Configuring RADIUS Support: Learning Who the Subscriber Is

This chapter contains the following information:

- Configuring RADIUS Inspection: Endpoint, page 5-2
- Configuring RADIUS Inspection: Proxy, page 5-2
- Configuring RADIUS Inspection: Monitor, page 5-3
- Configuring RADIUS Inspection: Packet of Disconnect, page 5-3
- Configuring RADIUS Inspection: Associating a Table Name with a RADIUS Proxy or Endpoint, page 5-4
- Configuring RADIUS Inspection: Preventing the CSG from Acknowledging Errors, page 5-4
- Extracting the Billing Plan ID Using RADIUS, page 5-5
- Reporting Arbitrary RADIUS Attributes and VSA Subattributes, page 5-5
- RADIUS Attributes Required for CSG User Table, page 5-6

Figure 5-2 illustrates the placement of the Content Services Gateway (CSG) as a RADIUS Accounting proxy or monitor in the RADIUS Accounting and data flows.

Figure 5-1 RADIUS Accounting and Data Flows—RADIUS Accounting Proxy or Monitor

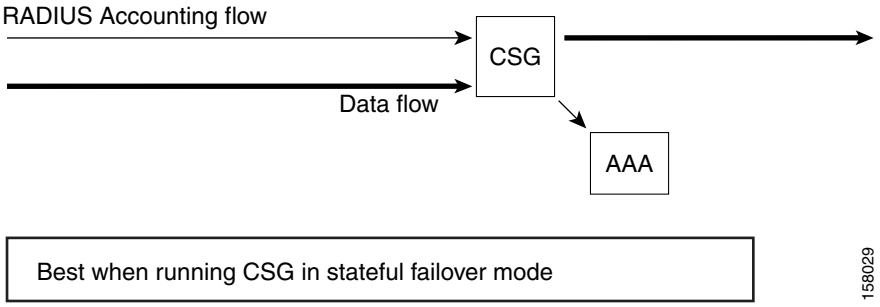
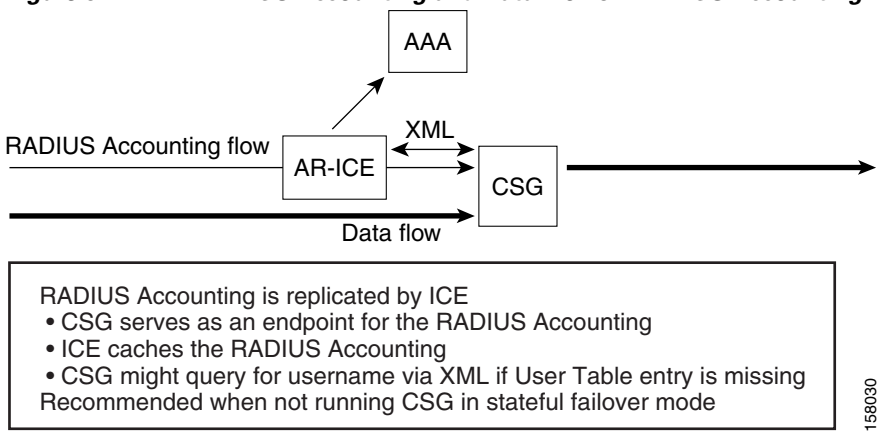


Figure 5-2 illustrates the placement of the CSG as a RADIUS Accounting endpoint plus Access Registrar-Identity Cache Engine (AR-ICE) in the RADIUS Accounting and data flows.

Figure 5-2 RADIUS Accounting and Data Flows—RADIUS Accounting Endpoint Plus AR-ICE



Configuring RADIUS Inspection: Endpoint

The CSG RADIUS features require that you configure the Network Access Server (NAS) to direct RADIUS messages to the CSG IP address (or to the alias address if this is a redundant configuration). You must also configure the NAS to the specific port number for the CSG. The following configuration specifies the port number for the RADIUS endpoint:

```
module csg 3
 radius endpoint 1.2.3.4 key secret
```

To support RADIUS endpoint, the CSG requires a route to 255.255.255.255. You can configure the route by using the **gateway (module CSG VLAN)** command or the **route (module CSG VLAN)** command. For example:

gateway 31.0.0.6

or:

route 255.255.255.255 255.255.255.255 gateway 31.0.0.6

Configuring RADIUS Inspection: Proxy

The CSG proxy function allows operation with clients that use many port numbers. RADIUS proxy can eliminate routing errors (RADIUS is targeted directly to the CSG addresses), and must be used in place of RADIUS monitor when the CSGs are being load-balanced.

RADIUS proxy supports both RADIUS Access and RADIUS Accounting.

Configuring RADIUS Inspection: Monitor

RADIUS monitor enables you to to insert the CSG into a network without changing the AAA or NAS addresses in the network. The CSG monitors the traffic between the RADIUS client and the RADIUS server, looking for RADIUS messages that match configured rules. The address of the server must be configured.

Optionally, a RADIUS key can be configured.

- If a RADIUS key is configured, the CSG parses and acts on a message only if the RADIUS Authenticator is correct. However, every message is forwarded, regardless of whether the RADIUS key is configured or is correct.
- If a RADIUS key is not configured, the CSG always parses and forwards every message.

Here is a sample configuration of a RADIUS key:

```
ip csg user-group U1
 radius userid User-Name
 radius monitor 10.2.3.4 1234 key cisco --> Address, Port, and Key for RADIUS AAA Server.
 radius monitor 10.2.3.9 1234 key cisco2
 radius monitor 10.2.7.4 3901 key cisco --> Multiple AAA destinations can be monitored.
```

All RADIUS messages, including access messages, are forwarded, except when the IP or User Datagram Protocol (UDP) headers specify a length that is larger than the physical packet size.

All RADIUS messages, including access messages, are forwarded, except when the IP or UDP headers specify a length larger than the physical packet size.

When configuring RADIUS monitor for a server that is in the same subnet as a CSG interface, you must first configure a dummy route for that server, such as:

route *ip-address* **255.255.255.255 gateway** *gw-ip-address*

where:

- *ip-address* is any IP address that is not used in the network
- *gw-ip-address* is the gateway IP address

Add a RADIUS monitor configuration only after you have added the dummy route.

Configuring RADIUS Inspection: Packet of Disconnect

This configuration specifies the following Packet of Disconnect (PoD) characteristics:

- The RADIUS attributes to be copied from the RADIUS Start message and sent to the NAS in the PoD message
- The NAS port to which the CSG is to send the PoD message, and the key to use in calculating the Authenticator
- The number of times to retry the RADIUS PoD message if it is not acknowledged, and the interval between retries

Here is a sample configuration for RADIUS PoD:

```
ip csg user-group G1
 radius userid User-Name
 radius pod attribute 44
 radius pod nas 1.1.1.0 1.1.1.255 1700 key secret
 radius pod nas 1701 key password
 radius pod timeout 30 retransmits 5
```

```
mod csg 3
 radius proxy 1.2.3.4 5.6.7.8 key secret
```

Configuring RADIUS Inspection: Associating a Table Name with a RADIUS Proxy or Endpoint

Interface awareness enables the CSG to distinguish between users and sessions that share the same IP address on different VLANs (that is, users and sessions with overlapping IP addresses). Interface awareness requires that each VLAN be associated with a table name. You can also associate the table name with a particular RADIUS proxy or endpoint.

To associate the table name with a particular RADIUS proxy, enter the following command in module CSG configuration mode, specifying the **table** keyword and a table name:

Command	Purpose
Router(config-csg-module)# **radius proxy** *csg_addr server addr* [*csg_source_addr*] [**key** [*encrypt*] *secret-string*] [**table** *table-name*]	Specifies that the CSG is to be a proxy for RADIUS messages.

To associate the table name with a particular RADIUS endpoint, enter the following command in module CSG configuration mode, specifying the **table** keyword and a table name:

Command	Purpose
Router(config-csg-module)# **radius endpoint** *csg_addr* **key** [*encrypt*] *secret-string* [**table** *table-name*]	Identifies the CSG as an endpoint for RADIUS Accounting messages.

Configuring RADIUS Inspection: Preventing the CSG from Acknowledging Errors

By default, the CSG acknowledges the following errors:

1. The User Table entry cannot be created because of resource constraints.
2. The CSG parses the RADIUS Accounting Request and encounters RADIUS protocol errors.
3. The CSG parses the RADIUS Accounting Request and a billing plan is specified in the RADIUS Accounting Request, but it does not match a billing plan in the CSG configuration.
4. The CSG parses the RADIUS Accounting Request and a quota server is specified in the RADIUS Accounting Request, but it does not match a quota server in the CSG configuration.
5. The CSG parses the RADIUS Accounting Request and a connect service is specified in the RADIUS Accounting Request, but it does not match a connect service in the CSG configuration.

   For errors 3, 4, and 5, the CSG can parse the configuration vendor-specific attribute (VSA) from the RADIUS Access-Accept. If the CSG uses any attribute from the RADIUS Access-Accept that does not match the CSG configuration, the CSG does not send a RADIUS response to the RADIUS Accounting Request.

For RADIUS endpoint and RADIUS proxy configurations, you can prevent the CSG from acknowledging these errors by entering the **no** form of the **radius ack error** command in CSG user group configuration mode.

For RADIUS Accounting requests processed as a result of matching a **radius endpoint** command, the CSG does not send a RADIUS acknowledgement.

For RADIUS Accounting requests processed as a result of matching a **radius proxy** command, the CSG does not forward the RADIUS Accounting Request to the RADIUS server.

Extracting the Billing Plan ID Using RADIUS

The CSG can extract the Billing Plan ID from the RADIUS Access-Accept by using a CSG VSA. The following information is included:

- Attribute number: 26 (=vendor specific)
- Vendor ID: 9 (=Cisco)
- Subattribute: 1 (=Cisco generic)
- Format: csg:billing_plan=

  where the billing plan name appears after the equal sign (=). If the attribute is present, but no billing plan is specified, the user is postpaid.

The new **user-profile** command enables the billing plan function. If the CSG is configured to obtain the billing plan from RADIUS, and the billing plan subattribute is included in the RADIUS messages, the CSG does not query the quota server (that is, the CSG does not send a User Profile Request). If the billing plan attribute is not present in the RADIUS messages when the CSG receives the RADIUS Accounting Start with the user ID, the CSG queries the quota server to obtain the attribute.

Reporting Arbitrary RADIUS Attributes and VSA Subattributes

The operator can specify a set of attributes and VSA subattributes to be extracted from the RADIUS Accounting Start messages for each subscriber and to be reported with each transaction record.

The CSG saves these attributes and VSA subattributes for each subscriber and replaces them when a new RADIUS Accounting Start is received.

For example, in a gateway general packet radio service (GPRS) environment you can use attributes as follows:

- NAS-IP-Address (4) identifies the gateway GPRS support node (GGSN) to which the subscriber is tunneled.
- SGSN IP (26/10415/6) identifies the Service GPRS Support Node (SGSN) that the subscriber is accessing.
- Acct-session-ID (44) uniquely identifies the session on this NAS and can be used for correlation to GGSN accounting records.

RADIUS Attributes Required for CSG User Table

The User Table identifies all users known to the CSG. The table is populated from the contents of RADIUS Accounting Start messages, or from the user database, if either feature is enabled in your configuration.

The following RADIUS attributes must be in the RADIUS Accounting Start in order for the CSG to build an entry for a user in the CSG User Table:

- 8 (Framed-IP-Address)
- Either 4 (NAS-IP-Address) or 32 (NAS-Identifier)
- Either 1 (User-Name) or 31 (Calling-Station-Id), as configured

When the CSG receives the RADIUS Access-Accept with Billing Plan ID included, it caches the information. The cached information is identified by user ID (either RADIUS Attribute 1 or RADIUS Attribute 31, as configured). When the CSG receives the RADIUS Accounting Start message with the user ID, the CSG builds a User Table entry by using the cached information.

Note Cached information is not displayed in the output of the **show module csg accounting users** command.