays the RADIUS server group configuration.
Step 7	`switch(config)# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

The following example shows how to configure a RADIUS server group:

```
switch# configure terminal
```

```
switch(config)# aaa group server radius RadServer
switch(config-radius)# server 10.10.1.1
switch(config-radius)# deadtime 30
switch(config-radius)# use-vrf management
switch(config-radius)# exit
switch(config)# show radius-server group
switch(config)# copy running-config startup-config
```

Allowing Users to Specify a RADIUS Server at Login

Note By default, the Nexus 5000 Series switch forwards an authentication request based on the default AAA authentication method. You can configure the Nexus 5000 Series switch to allow the user to specify a VRF and RADIUS server to send the authenticate request by enabling the directed-request option. If you enable this option, the user can log in as *username@hostname,* where *hostname* is the name of a configured RADIUS server. User specified logins are only supported for Telnet sessions.

To allow users to specify a RADIUS server at login, perform this task:

	Command	Purpose
Step 1	`switch# configure terminal`	Enters configuration mode.
Step 2	`switch(config)# switch(config)# radius-server directed-request`	Allows users to specify a RADIUS server to send the authentication request when logging in. The default is disabled.
Step 3	`switch(config)# exit`	Exits configuration mode.
Step 4	`switch# show radius-server directed-request`	(Optional) Displays the directed request configuration.
Step 5	`switch# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

Configuring the Global RADIUS Transmission Retry Count and Timeout Interval

You can configure a global retransmission retry count and timeout interval for all RADIUS servers. By default, a switch retries transmission to a RADIUS server only once before reverting to local authentication. You can increase this number up to a maximum of five retries per server. The timeout interval determines how long the Nexus 5000 Series switch waits for responses from RADIUS servers before declaring a timeout failure.

To configure the global RADIUS transmission retry count and timeout interval, perform this task:

:

	Command	Purpose
Step 1	`switch# configure terminal`	Enters configuration mode.
Step 2	`switch(config)# radius-server retransmit` *count*	Specifies the retransmission count for all RADIUS servers. The default retransmission count is 1 and the range is from 0 to 5.
Step 3	`switch(config)# radius-server timeout` *seconds*	Specifies the transmission timeout interval for RADIUS servers. The default timeout interval is 5 seconds and the range is from 1 to 60 seconds.
Step 4	`switch(config)# exit`	Exits configuration mode.
Step 5	`switch# show radius-server`	(Optional) Displays the RADIUS server configuration.
Step 6	`switch# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

Configuring the RADIUS Transmission Retry Count and Timeout Interval for a Server

By default, a Nexus 5000 Series switch retries transmission to a RADIUS server only once before reverting to local authentication. You can increase this number up to a maximum of five retries per server. You can also set a timeout interval that the Nexus 5000 Series switch waits for responses from RADIUS servers before declaring a timeout failure.

To configure RADIUS transmission retry count and timeout interval for a server, perform this task:

	Command	Purpose
Step 1	`switch# configure terminal`	Enters configuration mode.
Step 2	`#switch(config)# radius-server host` {*ipv4-address* |*ipv6-address* | *host-name*} `retransmit` *count*	Specifies the retransmission count for a specific server. The default is the global value. **Note** The retransmission count value specified for a RADIUS server overrides the count specified for all RADIUS servers in Step 2.
Step 3	`switch(config)# switch(config)# radius-server host` {*ipv4-address* |*ipv6-address* | *host-name*} `timeout` *seconds*	Specifies the transmission timeout interval for a specific server. The default is the global value. **Note** The timeout interval value specified for a RADIUS server overrides the interval value specified for all RADIUS servers in Step 3.
Step 4	`switch(config)# exit`	Exits configuration mode.

	Command	Purpose
Step 5	`switch# show radius-server`	(Optional) Displays the RADIUS server configuration.
Step 6	`switch# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

The following example shows how to configure RADIUS transmission retry count and timeout interval for a server:

```
switch# configure terminal
switch(config)# radius-server host server1 retransmit 3
switch(config)# radius-server host server1 timeout 10
switch(config)# exit
switch# show radius-server
switch# copy running-config startup-config
```

Configuring Accounting and Authentication Attributes for RADIUS Servers

You can specify that a RADIUS server is to be used only for accounting purposes or only for authentication purposes. By default, RADIUS servers are used for both accounting and authentication. You can also specify the destination UDP port numbers where RADIUS accounting and authentication messages should be sent.

To configure the accounting and authentication attributes for RADIUS servers, perform this task:

	Command	Purpose
Step 1	`switch# configure terminal`	Enters configuration mode.
Step 2	`switch(config) #radius-server host {ipv4-address | ipv6-address | host-name} acct-port udp-port`	(Optional) Specifies a UDP port to use for RADIUS accounting messages.The default UDP port is 1812. The range is from 0 to 65535.
Step 3	`switch(config)# radius-server host {ipv4-address | ipv6-address | host-name} accounting`	(Optional) Specifies that the specified RADIUS server it to be used only for accounting purposes. The default is both accounting and authentication.
Step 4	`switch(config)# radius-server host {ipv4-address | ipv6-address | host-name} auth-port udp-port`	(Optional) Specifies a UDP port to use for RADIUS authentication messages. The default UDP port is 1812. The range is from 0 to 65535.
Step 5	`switch(config)# radius-server host {ipv4-address | ipv6-address | host-name} authentication`	(Optional) Specifies that the specified RADIUS server only be used for authentication purposes. The default is both accounting and authentication.
Step 6	`switch(config)# exit`	Exits configuration mode.
Step 7	`switch(config)# show radius-server`	(Optional) Displays the RADIUS server configuration.
Step 8	`switch# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

The following example shows how to configure the accounting and authentication attributes for a RADIUS server:

```
switch# configure terminal
switch(config)# radius-server host 10.10.1.1 acct-port 2004
switch(config)# radius-server host 10.10.1.1 accounting
switch(config)# radius-server host 10.10.2.2 auth-port 2005
switch(config)# radius-server host 10.10.2.2 authentication
switch(config)# exit
switch(config)# show radius-server
switch# copy running-config startup-config
```

Configuring Periodic RADIUS Server Monitoring

You can monitor the availability of RADIUS servers. These parameters include the username and password to use for the server and an idle timer. The idle timer specifies the interval during which a RADIUS server receives no requests before the Nexus 5000 Series switch sends out a test packet. You can configure this option to test servers periodically.

Note For security reasons, we recommend that you do not configure a test username that is the same as an existing user in the RADIUS database.

The test idle timer specifies the interval during which a RADIUS server receives no requests before the Nexus 5000 Series switch sends out a test packet.

Note The default idle timer value is 0 minutes. When the idle time interval is 0 minutes, the Nexus 5000 Series switch does not perform periodic RADIUS server monitoring.

To configure periodic RADIUS server monitoring, perform this task:

	Command	Purpose
Step 1	`switch# configure terminal`	Enters configuration mode.
Step 2	`switch(config)# radius-server host {ipv4-address | ipv6-address | host-name} test {idle-time minutes | password password [idle-time minutes] | username name [password password [idle-time minutes]]}`	Specifies parameters for server monitoring. The default username is test and the default password is test. The default value for the idle timer is 0 minutes. The valid range is 0 to 1440 minutes. **Note** For periodic RADIUS server monitoring, you must set the idle timer to a value greater than 0.
Step 3	`switch(config)# radius-server deadtime minutes`	Specifies the number of minutes before the Nexus 5000 Series switch checks a RADIUS server that was previously unresponsive. The default value is 0 minutes. The valid range is 1 to 1440 minutes.
Step 4	`switch(config)# exit`	Exits configuration mode.
Step 5	`switch# show radius-server`	(Optional) Displays the RADIUS server configuration.
Step 6	`switch# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

The following example shows how to configure periodic RADIUS server monitoring:

```
switch# configure terminal
switch(config)# radius-server host 10.10.1.1 test username user1 password Ur2Gd2BH
idle-time 3
switch(config)# radius-server deadtime 5
switch(config)# exit
switch# show radius-server
switch# copy running-config startup-config
```

Configuring the Dead-Time Interval

You can configure the dead-time interval for all RADIUS servers. The dead-time interval specifies the time that the Nexus 5000 Series switch waits after declaring a RADIUS server is dead, before sending out a test packet to determine if the server is now alive. The default value is 0 minutes.

Note When the dead-time interval is 0 minutes, RADIUS servers are not marked as dead even if they are not responding. You can configure the dead-time interval for a RADIUS server group (see the "Configuring RADIUS Server Groups" section on page 1-8).

To configure dead time interval, perform this task:

	Command	Purpose
Step 1	`switch# configure terminal`	Enters configuration mode.
Step 2	`#switch(config)# radius-server deadtime`	Configures the dead-time interval. The default value is 0 minutes. The range is from 1 to 1440 minutes.
Step 3	`switch(config)# exit`	Exits configuration mode.
Step 4	`switch# show radius-server`	(Optional) Displays the RADIUS server configuration.
Step 5	`switch# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

Manually Monitoring RADIUS Servers or Groups

To manually send a test message to a RADIUS server or to a server group, perform this task:

	Command	Purpose
Step 1	`switch# test aaa server radius {ipv4-address | ipv6-address | server-name} [vrf vrf-name] username password`	Sends a test message to a RADIUS server to confirm availability.
Step 1	`switch# test aaa group group-name username password`	Sends a test message to a RADIUS server group to confirm availability.

The following example shows how to manually send a test message to a RADIUS server:

```
switch# test aaa server radius 10.10.1.1 user1 Ur2Gd2BH
switch# test aaa group RadGroup user2 As3He3CI
```

Verifying RADIUS Configuration

To display RADIUS configuration information, perform one of the following tasks:

Command	Purpose
show running-config radius [**all**]	Displays the RADIUS configuration in the running configuration.
show startup-config radius	Displays the RADIUS configuration in the startup configuration.
show radius-server [*server-name* | *ipv4-address* | *ipv6-address*] [**directed-request** | **groups** | **sorted** | **statistics**]	Displays all configured RADIUS server parameters.

For detailed information about the fields in the output from this command, refer to the *Cisco Nexus 5000 Series Command Reference*.

Displaying RADIUS Server Statistics

To display the statistics the Cisco Nexus 5000 Series switch maintains for RADIUS server activity, perform this task:

	Command	Purpose
Step 1	`switch# switch# show radius-server statistics {hostname | ipv4-address | ipv6-address}`	Displays the RADIUS statistics.

The following example shows how to display statistics:

```
switch# show radius-server statistics 10.10.1.1
```

Example RADIUS Configuration

The following example shows how to configure RADIUS:

```
radius-server key 7 "ToIkLhPpG"
radius-server host 10.10.1.1 key 7 "ShMoMhTl" authentication accounting
aaa group server radius RadServer
    server 10.10.1.1
use-vrf management
```

Default Settings

Table 1-1 lists the default settings for RADIUS parameters.

Table 1-1 Default RADIUS Parameters

Parameters	Default
Server roles	Authentication and accounting
Dead timer interval	0 minutes
Retransmission count	1
Retransmission timer interval	5 seconds
Idle timer interval	0 minutes
Periodic server monitoring username	test
Periodic server monitoring password	test