CHAPTER 2

Configuring RADIUS

This chapter describes how to configure the Remote Access Dial-In User Service (RADIUS) protocol on the Cisco 1000 Series Connected Grid Routers (hereafter referred to as Cisco CG-OS router).

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 Cisco CG-OS router 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 is 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 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 authentication, authorization, and accounting (AAA) authentication and set up per-user profiles. Per-user profiles enable the Cisco CG-OS router to better manage ports by using their existing RADIUS solutions and to efficiently manage shared resources by offering different Service-Level Agreements (SLAs).

RADIUS Operation

When a user attempts to log in to a Cisco CG-OS router and authenticate by using a remote RADIUS server, the following process occurs:

1. Server prompts the user for username and password.
2. Cisco CG-OS router sends entered username and encrypted password over the network to the RADIUS server.
3. The user receives one of the following responses from the RADIUS server:
   - ACCEPT—Server authenticates the user.
   - REJECT—Server does not authenticate the user and the Cisco CG-OS router prompts the user to reenter the username and password, or access is denied.
   - CHALLENGE—Server requests and collects additional information from the user.
   - CHANGE PASSWORD—Server requests that the user 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:

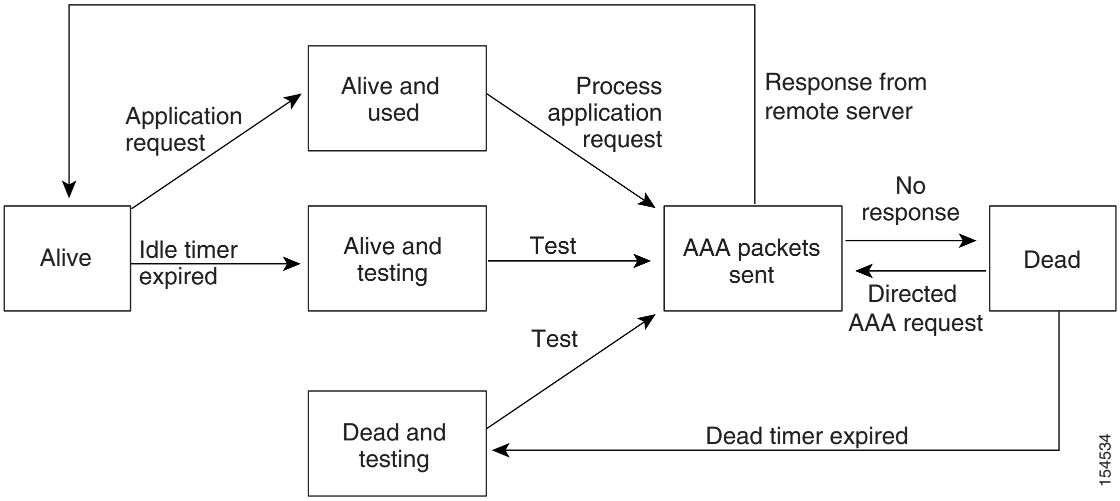
- Services that the user can access, including Telnet, rlogin, or Local-Area Transport (LAT) connections, and Point-to-Point Protocol (PPP), Serial Line Internet Protocol (SLIP), or EXEC services.
- Connection parameters, including the host or client IPv4 or IPv6 address, access list, and user timeouts.

RADIUS Server Monitoring

An unresponsive RADIUS server can cause a delay in processing AAA requests. You can configure the Cisco CG-OS router to periodically monitor a RADIUS server to check whether it is responding (or alive) to save time in processing AAA requests. The Cisco CG-OS router marks unresponsive RADIUS servers as dead and does not send AAA requests to any dead RADIUS servers. The Cisco CG-OS router periodically monitors the dead RADIUS servers and marks them as in the alive state when 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 state, the Cisco CG-OS router displays an error message that a failure is taking place. Figure 2-1 shows the RADIUS server states.

Figure 2-1 RADIUS Server States



Note The Cisco CG-OS router performs RADIUS server monitoring by sending a test authentication request to the RADIUS server. (See Configuring Periodic RADIUS Server Monitoring, page 2-14.)

Vendor-Specific Attributes

The Internet Engineering Task Force (IETF) draft standard specifies attribute 26 as the method for communicating Vendor-Specific Attributes (VSAs) between the network access server and the RADIUS server. 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 Cisco CG-OS router, the RADIUS protocol directs the RADIUS server to return user attributes, such as authorization information, with authentication results. This authorization information is specified through VSAs.

Cisco CG-OS software supports the following VSA protocol options:

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

Cisco CG-OS software 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. For example, if the user belongs to roles network-operator and vdc-admin, the value field is “network-operator vdc-admin.” This subattribute, which the RADIUS server sends in the VSA portion of the Access-Accept frames, can only be used with the shell protocol value. The following examples show the roles attribute that the Cisco Access Control Server (ACS) supports:

  ```
  shell:roles=“network-operator vdc-admin”

  shell:roles*“network-operator vdc-admin”
  ```

  The following examples show the roles attribute that is supported by FreeRADIUS:

  ```
  Cisco-AVPair = ”shell:roles=\“network-operator vdc-admin\””

  Cisco-AVPair = “shell:roles*\“network-operator vdc-admin\””
  ```

Note When you specify a VSA as shell:roles*"network-operator vdc-admin" or "shell:roles*\"network-operator vdc-admin\"", this VSA is flagged as an optional attribute and other Cisco devices ignore this attribute.

- accountinginfo—Stores accounting information in addition to the attributes covered by the standard RADIUS accounting protocol. This attribute is sent only in the VSA portion of the Account-Request frames from the RADIUS client on the Cisco CG-OS router. It can be used only with the accounting protocol data units (PDUs).

Prerequisites for RADIUS

Obtain IPv4 or IPv6 addresses or hostnames for the RADIUS servers.

Obtain keys from the RADIUS servers.

Ensure that the Cisco CG-OS router is is recognized as a RADIUS client on the AAA servers.

Guidelines and Limitations

You can configure a maximum of 64 RADIUS servers on the Cisco CG-OS router.

When you have a user account configured on the local Cisco CG-OS router that has the same name as a remote user account on an AAA server, Cisco CG-OS software applies the user roles for the local user account to the remote user, instead of the user roles configured on the AAA server.

Default Settings

Table 2-1 lists the default settings for RADIUS parameters.

Table 2-1 Default RADIUS Parameters

Parameters	Default
Server roles	Authentication and accounting
Dead timer interval	0 minutes
Retransmission count	1
Retransmission timer interval	5 seconds
Authentication UDP port	1812
Accounting UDP port	1813
Idle timer interval	0 minutes
Periodic server monitoring username	test
Periodic server monitoring password	test

Configuring RADIUS Servers

This section includes the following topics:

- RADIUS Server Configuration Process, page 2-5
- Configuring RADIUS Servers, page 2-6
- Configuring Global RADIUS Keys, page 2-7
- Configuring a Key for a Specific RADIUS Server, page 2-8
- Configuring RADIUS Server Groups, page 2-9
- Configuring the Global Source Interface for RADIUS Server Groups, page 2-10
- Configuring the Global RADIUS Transmission Retry Count and Timeout Interval, page 2-11
- Configuring the RADIUS Transmission Retry Count and Timeout Interval for a Specific Server, page 2-12
- Configuring Accounting and Authentication Attributes for RADIUS Servers, page 2-13
- Configuring Periodic RADIUS Server Monitoring, page 2-14
- Configuring the Dead-Time Interval, page 2-15
- Manually Monitoring RADIUS Server or Groups, page 2-16

RADIUS Server Configuration Process

To configure RADIUS servers, follow these steps:

Step 1 Establish the RADIUS server connections to the Cisco CG-OS router. (See Configuring RADIUS Servers, page 2-6.)

Step 2 Configure the RADIUS secret keys for the RADIUS servers. (See Configuring Global RADIUS Keys, page 2-7.)

Step 3 If needed, configure RADIUS server groups with subsets of the RADIUS servers for AAA authentication methods. (See Configuring RADIUS Server Groups, page 2-9 and Configuring AAA, page 4-6.)

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

- Dead-time interval (See Configuring the Dead-Time Interval, page 2-15.)
- Allow specification of a RADIUS server at login (See Configuring the Global RADIUS Transmission Retry Count and Timeout Interval, page 2-11.)
- Transmission retry count and timeout interval (See Configuring the Global RADIUS Transmission Retry Count and Timeout Interval, page 2-11.)
- Accounting and authentication attributes (See Configuring Accounting and Authentication Attributes for RADIUS Servers, page 2-13.)

Step 5 (Optional) Configure periodic RADIUS server monitoring. (See Configuring Periodic RADIUS Server Monitoring, page 2-14.)

Configuring RADIUS Servers

To access a remote RADIUS server, you must define the IP address or hostname of the RADIUS server on the Cisco CG-OS router. You can configure up to 64 RADIUS servers.

Note

- By default, when you define a RADIUS server IP address or hostname on the Cisco CG-OS router, the RADIUS server becomes a member of the default RADIUS server group.
- You can also add the RADIUS server to another RADIUS server group. For information about creating RADIUS server groups, see Configuring RADIUS Server Groups, page 2-9.

BEFORE YOU BEGIN

Ensure that the server is a member of a server group. Refer to Configuring RADIUS Server Groups, page 2-9.

Ensure that the server is configured to authenticate RADIUS traffic.

Ensure that the Cisco CG-OS router is recognized as a RADIUS client on the AAA servers.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**radius-server host** {*ipv4-address* | *ipv6-address* | *host-name*}	Specifies the IPv4 or IPv6 address or hostname for a RADIUS server to use for authentication.
Step 3	**show radius-server**	(Optional) Displays the RADIUS server configuration.
Step 4	**copy running-config startup-config**	(Optional) Saves this configuration change.

EXAMPLE

This example shows how to define an IPv4 address or hostname for those RADIUS servers that the Cisco CG-OS router wants to access.

```
router# configure terminal
router(config)# radius-server host 10.10.1.1
router(config)# copy running-config startup-config
```

Configuring Global RADIUS Keys

You can configure RADIUS keys for all servers used by the Cisco CG-OS router. A RADIUS key is a shared secret text string between the Cisco CG-OS router and the RADIUS server hosts. To configure a RADIUS key specific to a RADIUS server, see Configuring a Key for a Specific RADIUS Server, page 2-8.

BEFORE YOU BEGIN

Obtain the RADIUS key values for the remote RADIUS servers.

Configure the RADIUS key on the remote RADIUS servers.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**radius-server key** [**0** | **7**] *key-value*	Specifies a RADIUS key for all RADIUS servers. You can specify that the *key-value* be in clear-text (**0**) format or be encrypted (**7**). Cisco CG-OS software encrypts a clear-text key before saving it to the running configuration. The maximum length is 63 characters. The default format is clear-text. By default, no RADIUS key is configured.

	Command	Purpose
Step 3	**show radius-server [groups | sorted | statistics]**	(Optional) Displays the RADIUS server configuration or the specified options. **groups**–Displays RADIUS server group configuration. **sorted**–Lists RADIUS servers sorted by name. **statistics**–Displays RADIUS statistics. **Note** The Cisco CG-OS router saves the RADIUS keys in encrypted form in the running configuration. Use the **show running-config** command to display the encrypted RADIUS keys. Enter the **show** command in the EXEC mode to display all options above.
Step 4	**copy running-config startup-config**	(Optional) Saves the configuration change.

EXAMPLE

This example shows how to configure a global key for all RADIUS servers with which the Cisco CG-OS router communicates.

```
router# configure terminal
router(config)# radius-server key 0 PlIjUhYg
router(config)# copy running-config startup-config
```

Configuring a Key for a Specific RADIUS Server

You can configure a key on the Cisco CG-OS router for a specific RADIUS server. A RADIUS key is a secret text string shared between the Cisco CG-OS router and a specific RADIUS server.

BEFORE YOU BEGIN

Configure one or more RADIUS server hosts. (See Configuring RADIUS Servers, page 2-6.)

Obtain the key value for the remote RADIUS server.

Configure the key on the RADIUS server.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**radius-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **key** [**0** | **7**] *key-value*	Specifies a RADIUS key for a specific RADIUS server. You can specify that the *key-value* is in clear-text (**0**) format or is encrypted (**7**). The Cisco CG-OS software encrypts a clear-text key before saving it to the running configuration. The maximum length is 63 characters. The default format is clear-text. The specified RADIUS server uses this RADIUS key rather than the global RADIUS key.
Step 3	**show radius-server**	(Optional) Displays the RADIUS server configuration. **Note** Cisco CG-OS software saves the RADIUS keys in encrypted form in the running configuration. Use the **show running-config** command to display the encrypted RADIUS keys.
Step 4	**copy running-config startup-config**	(Optional) Saves this configuration change.

EXAMPLE

This example shows how to configure a shared key on a RADIUS server:

```
router# configure terminal
router(config)# radius-server host 10.10.1.1 key 0 PlIjUhYg
router(config)# 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 use the RADIUS protocol. The Cisco CG-OS router contacts the servers in the order in which they are configured. You can configure up to 100 server groups on the Cisco CG-OS router.

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 Remote AAA Services, page 4-2.

BEFORE YOU BEGIN

Ensure that all servers that you want to add to the group are RADIUS servers.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**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	**server** {*ipv4-address* | *ipv6-address* | *host-name*}	Configures the RADIUS server as a member of the RADIUS server group. **Tip** When the specified RADIUS server is not found, enter the **radius-server host** command to identify the server and then retry this command.
Step 4	**deadtime** *minutes*	(Optional) Configures the monitoring dead time. The range is from 1 through 1440. The default is 0 minutes. **Note** When 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 Configuring the Dead-Time Interval, page 2-15.)
Step 5	**source-interface** *interface*	(Optional) Configures a source interface to access the RADIUS servers in the server group. You can use Ethernet, cellular, and WiMax interfaces, and loopback interfaces. The default is the global source interface. (See Configuring the Global Source Interface for RADIUS Server Groups, page 2-10.)
Step 6	**show radius-server groups** [*group-name*]	(Optional) Displays the RADIUS server group configuration.
Step 7	**copy running-config startup-config**	(Optional) Copies the running configuration to the startup configuration.

EXAMPLE

This example shows how to create a RADIUS server group.

```
router# configure terminal
router(config)# aaa group server radius RadServer
router(config-radius)# server 10.10.1.1
router(config-radius)# copy running-config startup-config
```

Configuring the Global Source Interface for RADIUS Server Groups

You can configure a global source interface for RADIUS server groups to use when accessing RADIUS servers. To configure a different source interface for a specific RADIUS server group, see Configuring RADIUS Server Groups, page 2-9. By default, Cisco CG-OS software uses any available interface.

BEFORE YOU BEGIN

Configure at least one server group.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**ip radius source-interface** *interface*	Configures the global source interface for all RADIUS server groups configured on the device.
Step 3	**show radius-server [groups | sorted | statistics]**	(Optional) Displays the RADIUS server configuration information.
Step 4	**copy running-config startup-config**	(Optional) Copies the running configuration to the startup configuration.

EXAMPLE

```
router# configure terminal
router(config)# ip radius source-interface mgmt 0
router(config)# copy running-config startup-config
```

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 Cisco CG-OS router 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 Cisco CG-OS router waits for responses from RADIUS servers before declaring a timeout failure.

BEFORE YOU BEGIN

Configure at least one server group.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**radius-server retransmit** *count*	Specifies the number of times that a router retransmits data to a RADIUS server before it reverts to local authentication. Sets the retransmission count for all RADIUS servers. The count range is from 1 to 5. The default retransmission count is 1.
Step 3	**radius-server timeout** *seconds*	Specifies the transmission timeout interval for RADIUS servers. The range is from 1 to 60 seconds. The default timeout interval is 5 seconds.

	Command	Purpose
Step 4	**show radius-server**	(Optional) Displays the RADIUS server configuration.
Step 5	**copy running-config startup-config**	(Optional) Copies the running configuration to the startup configuration.

EXAMPLE

This example shows how to configure the global RADIUS parameters, transmission retry count and timeout interval.

```
router# configure terminal
router(config)# radius-server retransmit 3
router(config)# radius-server timeout 10
router(config)# copy running-config startup-config
```

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

By default, the Cisco CG-OS router retries a 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 Cisco CG-OS router waits for responses from RADIUS servers before declaring a timeout failure and reporting it to the system log.

BEFORE YOU BEGIN

Configure at least one RADIUS server. (See Configuring RADIUS Servers, page 2-6.)

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**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 specific RADIUS server overrides the global count value specified for all RADIUS servers.
Step 3	**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 specific RADIUS server overrides the global interval value specified for all RADIUS servers.

	Command	Purpose
Step 4	**show radius-server**	(Optional) Displays the RADIUS server configuration.
Step 5	**copy running-config startup-config**	(Optional) Copies the running configuration to the startup configuration.

EXAMPLE

This example shows how to configure the RADIUS parameters, transmission retry count and timeout interval, for a specific server.

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

Configuring Accounting and Authentication Attributes for RADIUS Servers

You can specify that a RADIUS server only be used for accounting purposes or only be used for authentication purposes. By default, RADIUS servers perform both accounting and authentication.

You can also specify the destination UDP port numbers for RADIUS accounting and authentication messages when there is a conflict with the default port.

BEFORE YOU BEGIN

Configure at least one RADIUS server. (See Configuring RADIUS Servers, page 2-6.)

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**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 range is from 0 to 65535. The default UDP port is 1813.
Step 3	**radius-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **accounting**	(Optional) Specifies the RADIUS server for accounting purposes only. The default is both accounting and authentication.
Step 4	**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 range is from 0 to 65535. The default UDP port is 1812.
Step 5	**radius-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **authentication**	(Optional) Specifies the RADIUS server for authentication purposes only. The default is both accounting and authentication.

	Command	Purpose
Step 6	**show radius-server**	(Optional) Displays the RADIUS server configuration.
Step 7	**copy running-config startup-config**	(Optional) Copies the running configuration to the startup configuration.

EXAMPLE

This example shows how to configure one RADIUS server to perform only accounting and another to perform only authentication.

```
router# configure terminal
router(config)# radius-server host 10.10.1.1 accounting
router(config)# radius-server host 10.10.2.2 authentication
router(config)# 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 Cisco CG-OS router sends out a test packet. You can configure this option to test servers periodically.

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

Note The default idle timer value is 0 minutes. When the idle time interval is 0 minutes, the Cisco CG-OS router does not perform periodic RADIUS server monitoring.

BEFORE YOU BEGIN

Configure at least one RADIUS server. (See Configuring RADIUS Servers, page 2-6.)

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**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 password is **test**. The valid range for the idle timer is from 0 to 1440 minutes. The default value for the idle timer is 0 minutes. **Note** For periodic RADIUS server monitoring, you must set the idle timer to a value greater than 0.

	Command	Purpose
Step 3	**radius-server dead-time** *minutes*	Specifies the number of minutes before the Cisco CG-OS router checks a RADIUS server that was previously unresponsive. The valid range is from 1 to 1440 minutes. The default value is 0 minutes.
Step 4	**show radius-server**	(Optional) Displays the RADIUS server configuration.
Step 5	**copy running-config startup-config**	(Optional) Copies the running configuration to the startup configuration.

EXAMPLE

This example shows how to configure RADIUS monitoring parameters.

```
router# configure terminal
router(config)# radius-server host 10.10.1.1 test username user1 password Ur2Gd2BH
idle-time 3
router(config)# radius-server dead-time 5
router(config)# 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 Cisco CG-OS router waits after declaring a RADIUS server as 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 Configuring RADIUS Server Groups, page 2-9.)

BEFORE YOU BEGIN

Configure at least one RADIUS server. (See Configuring RADIUS Servers, page 2-6.)

DETAILED STEPS

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

EXAMPLE

This example shows how to configure the dead interval for all RADIUS servers.

```
router# configure terminal
router(config)# radius-server deadtime 5
router(config)# copy running-config startup-config
```

Manually Monitoring RADIUS Server or Groups

You can manually issue a test message to a RADIUS server or to a server group.

BEFORE YOU BEGIN

Configure at least one RADIUS server and server group. (See Configuring RADIUS Servers, page 2-6 and Configuring RADIUS Server Groups, page 2-9.)

DETAILED STEPS

	Command	Purpose
Step 1	**test aaa server radius** {*ipv4-address* | *ipv6-address* | *host-name*} *username password*	Sends a test message to a RADIUS server to confirm availability.
Step 1	**test aaa group** *group-name username password*	Sends a test message to a RADIUS server group to confirm availability.

EXAMPLE

This example shows how to configure a test message to be sent to a RADIUS server.

```
router# test aaa server radius 10.10.1.1 user1 Ur2Gd2BH

This example shows how to configure a test message to be sent to a RADIUS server group.

router# test aaa group RadGroup user2 As3He3CI
```

Verifying Configuration

To display RADIUS configuration information, enter any or all of the following commands.

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 [*host-name* | *ipv4-address* | *ipv6-address*] [**groups** | **sorted** | **statistics**]	Displays all configured RADIUS server parameters or a subset using the optional parameters.

For detailed information about the fields in the output from these commands, see the Command Lookup Tool on Cisco.com.

Monitoring Statistics

BEFORE YOU BEGIN

Configure at least one RADIUS server. (See Configuring RADIUS Servers, page 2-6.)

DETAILED STEPS

To display the statistics that the Cisco CG-OS router maintains for RADIUS server activity, enter the command below.

Command	Purpose
show radius-server statistics {*hostname* | *ipv4-address* | *ipv6-address*}	Displays statistics for RADIUS servers.

Configuration Example

The following example shows how to configure a RADIUS server:

```
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
```

Where to Go Next

You can now configure AAA authentication methods to include the RADIUS server groups. (See Chapter 4, “Configuring AAA”.)