



CHAPTER 10

Configuring Security on the GGSN

This chapter describes how to configure security features on the gateway GPRS support node (GGSN), including Authentication, Authorization, and Accounting (AAA), and RADIUS.



Note

IPSec on the Cisco 7600 series router platform is performed on the IPSec VPN Acceleration Services module and requires no configuration on the GGSNs running on the Cisco MWAM.

For information about configuring IPSec on the Cisco 7600 series router platform, refer to the *IPSEC VPN Acceleration Services Module Installation and Configuration Note*.

The security configuration procedures and examples in this publication (aside from those related to GGSN-specific implementation) describe the basic commands that you can use to implement the security services.

For more detailed information about AAA, RADIUS, and IPSec security services in the Cisco IOS software, refer to the *Cisco IOS Security Configuration Guide* and *Cisco IOS Security Command Reference* publications. For information about IPSec security services on Cisco 7600 platform, see the *IPSec VPN Acceleration Services Module Installation and Configuration Note*.

For a complete description of the GGSN commands in this chapter, refer to the *Cisco GGSN Command Reference* for the Cisco GGSN release you are using. To locate documentation of other commands that appear in this chapter, use the command reference master index or search online.

This chapter includes the following sections:

- [Overview of Security Support on the GGSN, page 10-2](#)
- [Configuring AAA Security Globally, page 10-4](#) (Required)
- [Configuring RADIUS Server Communication Globally, page 10-5](#) (Required)
- [Configuring RADIUS Server Communication at the GGSN Configuration Level, page 10-6](#) (Required)
- [Configuring Additional RADIUS Services, page 10-10](#) (Optional)
- [Securing the GGSN Mobile \(Gn\) Interface, page 10-28](#) (Optional)
- [Configuration Examples, page 10-30](#)

Overview of Security Support on the GGSN

The GGSN supports many of the same levels of security that are available through the Cisco IOS software on the router, including the following types of security:

- Authentication, authorization, and accounting (AAA) network security services and server groups
- RADIUS security services
- IP Security Protocol (IPSec)

In addition, the GGSN software provides the ability to configure additional security features such as the following:

- Address verification
- Traffic redirection
- IP access lists

AAA and RADIUS support provides the security services to authenticate and authorize access by mobile users to the GGSN and its access point names (APNs). IPSec support allows you to secure your data between the GGSN and its associated peers.

In some cases, such as with AAA and IPSec support, the GGSN works with the standard Cisco IOS software configuration without requiring configuration of any additional GGSN commands.

In the case of RADIUS server configuration, the GGSN requires that you enable AAA security and establish RADIUS server communication globally on the router. From there, you can configure RADIUS security for all GGSN access points, or per access point, using new GGSN configuration commands.

**Note**

In addition to the AAA, RADIUS, and IPSec security services, the GGSN also supports IP access lists to further control access to APNs. The Cisco IOS GGSN software implements the new **ip-access-group** access-point configuration command to apply IP access list rules at an APN.

AAA Server Group Support

The Cisco GGSN supports authentication and accounting at APNs using AAA server groups. By using AAA server groups, you gain the following benefits:

- You can selectively implement groups of servers for authentication and accounting at different APNs.
- You can configure different server groups for authentication services and accounting services in the same APN.
- You can control which RADIUS services you want to enable at a particular APN, such as AAA accounting.

For GPRS tunneling protocol (GTP)-PPP termination and GTP-PPP regeneration on the GGSN, transparent access mode is used to allow PPP to perform the appropriate AAA functions; however, you can still configure AAA server groups to specify the corresponding server groups for AAA support.

The GGSN supports the implementation of AAA server groups at both the global and access-point configuration levels. You can minimize your configuration by specifying the configuration that you want to support across most APNs, at the global configuration level. Then, at the access-point configuration level, you can selectively modify the services and server groups that you want to support at a particular APN. Therefore, you can override the AAA server global configuration at the APN configuration level.

To configure a default AAA server group to be used for all APNs on the GGSN, use the **gprs default aaa-group** global configuration command. To specify a different AAA server group to be used at a particular APN for authentication or accounting, use the **aaa-group** access-point configuration command.

If authentication is enabled on the APN, then the GGSN first looks for an authentication server group at the APN. If an authentication server group is not found at the APN, then the GGSN looks for a globally configured, General Packet Radio Service/Universal Mobile Telecommunication System (GPRS/UMTS) default authentication server group.

If accounting is enabled on the APN, then the GGSN looks for an accounting server group at the APN or globally in the following order:

- First, at the APN for an accounting server group—configured in the **aaa-group accounting** command.
- Second, for a global GPRS/UMTS default accounting server group—configured in the **gprs default aaa-group accounting** command.
- Third, at the APN for an authentication server group—configured in the **aaa-group authentication** command.
- Last, for a global GPRS/UMTS default authentication server group—configured in the **gprs default aaa-group authentication** command.

To complete the configuration, you also must specify the following configuration elements on the GGSN:

- Configure the RADIUS servers by using the **radius-server host** command.
- Define a server group with the IP addresses of the AAA servers in that group, using the **aaa group server** global configuration command.
- Enable the type of AAA services (accounting and authentication) to be supported on the APN.
 - The GGSN enables accounting by default for non-transparent APNs.
You can disable accounting services at the APN by using the **aaa-accounting disable** command.
 - You can enable authentication at the APN level by configuring the **access-mode non-transparent** command. When you enable authentication, the GGSN automatically enables accounting on the APN. There is no a global configuration command for enabling or disabling authentication.
- Configure AAA accounting and authentication using the **aaa accounting** and **aaa authentication** global configuration commands.

**Note**

For more information about AAA and RADIUS global configuration commands, see the *Cisco IOS Security Command Reference*.

Configuring AAA Security Globally

Authentication, authorization, and accounting (AAA) network security services provide the primary framework through which you set up access control on your GGSN. This section provides information about the basic commands used to implement AAA security on a Cisco router.

To enable AAA and configure authentication and authorization, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# aaa new-model	Enables AAA globally.
Step 2	Router(config)# aaa authentication ppp {default list-name} method1 [method2...]	Creates a local authentication method list, with the following options: <ul style="list-style-type: none"> • default—Specifies that the authentication methods that follow this argument are the default list of authentication methods when a user logs in to the router. • <i>method</i>—Specifies a valid AAA authentication method for PPP. For example, group (RADIUS) enables global RADIUS authentication.
Step 3	Router(config)# aaa authorization {auth-proxy network exec commands level reverse-access} {default list-name} [method1 [method2...]]	Creates an authorization method list for a particular authorization type and enables authorization.
Step 4	Router(config)# aaa accounting {system default [vrf vrf-name] network {default none start-stop stop-only wait-start} group group-name	Enables AAA accounting of requested services for billing or security purposes when you use RADIUS.

For more information about configuring AAA, refer to the *Cisco IOS Security Configuration Guide* and *Cisco IOS Security Command Reference* publications.

Configuring RADIUS Server Communication Globally

This section describes how to configure a global RADIUS server host that the GGSN can use to authenticate and authorize users. You can configure additional RADIUS server communication at the GGSN global configuration level.

To globally configure RADIUS server communication on the router, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# radius-server host {hostname ip-address} [auth-port port-number] [acct-port port-number] [timeout seconds] [retransmit retries] [key string]	<p>Specifies the IP address or host name of the remote RADIUS server host. The following options are available:</p> <ul style="list-style-type: none"> • auth-port—Specifies the User Datagram Protocol (UDP) destination port for authentication requests. • acct-port—Specifies the UDP destination port for accounting requests. • timeout—Specifies the time interval (in the range 1 to 1000 seconds) that the router waits for the RADIUS server to reply before retransmitting. This setting overrides the global value of the radius-server timeout command. If no timeout value is specified, the global value is used. • retransmit—Specifies the number of times (in the range 1 to 100) a RADIUS request is re-sent to a server, if that server is not responding or is responding slowly. This setting overrides the global value of the radius-server retransmit command. • key—Specifies the authentication and encryption key used between the router and the RADIUS daemon running on this RADIUS server. This setting overrides the global value of the radius-server key command.
Step 2	Router(config)# radius-server key string	Specifies the shared secret text string used between the router and the vendor-proprietary RADIUS server. The router and the RADIUS server use this text string to encrypt passwords and exchange responses.

For more information about configuring RADIUS security, refer to the *Cisco IOS Security Configuration Guide* and *Cisco IOS Security Command Reference* publications. For an example, see the “[RADIUS Server Global Configuration Example](#)” section on page 10-31.



Note

Although you can configure the **radius-server host** command multiple times, the Cisco IOS software supports only one RADIUS server at the same IP address.

Configuring RADIUS Server Communication at the GGSN Configuration Level

To complete the security configuration for the GGSN, you must configure non-transparent access for each access point. When you configure security at the GGSN global configuration level, you can also configure RADIUS server communication for all access points or for a specific access point.

Configuring RADIUS at the GGSN global configuration level includes the following tasks:

- [Configuring Non-Transparent Access Mode, page 10-6](#) (Required)
- [Specifying an AAA Server Group for All Access Points, page 10-7](#) (Optional)
- [Specifying an AAA Server Group for a Particular Access Point, page 10-8](#) (Optional)
- [Configuring AAA Accounting Services at an Access Point, page 10-8](#) (Optional)

Configuring Non-Transparent Access Mode

To support RADIUS authentication on the GGSN, you must configure the GGSN access points for non-transparent access. You must configure non-transparent access for every access point at which you want to support RADIUS services. There is no way to globally specify the access mode.



Note

For GTP-PPP termination and GTP-PPP regeneration on the GGSN, transparent access mode is used to allow PPP to perform the appropriate AAA functions; however, you can still configure AAA server groups to specify the corresponding server groups for AAA support.

To configure non-transparent access for a GGSN access point, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# gprs access-point-list <i>list-name</i>	Specifies the access-point list name, and enters access-point list configuration mode.
Step 2	Router(config-ap-list)# access-point <i>access-point-index</i>	Specifies the number associated with an existing access point definition (or creates a new access point), and enters access point configuration mode.
Step 3	Router(config-access-point)# access-mode non-transparent	Specifies that the GGSN requests user authentication at the access point to a PDN.

For more information about configuring GGSN access points, see the [“Configuring Access Points on the GGSN”](#) section on page 7-7.

Specifying an AAA Server Group for All Access Points

After you have configured RADIUS server communication at the global level, you can configure a default AAA server group to be used by all GGSN access points.

To specify a default AAA server group for all GGSN access points, use the following command in global configuration mode:

Command	Purpose
<pre>Router(config)# gprs default aaa-group {authentication accounting} server-group</pre>	<p>Specifies a default AAA server group and assigns the type of AAA services to be supported by the server group for all access points on the GGSN, where:</p> <ul style="list-style-type: none"> • authentication—Assigns the selected server group for authentication services on all APNs. • accounting—Assigns the selected server group for accounting services on all APNs. • <i>server-group</i>—Specifies the name of an AAA server group to be used for AAA services on all APNs. <p>Note The name of the AAA server group that you specify must correspond to a server group that you configure using the aaa group server command.</p>

Specifying an AAA Server Group for a Particular Access Point

To override the default AAA server group configured for all access points, you can specify a different AAA server group for a particular access point. Or, if you choose not to configure a default AAA server group, you can specify an AAA server group at each access point.

To specify an AAA server group for a particular access point, use the following command in access-point configuration mode:

Command	Purpose
Router(config-access-point)# aaa-group { authentication accounting } <i>server-group</i>	<p>Specifies a default AAA server group and assigns the type of AAA services to be supported by the server group for a particular access point on the GGSN, where:</p> <ul style="list-style-type: none"> • authentication—Assigns the selected server group for authentication services on the APN. • accounting—Assigns the selected server group for accounting services on the APN. • <i>server-group</i>—Specifies the name of an AAA server group to be used for AAA services on the APN. <p>Note The name of the AAA server group that you specify must correspond to a server group that you configure using the aaa group server command.</p>

Configuring AAA Accounting Services at an Access Point

The Cisco GGSN has different defaults for enabling and disabling accounting services for transparent and non-transparent access points:

- If you configure an APN for non-transparent access using the **access-mode** command, the GGSN automatically enables accounting with authentication at the APN.
- If you configure an APN for transparent access, which is the default access mode, the GGSN automatically disables accounting at the APN.

Therefore, if you have configured a transparent access APN and you want to provide accounting at that APN, you need to configure the **aaa-accounting enable** command at the APN.

However, for accounting to occur, you also must complete the configuration by specifying the following other configuration elements on the GGSN:

- Enable AAA services by using the **aaa new-model** global configuration command.
- Define a server group with the IP addresses of the RADIUS servers in that group by using the **aaa group server** global configuration command.

- Configure the following AAA services:
 - AAA authentication using the **aaa authentication** global configuration command
 - AAA authorization using the **aaa authorization** global configuration command
 - AAA accounting using the **aaa accounting** global configuration command
- Assign the type of services that the AAA server group should provide. If you want the server group to only support accounting services, then you need to configure the server for accounting only. You can assign the AAA services to the AAA server groups either at the GGSN global configuration level by using the **gprs default aaa-group** command, or at the APN by using the **aaa-group** command.
- Configure the RADIUS servers by using the **radius-server host** command.

**Note**

For more information about AAA and RADIUS global configuration commands, see the *Cisco IOS Security Command Reference*.

To selectively disable accounting at specific APNs where you do not want that service, use the **aaa-accounting disable** access-point configuration command.

There is not a **no** form of this command.

Enabling and Disabling Accounting Services on an Access Point

The Cisco Systems GGSN has different defaults for enabling and disabling accounting services for transparent and non-transparent access points:

- If you configure an APN for non-transparent access using the **access-mode** command, the GGSN automatically enables accounting with authentication at the APN.
- If you configure an APN for transparent access, which is the default access mode, the GGSN automatically disables accounting at the APN.

To selectively disable accounting at specific APNs where you do not want that service, use the **aaa-accounting disable** access-point configuration command.

Configuring Interim Accounting on an Access Point

Using the **aaa-accounting interim** access-point configuration command, you can configure the GGSN to send Interim-Update Accounting requests to the AAA server when a routing area update (resulting in an SGSN change) or quality of service (QoS) change has occurred for a Packet Data Protocol (PDP) context. These changes are conveyed to the GGSN by an Update PDP Context request.

**Note**

Interim accounting support requires that accounting services be enabled for the APN and that the **aaa accounting update newinfo** global configuration command be configured.

To configure accounting services at an access point, use the following command in access-point configuration mode:

Command	Purpose
Router(config-access-point)# aaa-accounting [enable disable interim update]	<p>Configures accounting services on an access point on the GGSN, with the following options:</p> <ul style="list-style-type: none"> • enable—(Optional) Enables accounting services on an access point on the GGSN. • disable—(Optional) Disables accounting services on an access point on the GGSN. • interim update—(Optional) Enables interim accounting records to be sent to an accounting server when a routing area update (resulting in a serving GPRS support node [SGSN] change) or QoS change has occurred.

Configuring Additional RADIUS Services

This section describes how to configure RADIUS security services that the GGSN can use to authenticate and authorize users.

This section includes the following tasks:

- [Configuring RADIUS Attributes in Access Requests to the RADIUS Server, page 10-10](#)
- [Configuring the Vendor-Specific Attribute in Access Requests to the RADIUS Server, page 10-12](#)
- [Suppressing Attributes for RADIUS Authentication, page 10-14](#)
- [Obtaining DNS and NetBIOS Address Information from a RADIUS Server, page 10-16](#)
- [Configuring the RADIUS Packet of Disconnect, page 10-16](#)
- [Configuring the GGSN to Wait for a RADIUS Response, page 10-18](#)
- [Configuring Access to a RADIUS Server Using VRF, page 10-19](#)

Configuring RADIUS Attributes in Access Requests to the RADIUS Server

You configure the how the GGSN sends RADIUS attributes in access requests to the RADIUS server. This section includes the following tasks:

- [Configuring the CHAP Challenge, page 10-11](#)
- [Configuring the MSISDN IE, page 10-11](#)
- [Configuring the NAS-Identifier, page 10-11](#)
- [Configuring the Charging ID in the Acct-Session-ID Attribute, page 10-12](#)
- [Configuring the MSISDN in the User-Name Attribute, page 10-12](#)

Configuring the CHAP Challenge

To specify that the Challenge Handshake Authentication Protocol (CHAP) challenge always be included in the Challenge Attribute field (and not in the Authenticator field) in access requests to the RADIUS server, use the following command in global configuration mode:

Command	Purpose
Router(config)# gprs radius attribute chap-challenge	Specifies that the CHAP challenge is always included in the challenge attribute in a RADIUS request.



Note

When the **gprs radius attribute chap-challenge** command is configured, the CHAP challenge is always sent in the Challenge Attribute field of an access request to the RADIUS server and not in the Authenticator field. When the command is not configured, the CHAP challenge is sent in the Authenticator field unless the challenge exceeds 16 bytes, in which case, it is sent in the Challenge Attribute field of the Access Request.

Configuring the MSISDN IE

To specify that the first byte of the mobile station ISDN (MSISDN) information element (IE) is included in access requests to the RADIUS server, use the following command in global configuration mode:

Command	Purpose
Router(config)# gprs radius msisdn first-byte	Specifies that the first byte of the MSISDN IE is included in access requests.

Configuring the NAS-Identifier

You can configure the GGSN to send the network access server (NAS)-Identifier (RADIUS attribute 32) in access requests to a RADIUS server at a global or APN level. The APN-level configuration overrides the global-level configuration.

To specify that the NAS-Identifier be included in all access requests, use the following command in global configuration mode:

Command	Purpose
Router(config)# radius-server attribute 32 include-in-access-req format <i>format</i>	Specifies that the GGSN sends the RADIUS attribute 32 (NAS-Identifier) in access requests where <i>format</i> is a string sent in attribute 32 containing an IP address (%i), a hostname (%h), and a domain name (%d).

To disable this global configuration, use the **no** form of this command while in global configuration mode.

To specify that the NAS-Identifier be included in all access requests at an APN, use the following command in access point configuration mode:

Command	Purpose
Router(config-access-point)# radius attribute nas-id <i>format</i>	Specifies that the GGSN sends the NAS-Identifier in access requests at an APN where <i>format</i> is a string sent in attribute 32 containing an IP address (%i), a hostname (%h), and a domain name (%d).

To disable this APN configuration, use the **no** form of this command while in access point configuration mode.

Configuring the Charging ID in the Acct-Session-ID Attribute

To specify that the GGSN include the charging ID in the Acct-Session-ID (attribute 44) in accounting requests at an APN, use the following command in access-point configuration mode:

Command	Purpose
Router(config)# radius attribute acct-session-id charging-id	Specifies that the charging ID in the Acct-Session-ID (attribute 44) is included in accounting requests.

To disable this APN configuration, use the **no** form of this command while in access point configuration mode.

Configuring the MSISDN in the User-Name Attribute

To specify that the GGSN include the MSISDN in the User-Name attribute (attribute 1) in access requests at an APN, use the following command in access-point configuration mode:

Command	Purpose
Router(config)# radius attribute user-name msisdn	Specifies that the MSISDN is included in the User-Name (attribute 1) field in access requests.

To disable this APN configuration, use the **no** form of this command while in access point configuration mode.

Configuring the Vendor-Specific Attribute in Access Requests to the RADIUS Server

The Internet Engineering Task Force (IETF) draft standard specifies a method for communicating vendor-specific information to the RADIUS server by using the vendor-specific attribute (attribute 26). Vendor-specific attributes (VSAs) make a larger set of information available for communication by allowing vendors to support their own extended attributes not suitable for general use.

Table 10-1 lists and describes the Third Generation Partnership Project (3GPP) VSA sub-attributes that the GGSN can send in authentication and accounting requests to a RADIUS server when the attribute 26 is configured.

Table 10-1 3GPP VSA Sub-Attributes

Number	Vendor-Proprietary Attribute	Description
1	3GPP-IMSI	International Mobile Subscriber Identity (IMSI) number for a user. This sub-attribute can be suppressed using the radius attribute suppress imsi command.
2	3GPP-Charging-Id	Charging ID for this PDP context.
3	3GPP-PDP-Type	Type of PDP context (for example, IP or PPP).
4	3GPP-CG-Address	IP address of the current active charging gateway. If there is no current active charging gateway, GGSN sends 0.0.0.0.
5	3GPP-GPRS-QoS-Profile	QoS negotiated values. This sub-attribute can be suppressed using the radius attribute suppress qos command.
6	3GPP-SGSN-Address	IP address of the SGSN that is used by the GTP control plane for handling control messages. This address might be used to identify the public land mobile network (PLMN) to which the user is attached. This sub-attribute can be suppressed using the radius attribute suppress sgsn-address command.
7	3GPP-GGSN-Address	IP address of the GGSN that is used by the GTP control plane for the context establishment. This address is the same as the GGSN IP address used in G-CDRs.
8	3GPP-IMSI-MCC-MNC	Mobile country code (MCC) and mobile network code (MNC) extracted from the user's IMSI number (the first 5 or 6 digits depending on the IMSI). This sub-attribute requires that the MCC and MNC values that the GGSN uses be configured using the gprs mcc mnc global configuration command.
9	3GPP-GGSN-MCC-MNC	MCC and MNC of the network to which the GGSN belongs. This sub-attribute requires that the MCC and MNC values that the GGSN uses be configured using the gprs mcc mnc global configuration command.

Table 10-1 3GPP VSA Sub-Attributes (continued)

Number	Vendor-Proprietary Attribute	Description
12	3GPP-Selection-Mode	Selection mode for this PDP context received in the Create PDP Context request.
18	3GPP-SGSN-MCC-MNC	Encoding of the Routing Area Identity (RAI) MCC-MNC values.

To configure the GGSN to send and recognize VSAs as defined by RADIUS attribute 26, use the following command in global configuration mode:

Command	Purpose
<code>Router(config)#radius-server vsa send [accounting authentication]</code>	(Optional) Enables the GGSN to send and recognized VSAs as defined by RADIUS IETF attribute 26.

For more information on configuring the use of vendor-specific attributes, refer to the *Cisco IOS Security Configuration Guide* and *Cisco IOS Security Command Reference* publications.

Suppressing Attributes for RADIUS Authentication

You can configure the GGSN to suppress certain attributes in its access requests to a RADIUS server. The following sections describe the attributes you can suppress and how to do so.

The following topics are included in this section:

- [Suppressing the MSISDN Number for RADIUS Authentication, page 10-14](#)
- [Suppressing the 3GPP-IMSI VSA Sub-Attribute for RADIUS Authentication, page 10-15](#)
- [Suppressing the 3GPP-GPRS-QoS Profile VSA Sub-Attribute for RADIUS Authentication, page 10-15](#)
- [Suppressing the 3GPP-GPRS-SGSN-Address VSA Sub-Attribute for RADIUS Authentication, page 10-16](#)

Suppressing the MSISDN Number for RADIUS Authentication

Some countries have privacy laws that prohibit service providers from identifying the MSISDN number of mobile stations in authentication requests. Use the **msisdn suppression** command to specify a value that the GGSN sends instead of the MSISDN number in its authentication requests to a RADIUS server. If no value is configured, then no number is sent to the RADIUS server.

To use the **msisdn suppression** command, you must configure a RADIUS server either globally or at the access point and specify non-transparent access mode.

To specify that the GGSN override or suppress the MSISDN number in its access-requests sent to the RADIUS server, use the following command in access-point configuration mode:

Command	Purpose
Router(config-access-point)# msisdn suppression [value]	(Optional) Specifies that the GGSN overrides the MSISDN number with a preconfigured value in its access requests.

To disable this APN configuration, use the **no** form of this command while in access point configuration mode.

Suppressing the 3GPP-IMSI VSA Sub-Attribute for RADIUS Authentication

To configure the GGSN to suppress the Third Generation Partnership Project (3GPP) vendor-specific attribute (VSA) 3GPP-International Mobile Subscriber Identity (3GPP-IMSI) number in its authentication and accounting requests to a RADIUS server, use the **radius attribute suppress imsi** access point configuration command.

To configure the GGSN to suppress the 3GPP VSA 3GPP-IMSI number in its authentication and accounting requests to a RADIUS server, use the following command in access-point configuration mode:

Command	Purpose
Router(config-access-point)# radius attribute suppress imsi	(Optional) Configures the GGSN to suppress the 3GPP-IMSI number in its authentication and accounting requests to a RADIUS server.

To disable this APN configuration, use the **no** form of this command while in access point configuration mode.

Suppressing the 3GPP-GPRS-QoS Profile VSA Sub-Attribute for RADIUS Authentication

To configure the GGSN to suppress the 3GPP-GPRS-QoS Profile in its authentication and accounting requests to a RADIUS server, use the **radius attribute suppress qos** access point configuration command.

To configure the GGSN to suppress the 3GPP-GPRS-QoS Profile in its authentication and accounting requests to a RADIUS server, use the following command in access-point configuration mode:

Command	Purpose
Router(config-access-point)# radius attribute suppress qos	(Optional) Specifies that the GGSN suppresses the 3GPP-GPRS-QoS Profile in its authentication and accounting requests to a RADIUS server.

Suppressing the 3GPP-GPRS-SGSN-Address VSA Sub-Attribute for RADIUS Authentication

To configure the GGSN to suppress the 3GPP-GPRS-SGSN-Address in its authentication and accounting requests to a RADIUS server, use the **radius attribute suppress sgsn-address** access point configuration command.

To specify that the GGSN suppress the 3GPP-GPRS-SGSN-Address in its authentication and accounting requests to a RADIUS server, use the following command in access-point configuration mode:

Command	Purpose
Router(config-access-point)# radius attribute suppress sgsn-address	(Optional) Specifies that the GGSN suppresses the 3GPP-GPRS-SGSN-Address in its requests.

Obtaining DNS and NetBIOS Address Information from a RADIUS Server

To obtain Domain Name System (DNS) address and Network Basic Input/Output System (NetBIOS) address information from a RADIUS server, configure the GGSN to send and recognize VSAs as defined by RADIUS attribute 26 using the following command in global configuration mode:

Command	Purpose
Router(config)# radius-server vsa send [accounting authentication]	(Optional) Enables the GGSN to send and recognize VSAs as defined by RADIUS IETF attribute 26.



Note

For the DNS and NetBIOS address information to be sent to an MS, the dynamic address allocation method using an IP address pool supplied by a RADIUS server must be configured for the access point by using the **ip-address-pool radius-client** command. For more information about configuring an access point, see the [“Configuring Access Points on the GGSN” section on page 7-7](#).

Configuring the RADIUS Packet of Disconnect

The RADIUS Packet of Disconnect (POD) feature is a method for terminating a user session after the session has been established. The POD is a RADIUS Disconnect-Req packet and is intended to be used in situations when an authenticating agent server wants to disconnect a user after a session has been accepted by the RADIUS access-accept packet. For example, in the case of pre-paid billing, a typical use of this feature would be for the pre-paid billing server to send a POD when the quota expires for a pre-paid user.

Upon receiving a POD, the GGSN performs the following actions:

- Identifies the PDP context for which the POD was generated by the attribute information present in the POD. The VSA sub-attributes 3GPP-IMSI and 3GPP-NSAPI uniquely identify a PDP context, and the presence of these sub-attributes in a POD also identifies that the POD is for a GPRS user session.
- Sends a Delete PDP Context request to the SGSN.

- Sends a Disconnect ACK or Disconnect NAK to the device that generated the POD. The GGSN sends a Disconnect ACK when it is able to terminate a user session and sends a Disconnect NAK when it is unable to terminate a user session. The Disconnect ACK/NAK requests are RADIUS packets that contain no attributes.

**Note**

For the POD feature to function properly on the GGSN, ensure that the IMSI attribute has not been suppressed using the **radius attribute suppress imsi** command.

To enable POD support on the GGSN, use the following command in global configuration mode:

Command	Purpose
<pre>Router(config)# aaa pod server [port port-number] [auth-type {any all session-key}] server-key [encryption-type] string</pre>	<p>Enables inbound user sessions to be disconnected when specific session attributes are presented.</p> <ul style="list-style-type: none"> • port port-number—(Optional) Network access server User Datagram Protocol (UDP) port to use for POD requests. Default value is 1700. This is the port on which GGSN listens for the POD requests. • auth-type—(Optional) Type of authorization required for disconnecting sessions. <ul style="list-style-type: none"> – any—Session that matches all of the attributes sent in the POD packet is disconnected. The POD packet may contain one or more of four key attributes (user-name, framed-IP-address, session-ID, and session-key). – all—Only a session that matches all four key attributes is disconnected. All is the default. – session-key—Session with a matching session-key attribute is disconnected. All other attributes are ignored. <p> Note When configuring a POD on the GGSN, we recommend that you do not configure the auth-type keyword option.</p> <ul style="list-style-type: none"> • server-key—Configures the shared-secret text string. • encryption-type—(Optional) Single-digit number that defines whether the text immediately following is encrypted, and, if so, what type of encryption is used. Defined encryption types are 0, which means that the text immediately following is not encrypted, and 7, which means that the text is encrypted using an encryption algorithm defined by Cisco. • string—Shared-secret text string that is shared between the network access server and the client workstation. This shared-secret string must be the same on both systems.

Configuring the GGSN to Wait for a RADIUS Response

Use the **gtp response-message wait-accounting** command to configure the GGSN to wait for a RADIUS accounting response from the RADIUS accounting server before sending a Create PDP Context response to the SGSN.

If the GGSN does not receive a response from the RADIUS accounting server when you have configured the **gtp response-message wait-accounting** command, it rejects the PDP context request.

When broadcast accounting is used (accounting requests are sent to multiple RADIUS servers), if a RADIUS server responds with an accounting response, the GGSN sends a create PDP context response and does not wait for the other RADIUS servers to respond.

The GGSN supports configuration of RADIUS response message waiting at both the global and access-point configuration levels. You can minimize your configuration by specifying the configuration that you want to support across most APNs, at the global configuration level. Then, at the access-point configuration level, you can selectively modify the behavior that you want to support at a particular APN. Therefore, at the APN configuration level, you can override the global configuration of RADIUS response message waiting.

To configure the GGSN to wait for a RADIUS accounting response as the default behavior for all APNs, use the **gprs gtp response-message wait-accounting** global configuration command. To disable this behavior for a particular APN, use the **no gtp response-message wait-accounting** access-point configuration command.

To verify whether RADIUS response message waiting is enabled or disabled at an APN, you can use the **show gprs access-point** command and observe the value reported in the `wait_accounting` output field.

To configure the GGSN to wait for a RADIUS accounting response globally, use the following command in global configuration mode:

Command	Purpose
Router(config)# gprs gtp response-message wait-accounting	Configures the GGSN to wait for a RADIUS accounting response before sending a Create PDP Context response to the SGSN, for Create PDP Context requests received across all access points.

To configure the GGSN to wait for a RADIUS accounting response for a particular access point, use the following command in access-point configuration mode:

Command	Purpose
Router(config-access-point)# gtp response-message wait-accounting	Configures the GGSN to wait for a RADIUS accounting response before sending a Create PDP Context response to the SGSN, for Create PDP Context requests received at a particular access point.

Configuring Access to a RADIUS Server Using VRF

The Cisco IOS GGSN software supports access to a RADIUS server using VRF. This Cisco IOS software feature is called *Per VRF AAA* and using this feature, Internet service providers (ISPs) can partition AAA services based on VRF. This permits the GGSN to communicate directly with the customer RADIUS server associated with the customer Virtual Private Network (VPN) without having to go through a RADIUS proxy. Thus, ISPs can scale their VPN offerings more efficiently because they no longer need to proxy AAA to provide their customers the flexibility demanded.

To support this configuration, AAA must be VRF aware. ISPs must define multiple instances of the same operational parameters—such as AAA server groups, method lists, system accounting, and protocol-specific parameters—and secure the parameters to the VRF partitions.

**Note**

VRF is not supported on the Cisco 7600 Supervisor II / MSFC2; therefore, if using the Supervisor II, you must tunnel encapsulated VRF traffic through the Supervisor via a GRE tunnel between the GGSN to RADIUS server. For more information on configuration a GRE tunnel, see [“Configuring Access to a RADIUS Server With a Tunnel”](#) section on page 10-25.

The Cisco 7600 Sup720 supports VRF.

If an AAA configuration, such as a method list, is uniquely defined many times, the specification of an AAA server that is based on IP addresses and port numbers might create an overlapping of private addresses between VRFs. Securing AAA method lists to a VRF can be accomplished from one or more of the following sources:

- Virtual Template—Used as a generic interface configuration.
- Service Provider AAA server—Used to associate a remote user with a specific VPN based on the domain name or Dialed Number Identification Service (DNIS). The server then provides the VPN-specific configuration for the virtual access interface, which includes the IP address and port number of the customer AAA server.
- Customer VPN AAA server—Used to authenticate the remote user and to provide user-specific configurations for the virtual access interface.

**Note**

Global AAA accounting configurations and some AAA protocol-specific parameters cannot be logically grouped under the Virtual Template configuration.

When configuring the Per VRF feature, keep in mind the following:

- To prevent possible overlapping of private addresses between VRFs, AAA servers must be defined in a single global pool that is to be used in the server groups.
- Servers can no longer be uniquely identified by IP addresses and port numbers.

- “Private” servers (servers with private addresses within the default server group that contains all the servers) can be defined within the server group and remain hidden from other groups. The list of servers in server groups includes references to the hosts in the global configuration as well as the definitions of private servers.



Note If private server parameters are not specified, global configurations are used. If global configurations are not specified, default values are used.

- All server operational parameters can be configured per host, per server group, or globally. Per-host configurations have precedence over per-server group configurations. Per-server group configurations have precedence over global configurations.



Note

For complete information on configuring access to a RADIUS server using VRF, refer to the *Per VRF AAA* feature module.

This section describes configuring and establishing access to a private RADIUS server using VRF. For global RADIUS services, ensure that you have configured a globally located server.

To configure access to a RADIUS server using VRF, complete the following tasks:

- [Enabling AAA Globally, page 10-20](#) (Required)
- [Configuring a VRF-Aware Private RADIUS Server Group, page 10-21](#) (Required)
- [Configuring Authentication, Authorization, and Accounting Using Named Method Lists, page 10-22](#) (Required)
- [Configuring a VRF Routing Table, page 10-22](#) (Required)
- [Configuring VRF on an Interface, page 10-22](#) (Required)
- [Configuring VRF Under an Access Point for Access to the Private RADIUS Server, page 10-23](#) (Required)
- [Configuring a Route to the RADIUS Server Using VRF, page 10-27](#) (Optional)

Enabling AAA Globally

If AAA has not been enabled globally on the GGSN, you will need to enable it before configuring access to a private RADIUS server via VRF.

To enable AAA globally, use the following command in global configuration mode:

	Command	Purpose
Step 1	Router(config)# aaa new-model	Enables AAA globally.

Configuring a VRF-Aware Private RADIUS Server Group

To configure private server operational parameters, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# aaa group server radius <i>group-name</i>	Groups different RADIUS server hosts into distinct lists and distinct methods. <ul style="list-style-type: none"> • <i>group-name</i>—Character string used to name the group of servers.
Step 2	Router(config-sg-radius)# server-private <i>ip-address</i> auth-port <i>port_num</i> acct-port <i>port_num</i> key <i>string</i>	Configures the IP address of the private RADIUS server for the group server. <ul style="list-style-type: none"> • <i>ip-address</i>—Specifies the IP address of the private RADIUS server host. • auth-port <i>port_num</i>—Specifies a port solely for authentication. • acct-port <i>port_num</i>—Specifies a port solely for accounting. • <i>string</i>—(Optional) Specifies the authentication and encryption key for all RADIUS communications between the router and the RADIUS server. <p>Note If private server parameters are not specified, global configurations are used. If global configurations are not specified, default values are used.</p>
Step 3	Router(config-sg-radius)# ip vrf forwarding <i>vrf-name</i>	Configures the VRF reference of the AAA RADIUS server group. <ul style="list-style-type: none"> • <i>vrf-name</i>—Name assigned to a VRF.

Configuring Authentication, Authorization, and Accounting Using Named Method Lists

To configure AAA using named method lists, perform the following tasks, beginning in global configuration mode:

Step 1	Router(config)# aaa authentication ppp {default list-name} method1 [method2...]	Creates a local authentication method list, with the following options: <ul style="list-style-type: none"> • default—Specifies that the authentication methods that follow this argument are the default list of authentication methods when a user logs in to the router. • method—Specifies a valid AAA authentication method for PPP. For example, group RADIUS enables global RADIUS authentication.
Step 2	Router(config)# aaa authorization {auth-proxy network exec commands level reverse-access} {default list-name} [method1 [method2...]]	Creates an authorization method list for a particular authorization type and enables authorization.
Step 3	Router(config)# aaa accounting {system default [vrf vrf-name] network {default none start-stop stop-only wait-start} group group-name	Enables AAA accounting of requested services for billing or security purposes when you use RADIUS.

Configuring a VRF Routing Table

To configure a VRF routing table on the GGSN for access to the private RADIUS server, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# ip vrf vrf-name	Configures a VRF routing table, and enters VRF configuration mode.
Step 2	Router(config-vrf)# rd route-distinguisher	Creates routing and forwarding tables for a VRF and specifies the default route distinguisher for a VPN.

Configuring VRF on an Interface

To access the private RADIUS server, VRF must be configured on the interface to the server.

On the Cisco 7600 series router platform, this interface is a logical one (on which IEEE 802.1Q-encapsulation has been configured) to a Layer 3 routed VLAN configured on the supervisor engine.

For more information about required VLANs on the supervisor engine, see the [“Platform Prerequisites” section on page 2-2](#).

For more information about configuring interfaces, refer to the *Cisco IOS Interface Configuration Guide* and the *Cisco IOS Interface Command Reference*.

Configuring 802.1Q-Encapsulated Subinterfaces

To configure a subinterface that supports IEEE 802.1Q encapsulation to the associated VLAN on the supervisor engine, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# interface gigabitethernet <i>slot/port.subinterface-number</i>	Specifies the subinterface on which IEEE 802.1Q will be used.
Step 2	Router(config-if)# encapsulation dot1q <i>vlanid</i>	Defines the encapsulation format as IEEE 802.1Q (dot1q), and specifies the VLAN identifier.
Step 3	Router(config-if)# ip address <i>ip-address mask</i>	Sets a primary IP address for an interface.

Configuring VRF Under an Access Point for Access to the Private RADIUS Server

After you have completed the prerequisite configuration tasks, you can configure access to a RADIUS server with a tunnel or without a tunnel.

VRF is not supported on the Cisco 7600 Supervisor II / MSFC2; therefore, if using the Supervisor II, you must tunnel encapsulated VRF traffic through the Supervisor via a GRE tunnel between the GGSN to RADIUS server.

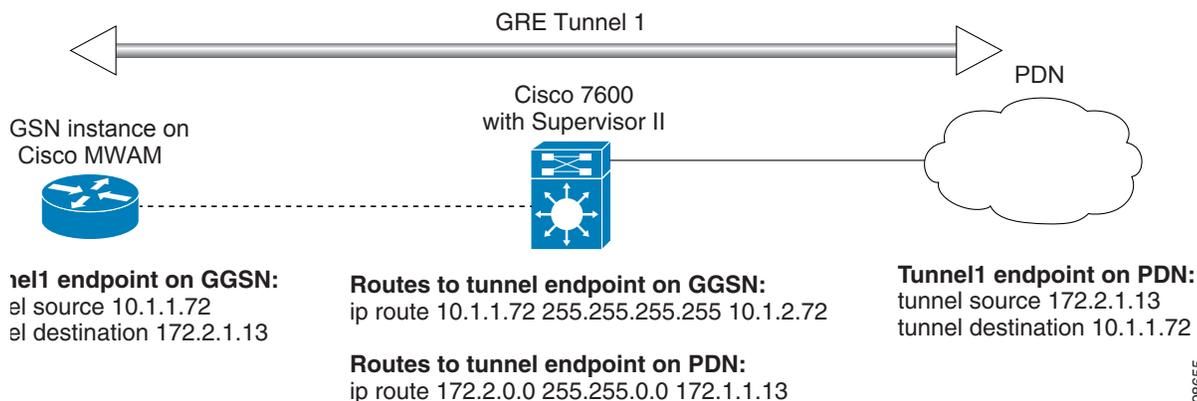


Note

The Cisco 7600 Sup720 supports VRF.

Figure 10-1 is a logical view of a GRE tunnel configured between the VRF-aware GGSN and RADIUS server, which tunnels the encapsulated VRF traffic through the VRF-unaware Supervisor II / MSFC2.

Figure 10-1 GRE Tunnel Configuration from the GGSN to RADIUS Server through the Cisco 7600 Supervisor/MSFC2



The following sections describe the different methods you can use to configure access a RADIUS server:

- [Configuring Access to a RADIUS Server Without a Tunnel](#)
- [Configuring Access to a RADIUS Server With a Tunnel](#)

Configuring Access to a RADIUS Server Without a Tunnel

To configure access to the RADIUS server without a tunnel, you need to configure the **vrf** access point configuration command.



Note

The Cisco 7600 Supervisor/MSFC2 does not support VRR; therefore, you must tunnel VRF traffic through the Supervisor via a GRE tunnel as described in the “[Configuring Access to a RADIUS Server With a Tunnel](#)” section on page 10-25.

To configure access to a RADIUS server in the GPRS access point list, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# gprs access-point-list <i>list-name</i>	Specifies a name for a new access point list, or references the name of the existing access point list, and enters access-point list configuration mode.
Step 2	Router(config-ap-list)# access-point <i>access-point-index</i>	Specifies an index number for a new access point definition, or references an existing access point definition, and enters access point configuration mode.
Step 3	Router(config-access-point)# access-point-name <i>apn-name</i>	Specifies the network (or domain) name for a PDN that users can access from the GGSN at a defined access point. Note The <i>apn-name</i> must match the APN that has been provisioned at the MS, HLR, and DNS server.
Step 4	Router(config-access-point)# aaa-group authentication <i>server-group</i>	Specifies a default AAA server group and assigns the type of AAA services to be supported by the server group for a particular access point on the GGSN, where: <ul style="list-style-type: none"> • authentication—Assigns the selected server group for authentication services on the APN. • <i>server-group</i>—Specifies the name of a AAA server group to be used for AAA services on the APN. Note The name of the AAA server group that you specify must correspond to a server group that you configure using the aaa group server command.
Step 5	Router(config-access-point)# access-mode non-transparent	Specifies for the GGSN to act as a proxy for authentication.
Step 6	Router(config-access-point)# ip-address-pool radius-client	Specifies for the RADIUS server to provide the IP address pool for the current access point. Note If you are using a dynamic address allocation method, then you must configure this command according to the appropriate IP address pool source.

	Command	Purpose
Step 7	Router(config-access-point)# vrf <i>vrf-name</i>	Configures VPN routing and forwarding at a GGSN access point, and associates the access point with a particular VRF instance. Note The <i>vrf-name</i> argument should match the name of the VRF that you configured using the ip vrf command in the “Configuring Authentication, Authorization, and Accounting Using Named Method Lists” section on page 10-22.
Step 8	Router(config-access-point)# exit	Exits access point configuration mode.

Configuring Access to a RADIUS Server With a Tunnel

If you have only a single interface to a RADIUS server from which you need to access one or more private RADIUS servers, you can configure an IP tunnel to access those private servers.

To configure access to the RADIUS server using a tunnel, perform the following tasks:

- [Configuring the Private RADIUS Server Access Point](#) (Required)
- [Configuring the IP Tunnel](#) (Required)

Configuring the Private RADIUS Server Access Point

To configure access to a private RADIUS server in the GPRS access point list, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# gprs access-point-list <i>list-name</i>	Specifies a name for a new access point list, or references the name of the existing access point list, and enters access-point list configuration mode.
Step 2	Router(config-ap-list)# access-point <i>access-point-index</i>	Specifies an index number for a new access point definition, or references an existing access point definition, and enters access point configuration mode.
Step 3	Router(config-access-point)# access-point name <i>apn-name</i>	Specifies the access point network ID, which is commonly an Internet domain name. Note The <i>apn-name</i> must match the APN that has been provisioned at the mobile station (MS), home location register (HLR), and DNS server.
Step 4	Router(config-access-point)# access-mode { transparent non-transparent }	(Optional) Specifies whether the GGSN requests user authentication at the access point. The available options are: <ul style="list-style-type: none"> • transparent—No security authorization or authentication is requested by the GGSN for this access point. This is the default value. • non-transparent—GGSN acts as a proxy for authenticating.

	Command	Purpose
Step 5	Router(config-access-point)# access-type real	Specifies an APN type that corresponds to an interface to an external network on the GGSN. Real is the default value.
Step 6	Router(config-access-point)# ip-address-pool { dhcp-proxy-client radius-client local pool-name disable }	(Optional) Specifies a dynamic address allocation method using IP address pools for the current access point. The available options are: <ul style="list-style-type: none"> • dhcp-proxy-client—DHCP server provides the IP address pool. • radius-client—RADIUS server provides the IP address pool. • local—Specifies that a local pool provides the IP address. This option requires that the address range be configured using the aggregate access point configuration command and that a local pool has been configured using the ip local pool global configuration command. • disable—Turns off dynamic address allocation. Note If you are using a dynamic address allocation method, then you must configure this command according to the appropriate IP address pool source.
Step 7	Router(config-access-point)# vrf vrf-name	Configures VPN routing and forwarding at a GGSN access point and associates the access point with a particular VRF instance.
Step 8	Router(config-access-point)# exit	Exits access point configuration mode.

Configuring the IP Tunnel

When you configure a tunnel, you might consider using loopback interfaces as the tunnel endpoints instead of real interfaces because loopback interfaces are always up.

To configure an IP tunnel to a private network, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# interface tunnel number	Configures a logical tunnel interface number.
Step 2	Router(config-if)# ip vrf forwarding vrf-name	Associates a VRF instance with the interface.
Step 3	Router(config-if)# ip address ip-address mask [secondary]	Specifies an IP address for the tunnel interface. Note This IP address is not used in any other part of the GGSN configuration.
Step 4	Router(config-if)# tunnel source {ip-address type number}	Specifies the IP address (or interface type and port or card number) of the interface to the RADIUS server or a loopback interface.
Step 5	Router(config-if)# tunnel destination {hostname ip-address}	Specifies IP address (or host name) of the private network that you can access from this tunnel.

Configuring a Route to the RADIUS Server Using VRF

Be sure a route exists between the VRF instance and the RADIUS server. You can verify connectivity by using the **ping** command from the VRF to the RADIUS server. To configure a route, you can use a static route or a routing protocol.

Configuring a Static Route Using VRF

To configure a static route using, use the following command, beginning in global configuration mode:

Command	Purpose
<pre>Router(config)# ip route vrf vrf-name prefix mask [next-hop-address] [interface {interface-number}] [global] [distance] [permanent] [tag tag]</pre>	<p>Configures a static IP route, where:</p> <ul style="list-style-type: none"> • <i>vrf-name</i>—Specifies the name of the VPN routing/forwarding (VRF) instance for the static route. • <i>prefix</i>—Specifies the IP route prefix for the destination. • <i>mask</i>—Specifies the prefix mask for the destination. • <i>next-hop-address</i>—Specifies the IP address of the next hop that can be used to reach the destination network. • <i>interface interface-number</i>—Specifies the network interface type and interface number that can be used to reach the destination network. • global—Specifies that the given next hop address is in the non-VRF routing table. • <i>distance</i>—Specifies an administrative distance for the route. • permanent—Specifies that the route will not be removed, even if the interface shuts down. • tag tag—Specifies a tag value that can be used as a “match” value for controlling redistribution via route maps.

Verifying a Static Route Using VRF

To verify the static VRF route that you configured, use the **show ip route vrf** privileged EXEC command as shown in the following example:

```
GGSN# show ip route vrf vpn1 static

      172.16.0.0/16 is subnetted, 1 subnets
C       172.16.0.1 is directly connected, Ethernet5/1
C       10.100.0.3/8 is directly connected, Virtual-Access5
```

Configuring an OSPF Route Using VRF

To configure an OSPF route using VRF, use the following command, beginning in global configuration mode:

Command	Purpose
Router(config)# router ospf <i>process-id</i> [vrf <i>vrf-name</i>]	<p>Enables OSPF routing, and enters router configuration mode, where,</p> <ul style="list-style-type: none"> • <i>process-id</i>—Specifies an internally used identification parameter for an OSPF routing process. The <i>process-id</i> is locally assigned and can be any positive integer. A unique value is assigned for each OSPF routing process. • vrf <i>vrf-name</i>—Specifies the name of the VPN routing/forwarding instance.

Securing the GGSN Mobile (Gn) Interface

The following features provide additional security for the GGSN mobile interface against attacks that can lead to illegal access to a network or even network downtime: address verification and mobile-to-mobile traffic redirection. The following tasks are necessary for configuring these features:

- [Configuring Address Verification, page 10-28](#)
- [Configuring Mobile-to-Mobile Traffic Redirection, page 10-29](#)
- [Redirecting All Traffic, page 10-30](#)

Configuring Address Verification

Use the **security verify source** (IPv4 address verification) and **ipv6 security verify source** (IPv6 address verification) access point configuration command to configure the GGSN to verify the source IP address of an upstream TPDU against the address previously assigned to an MS.

When the **security verify source** or **ipv6 security verify source** commands are configured on an APN, the GGSN verifies the source address of a TPDU before GTP will accept and forward it. If the GGSN determines that the address differs from that previously assigned to the MS, it drops the TPDU and regards it as an illegal packet in its PDP context and APN. Configuring the **security verify source** and **ipv6 security verify source** access point configuration commands protects the GGSN from faked user identities.

Use the **security verify destination** access point configuration command (IPv4 address verification only) to have the GGSN verify the destination addresses of upstream TPDU against global lists of PLMN addresses specified using the **gprs plmn ip address** command. If the GGSN determines that a destination address of a TPDU is within the range of a list of addresses, it drops the TPDU. If it determines that the TPDU contains a destination address that does not fall within the range of a list, it forwards the TPDU to its final destination.



Note

The **security verify destination** command is not applied to APNs using VRF or IPv6 address verification. In addition, the verification of destination addresses does not apply to GTP-PPP regeneration or GTP-PPP with L2TP.

To configure IPv4 address verification on an access point, use the following command in access-point configuration mode:

Command	Purpose
Router(config-access-point)# security verify {source destination}	(Optional) Specifies that the GGSN verify the source or destination address in TPDU received from a Gn interface.

**Note**

Both the verification of IPv4 destination addresses and source addresses can be configured on an APN.

To configure IPv6 source address verification on an access point, use the following command in access-point configuration mode:

Command	Purpose
Router(config-access-point)# ipv6 security verify source	(Optional) Configures the GGSN to verify the IPv6 source address of an upstream TPDU against the address previously assigned to an MS, use the ipv6 security verify source command in access-point configuration mode.

Configuring Mobile-to-Mobile Traffic Redirection

Mobile-to-mobile traffic enters and exits through a Gn interface. Therefore, it is switched by the GGSN without ever going through a Gi interface on the network side. Because of this, firewalls deployed on the network side of a GGSN do not have an opportunity to verify this level of traffic.

Use the **redirect intermobile ip** access-point command to redirect mobile-to-mobile traffic to an external device (such as an external firewall) for verification.

Command	Purpose
Router(config-access-point)# redirect intermobile ip ip address	(Optional) Configures the GGSN to redirect all IPv4 mobile-to-mobile traffic to an external device.
Router(config-access-point)# ipv6 redirect intermobile ipv6-address	(Optional) Configures the GGSN to redirect all IPv6 mobile-to-mobile traffic to an external IPv6 device.

**Note**

On the Cisco 7600 series internet router platform, the mobile-to-mobile redirection feature requires that policy based routing (PBR) is configured on the supervisor engine and incoming VLAN interface from the Cisco MWAM, and that the next hop to route the packets that match the criteria is set using the **set ip next-hop** command.

**Note**

Redirection of intermobile traffic does not occur on an ingress APN unless the TPDU's are exiting the same APN. In addition, redirection of TPDU's tunneled by L2TP from the ingress APN to the LNS of the PDN does not occur.

Redirecting All Traffic

The redirect all traffic feature enables you to do the following:

- Redirect all packets to a specified destination regardless of whether the destination address belongs to a mobile station (MS) on the same GGSN or not. If redirecting traffic using the Mobile-to-Mobile Redirect feature, only packets for which the destination address belongs to an MS that is active on the same GGSN can be redirected. If the receiving MS has no PDP context in the GGSN where the sending MS PDP context is created, the packets are dropped.
- Redirect all traffic to a specific destination when aggregate routes are configured.

To redirect all traffic to a specific IP address, issue the following command while in access-point configuration mode:

Command	Purpose
Router(config-access-point)# redirect all ip <i>ip address</i>	(Optional) Configures the GGSN to redirect all IPv4 traffic to an external device.
Router(config-access-point)# ipv6 redirect all intermobile <i>ipv6-address</i>	(Optional) Configures the GGSN to redirect all IPv6 traffic to an external IPv6 device.

Configuration Examples

This section includes the following configuration examples for security on the GGSN:

- [AAA Security Configuration Example, page 10-30](#)
- [RADIUS Server Global Configuration Example, page 10-31](#)
- [RADIUS Server Group Configuration Example, page 10-31](#)
- [RADIUS Response Message Configuration Example, page 10-33](#)
- [Address Verification and Mobile-to-Mobile Traffic Redirection Example, page 10-34](#)

AAA Security Configuration Example

The following example shows how to enable AAA security globally on the router and how to specify global RADIUS authentication and authorization:

```
! Enables AAA globally
aaa new-model
!
! Creates a local authentication list for use on
! serial interfaces running PPP using RADIUS
!
aaa authentication ppp abc group abc
```

```

!
! Enables authorization and creates an authorization
! method list for all network-related service requests
! and enables authorization using a RADIUS server
!
aaa authorization network network abc group abc

```

For more information about configuring AAA, refer to the *Cisco IOS Security Configuration Guide* and *Cisco IOS Security Command Reference* publications.

RADIUS Server Global Configuration Example

The following example shows how to globally configure RADIUS server communication on the router:

```

! Specifies a global RADIUS server host at IP address 10.100.0.2
! Port 1645 is destination port for authentication requests
! Port 1646 is the destination port for accounting requests
! Specifies the key "abc" for this radius host only
!
radius-server host 10.100.0.2 auth-port 1645 acct-port 1646 key abc
!
! Sets the authentication and encryption key to mykey for all
! RADIUS communications between the router and the RADIUS daemon
!
radius-server key mykey

```



Note

Although you can configure the **radius-server host** command multiple times, the Cisco IOS software supports only one RADIUS server at the same IP address.

For more information about configuring RADIUS security, refer to the *Cisco IOS Security Configuration Guide* and *Cisco IOS Security Command Reference* publications.

RADIUS Server Group Configuration Example

The following configuration example defines four AAA server groups on the GGSN: abc, abc1, abc2, and abc3, shown by the **aaa group server** commands.

Using the **gprs default aaa-group** command, two of these server groups are globally defined as default server groups: abc2 for authentication, and abc3 for accounting.

At access-point 1, which is enabled for authentication, the default global authentication server group of abc2 is overridden and the server group named abc is designated to provide authentication services on the APN. Notice that accounting services are not explicitly configured at that access point, but are automatically enabled because authentication is enabled. Because there is a globally defined accounting server-group defined, the server named abc3 will be used for accounting services.

At access-point 4, which is enabled for accounting using the **aaa-accounting enable** command, the default accounting server group of abc3 is overridden and the server group named abc1 is designated to provide accounting services on the APN.

Access-point 5 does not support any AAA services because it is configured for transparent access mode.

```

! Enables AAA globally
!
aaa new-model
!
! Defines AAA server groups

```

```

!
aaa group server radius abc
  server 10.2.3.4 auth-port 1645 acct-port 1646
  server 10.6.7.8 auth-port 1645 acct-port 1646
aaa group server radius abc1
  server 10.10.0.1 auth-port 1645 acct-port 1646
aaa group server radius abc2
  server 10.2.3.4 auth-port 1645 acct-port 1646
  server 10.10.0.1 auth-port 1645 acct-port 1646
aaa group server abc3
  server 10.6.7.8 auth-port 1645 acct-port 1646
  server 10.10.0.1 auth-port 1645 acct-port 1646
!
! Configures AAA authentication
! and authorization
!
aaa authentication ppp abc group abc
aaa authentication ppp abc2 group abc2
aaa authorization network abc group abc
aaa accounting network abc start-stop group abc
aaa accounting network abc1 start-stop group abc1
aaa accounting network abc2 start-stop group abc2
aaa accounting network abc3 start-stop group abc3
!
gprs access-point-list gprs
  access-point 1
    access-mode non-transparent
    access-point-name www.pdn1.com
  !
  ! Specifies a RADIUS server group
  ! for use by the GGSN to authenticate
  ! mobile users at this access point
  !
  aaa-group authentication abc
  !
  access-point 4
    access-point-name www.pdn2.com
  !
  ! Enables AAA accounting services
  !
  aaa-accounting enable
  !
  ! Specifies a RADIUS server group
  ! for use by the GGSN for accounting
  ! services at this access point
  !
  aaa-group accounting abc1
  !
  access-point 5
    access-point-name www.pdn3.com
  !
  ! Configures default AAA server
  ! groups for the GGSN for authentication
  ! and accounting services
  !
gprs default aaa-group authentication abc2
gprs default aaa-group accounting abc3
!
! Configures global RADIUS server hosts
! and specifies destination ports for
! authentication and accounting requests
!
radius-server host 10.2.3.4 auth-port 1645 acct-port 1646 non-standard
radius-server host 10.6.7.8 auth-port 1645 acct-port 1646 non-standard

```

```
radius-server host 10.10.0.1 auth-port 1645 acct-port 1646 non-standard
radius-server key ggsntel
```

**Note**

Although you can configure the **radius-server host** command multiple times, the Cisco IOS software supports only one RADIUS server at the same IP address.

RADIUS Response Message Configuration Example

The following example globally configures the GGSN to wait for a RADIUS accounting response from the RADIUS server before sending a Create PDP Context response to the SGSN. The GGSN waits for a response for PDP context requests received across all access points, except access-point 1. RADIUS response message waiting has been overridden at access-point 1 by using the **no gtp response-message wait-accounting** command:

```
! Enables AAA globally
!
aaa new-model
!
! Defines AAA server group
!
aaa group server radius abc
  server 10.2.3.4 auth-port 1645 acct-port 1646
  server 10.6.7.8 auth-port 1645 acct-port 1646
!
! Configures AAA authentication
! and authorization
!
aaa authentication ppp abc group abc
aaa authorization network abc group abc
aaa accounting network abc start-stop group abc
!
gprs access-point-list gprs
  access-point 1
    access-mode non-transparent
    access-point-name www.pdn1.com
    aaa-group authentication abc
  !
  ! Disables waiting for RADIUS response
  ! message at APN 1
  !
  no gtp response-message wait-accounting
  exit
  access-point 2
    access-mode non-transparent
    access-point-name www.pdn2.com
    aaa-group authentication abc
  !
  ! Enables waiting for RADIUS response
  ! messages across all APNs (except APN 1)
  !
gprs gtp response-message wait-accounting
!
! Configures global RADIUS server hosts
! and specifies destination ports for
! authentication and accounting requests
!
radius-server host 10.2.3.4 auth-port 1645 acct-port 1646 non-standard
radius-server host 10.6.7.8 auth-port 1645 acct-port 1646 non-standard
radius-server key ggsntel
```

Address Verification and Mobile-to-Mobile Traffic Redirection Example

The following examples show how to enable IPv4 address verification and specify that IPv4 mobile-to-mobile traffic be redirected to an external device.

GGSN Configuration

```

service gprs ggsn
!
hostname t7600-7-2
!
ip cef
!
ip vrf vpn4
  description abc_vrf
  rd 104:4
!
!
interface Loopback2
  description USED FOR DHCP2 - range IN dup prot range
  ip address 111.72.0.2 255.255.255.255
!
interface Loopback100
  description GPRS GTP V-TEMPLATE IP ADDRESS
  ip address 9.9.9.72 255.255.255.0
!
interface GigabitEthernet0/0
  no ip address
!
interface GigabitEthernet0/0.2
  description Ga/Gn Interface
  encapsulation dot1Q 101
  ip address 10.1.1.72 255.255.255.0
  no cdp enable
!
interface GigabitEthernet0/0.3
  encapsulation dot1Q 103
  ip vrf forwarding vpn4
  ip address 10.1.3.72 255.255.255.0
  no cdp enable
!
interface GigabitEthernet0/0.95
  description CNR and CAR
  encapsulation dot1Q 95
  ip address 10.2.25.72 255.255.255.0
!
interface Virtual-Template1
  description GTP v-access
  ip unnumbered Loopback100
  encapsulation gtp
  gprs access-point-list gprs
!
! In case the ms is on another MWAM GGSN
ip route vrf vpn4 0.0.0.0 0.0.0.0 10.1.3.1
!
gprs access-point-list gprs
  access-point 7
    access-point-name ms_redirect.com
    ip-address-pool dhcp-proxy-client
    aggregate auto
    dhcp-server 10.2.25.90
    dhcp-gateway-address 111.72.0.2
    vrf vpn4

```

```

! In case the ms is on this GGSN.
redirect intermobile ip 10.1.3.1
!

```

Supervisor Engine Configuration

```

hostname 7600-a

interface FastEthernet9/15
description OUT to Firewall
no ip address
duplex half
switchport
switchport access vlan 162
!
interface FastEthernet9/16
description In from Firewall
no ip address
switchport
switchport access vlan 163
!
interface Vlan103
description Vlan to GGSN redirect to FW
ip address 10.1.3.1 255.255.255.0
ip policy route-map REDIRECT-TO-FIREWALL
!
interface Vlan162
ip address 162.1.1.1 255.255.255.0
!
interface Vlan163
ip address 163.1.1.1 255.255.255.0
!
ip route 111.72.0.0 255.255.0.0 10.1.3.72
ip route 111.73.0.0 255.255.0.0 10.1.3.73
ip route 111.74.0.0 255.255.0.0 10.1.3.74
ip route 111.75.0.0 255.255.0.0 10.1.3.75
ip route 111.76.0.0 255.255.0.0 10.1.3.76
!
access-list 102 permit ip any any
!
route-map REDIRECT-TO-FIREWALL permit 10
match ip address 102
set ip next-hop 162.1.1.11
!

```

Access to a Private RADIUS Server Using VRF Configuration Example

The following examples shows an example of configuring access to a private RADIUS server using VRF.

GGSN Configuration

```

aaa new-model
!

aaa group server radius vrf_aware_radius
server-private 99.100.0.2 auth-port 1645 acct-port 1646 key cisco
ip vrf
!
aaa authentication ppp vrf_aware_radius group vrf_aware_radius
aaa authorization network default local group radius
aaa authorization network vrf_aware_radius group vrf_aware_radius
aaa accounting network vrf_aware_radius start-stop group vrf_aware_radius

```

```

aaa session-id common

!
ip vrf vpn2
 rd 101:1
!
interface Loopback1
 ip address 150.1.1.72 255.255.0.0
!
interface Tunnel2
 ip vrf forwarding vpn2
 ip address 80.80.72.72 255.255.255.0
 tunnel source 150.1.1.72
 tunnel destination 167.2.1.12
!
ip local pool vpn2_pool 100.72.0.1 100.72.255.255 group vpn2
ip route vrf vpn2 0.0.0.0 0.0.0.0 Tunnel2
!
gprs access-point-list gprs
 access-point 1
  access-point-name apn.vrf2.com
  access-mode non-transparent
  aaa-group authentication vrf_aware_radius
  aaa-group accounting vrf_aware_radius
  ip-address-pool local vpn2_pool
  aggregate 100.72.0.0 255.255.0.0
  vrf vpn2
  !

```

Supervisor Engine Configuration

```

...
!
interface FastEthernet9/5
 switchport
 switchport access vlan 167
!

interface Vlan167
 ip address 167.1.1.1 255.255.0.0
!
ip route 150.1.1.72 255.255.255.255 10.1.1.72
ip route 167.2.0.0 255.255.0.0 167.1.1.12
!
...

```