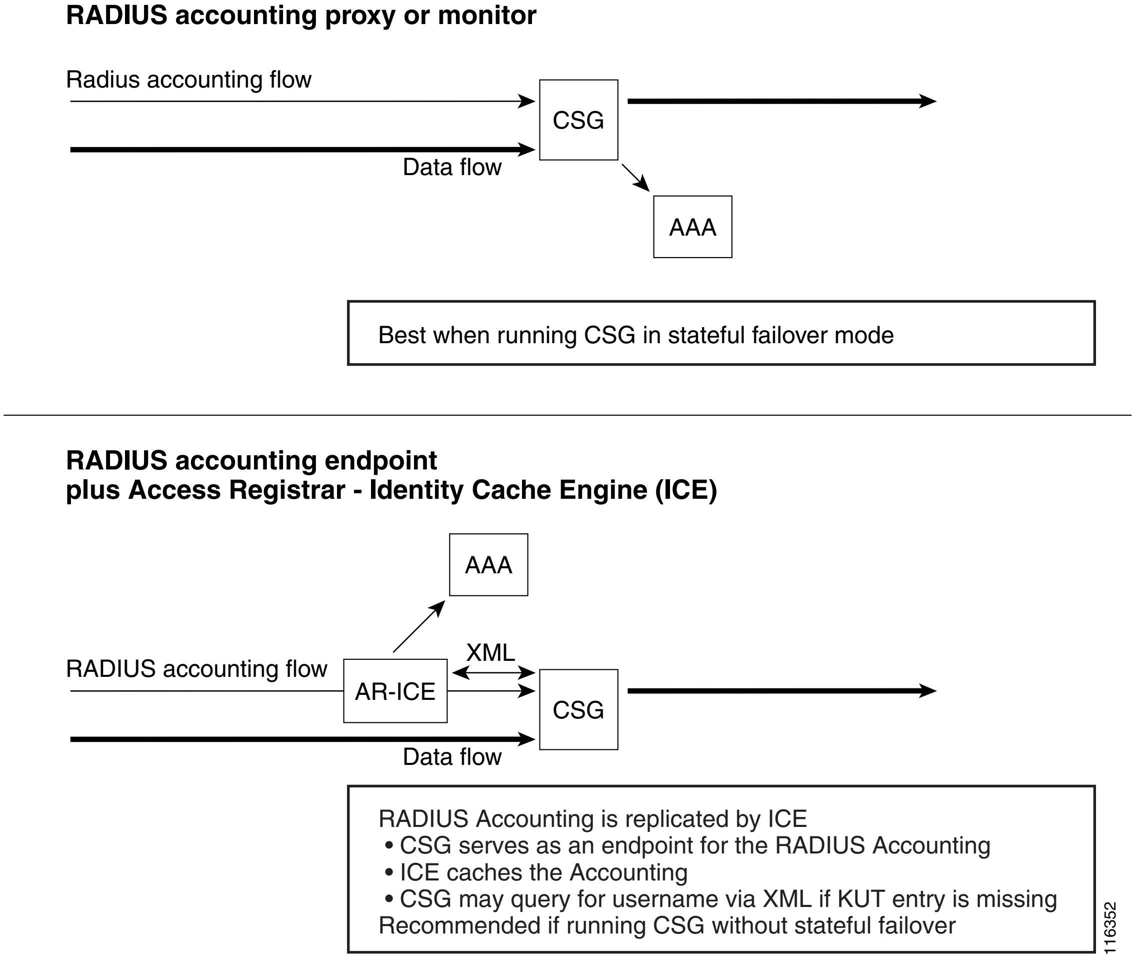
CHAPTER 5

Configuring RADIUS Support: Learning Who the Subscriber Is

Figure 5-1 illustrates the placement of the CSG in the RADIUS accounting and data flows.

Figure 5-1 RADIUS Accounting and Data Flows


RADIUS accounting proxy or monitor
Radius accounting flow
CSG
Data flow
AAA
Best when running CSG in stateful failover mode
RADIUS accounting endpoint
plus Access Registrar - Identity Cache Engine (ICE)
AAA
XML
RADIUS accounting flow
AR-ICE
CSG
Data flow
RADIUS Accounting is replicated by ICE
• CSG serves as an endpoint for the RADIUS Accounting
• ICE caches the Accounting
• CSG may query for username via XML if KUT entry is missing
Recommended if running CSG without stateful failover
116352

This chapter contains the following information:

Configuring RADIUS Inspection: Endpoint

This configuration specifies the port number for the RADIUS accounting endpoint.

The CSG RADIUS features require that you configure the 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 your NAS to the specific CSG port number. The following example illustrates the configuration:

```
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

Note When the CSG2 is configured as a RADIUS endpoint, the CSG2 drops all RADIUS packets other than RADIUS Accounting-Request messages.

Configuring RADIUS Inspection: Proxy

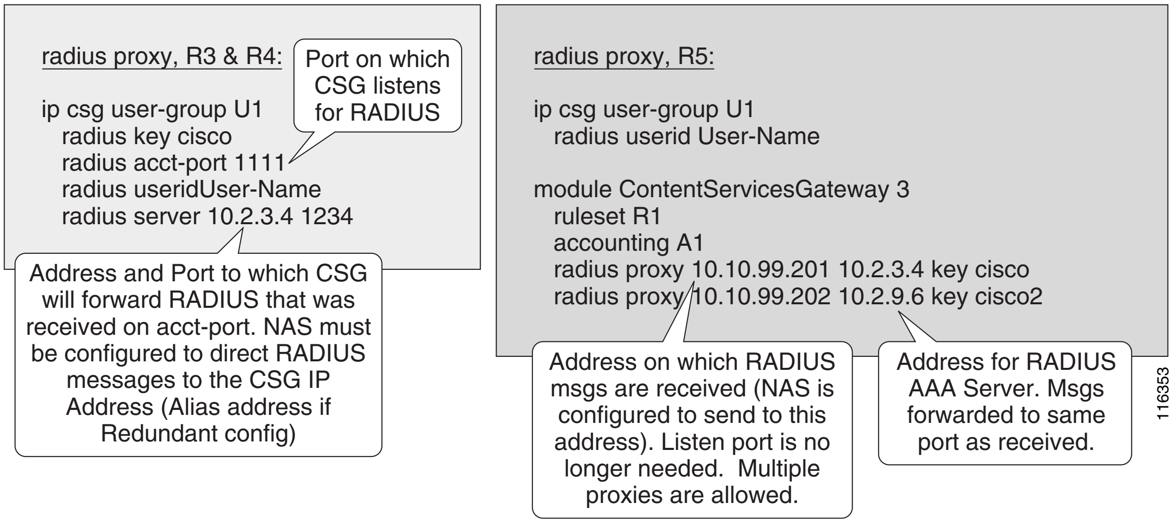
The CSG enhances the proxy function to allow operation with clients that use large numbers of port numbers. RADIUS proxy provides a way to remove the chance of routing errors (RADIUS is targeted at the CSG IP addresses directly), and must be used in place of RADIUS monitor when the CSGs are being load-balanced.

RADIUS proxy supports both RADIUS Access and RADIUS Accounting.

Note The old proxy function is still supported, and operates as before if you configure it in the old way. However, we strongly recommend that you use the new proxy support.

Figure 5-2 illustrates the differences between configurations.

Figure 5-2 RADIUS Proxy Configuration Changes


radius proxy, R3 & R4:
ip csg user-group U1
radius key cisco
radius acct-port 1111
radius useridUser-Name
radius server 10.2.3.4 1234
Port on which CSG listens for RADIUS
Address and Port to which CSG will forward RADIUS that was received on acct-port. NAS must be configured to direct RADIUS messages to the CSG IP Address (Alias address if Redundant config)
radius proxy, R5:
ip csg user-group U1
radius userid User-Name
module ContentServicesGateway 3
ruleset R1
accounting A1
radius proxy 10.10.99.201 10.2.3.4 key cisco
radius proxy 10.10.99.202 10.2.9.6 key cisco2
Address on which RADIUS msgs are received (NAS is configured to send to this address). Listen port is no longer needed. Multiple proxies are allowed.
Address for RADIUS AAA Server. Msgs forwarded to same port as received.
116353

Using a CSG 3.1(3)C4(1) RADIUS configuration on the CSG 3.1(3)C5(1) or later results in the CSG 3.1(3)C4(1) behavior.

Configuring RADIUS Inspection: Monitor

RADIUS monitor provides a way to insert the CSG 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 flowing through it that match the configured rule. The address of the server must be configured.

Optionally, a RADIUS key is configured. If the key is configured, the CSG parses and acts on the message only if the RADIUS Authenticator is correct. If the key is not configured, the CSG always parses the message. The message is forwarded regardless of the key being configured or correct. Here is a sample configuration:

```
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 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 should 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 should 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 due to resource constraints.
2. The CSG parses the Accounting Request and encounters RADIUS protocol errors.
3. The CSG parses the Accounting Request and a billing plan is specified in the Accounting Request, but it does not match a billing plan in the CSG configuration.
4. The CSG parses the Accounting Request and a quota server is specified in the Accounting Request, but it does not match a quota server in the CSG configuration.
5. The CSG parses the Accounting Request and a connect service is specified in the 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 VSA from the Access-Accept. If the CSG uses any attribute from the Access-Accept that does not match the CSG configuration, the CSG does not send a RADIUS response to the 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 Accounting Request to the RADIUS server.

Extracting the Billing Plan ID Using RADIUS

Prior to the CSG 3.1(3)C5(1), the CSG required that the quota server provide the Billing Plan ID. The information had to be provisioned to the quota server, or the quota server had to act as a surrogate (retrieving from the authentication, authorization, and accounting (AAA) server in order to send to the CSG). It was not possible to distinguish between prepaid and postpaid users if the quota server was unavailable.

The CSG now adds the ability to extract the Billing Plan ID from RADIUS Access Accept 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 get the billing plan from RADIUS, and the billing plan sub-attribute is included in the RADIUS messages, the CSG does not query the quota server (that is, no User Profile Request). If the billing plan attribute is not present in the RADIUS messages by the time the CSG receives the Accounting Start with the user ID, the CSG queries the quota server.

Reporting Arbitrary RADIUS Attributes

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

Note VSAs (attribute 26) are not separable (all are sent).

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

For example, in a GPRS environment you can use this capability as follows:

- NAS-IP-Address (4) identifies the GGSN to which the subscriber is tunneled.
- SGSN IP (26/10415/6) identifies the SGSN 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 based on the contents of RADIUS Accounting Start messages, or from the user database, if either feature is enabled in your configuration. The CSG requires the following RADIUS attributes in the RADIUS Accounting Start in order to build an entry for a user in the CSG User Table 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, it builds a User Table entry using the cached information.

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