CHAPTER 10

Configuring Security on the GGSN

This chapter describes how to configure security features on the GGSN, including AAA, RADIUS, and IPSec.

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 a complete description of the GGSN commands in this chapter, refer to the *Cisco IOS Mobile Wireless Command Reference*. 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 10-1
- Configuring AAA Security Globally, page 10-4 (Required)
- Configuring RADIUS Server Communication Globally, page 10-5 (Required)
- Configuring RADIUS Server Communication at the GPRS/UMTS Configuration Level, page 10-6 (Required)
- Configuring Additional RADIUS Security Services, page 10-9 (Optional)
- Configuring IPSec Network Security, page 10-21 (Optional)
- Securing the GGSN Mobile (Gn) Interface, page 10-25 (Optional)
- Configuration Examples, page 10-27

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
- Mobile-to-mobile 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 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 on a per-access-point basis, 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 Systems 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 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, 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 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 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 not a global configuration command to enable or disable 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 Systems' 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: • **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 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 GPRS 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*]	Specifies the IP address or host name of the remote RADIUS server host. The following options are available: • **auth-port**—Specifies the UDP destination port for authentication requests. • **acct-port**—Specifies the UDP destination port for accounting requests. • **timeout**—Specifies the time interval (in the range1 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 resent 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 10-28.

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 GPRS/UMTS 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 GPRS global configuration level, you also can configure RADIUS server communication for all access points or for a specific access point.

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

- Configuring Non-Transparent Access Mode, page 10-6 (Required)
- Specifying a AAA Server Group for All Access Points, page 10-7 (Optional)
- Specifying a 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 not a 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 list-name`	Specifies the access-point list name and enters access-point list configuration mode.
Step 2	`Router(config-ap-list)# access-point access-point-index`	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 6-6.

Specifying a 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
`Router(config)# gprs default aaa-group {authentication | accounting} server-group`	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: • **authentication**—Assigns the selected server group for authentication services on all APNs. • **accounting**—Assigns the selected server group for accounting services on all APNs. • *server-group*—Specifies the name of a AAA server group to be used for AAA services on all APNs. **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.

Specifying a 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 a AAA server group at each access point.

To specify a 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`**`}` *`server-group`*	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: • **authentication**—Assigns the selected server group for authentication services on the APN. • **accounting**—Assigns the selected server group for accounting services on the APN. • *server-group*—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.

Configuring AAA Accounting Services at 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.

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 using the **aaa new-model** global configuration command.
- Define a server group with the IP addresses of the RADIUS servers in that group 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 only want the server group to 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 GPRS global configuration level using the **gprs default aaa-group** command, or at the APN using the **aaa-group** command.
- Configure the RADIUS servers 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.

You can verify whether AAA accounting is enabled or disabled at an APN using the **show gprs access-point** command.

To enable or disable accounting at an access point, use the following command in access-point configuration mode:

Command	Purpose
`Router(config-access-point)#` **`aaa-accounting`** `{`**`enable`** `|` **`disable`**`}`	Enables or disables accounting for a particular access point on the GGSN.

Configuring Additional RADIUS Security 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 the MSISDN IE for RADIUS Requests

To specify that the first byte of the Mobile Station International PSTN/ISDN (MSISDN) information element is included in a RADIUS request, use the following command beginning 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 a RADIUS request.

Configuring the Vendor-Specific Attribute for RADIUS Requests

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) makes 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.

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 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.

Table 10-1 3GPP VSA Sub-Attributes

Number	Vendor-Proprietary Attribute	Description
8	3GPP-IMSI-MCC-MNC	MCC and 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.
12	3GPP-Selection-Mode	Selection mode for this PDP context received in the Create PDP Context request.

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
`Router(config)#`**`radius-server vsa send`**` [`**`accounting`**`	`**`authentication`**`]`	(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 authentication and accounting request 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 10-12
- Suppressing the 3GPP-IMSI VSA Sub-Attribute for RADIUS Authentication, page 10-12
- Suppressing the 3GPP-GPRS-QoS Profile VSA Sub-Attribute for RADIUS Authentication, page 10-12
- Suppressing the 3GPP-GPRS-SGSN-Address VSA Sub-Attribute for RADIUS Authentication, page 10-13

Suppressing the MSISDN Number for RADIUS Authentication

Certain countries have privacy laws which 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 in place 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 overrides or suppresses the MSISDN number in its RADIUS authentication, use the following command beginning 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 pre-configured value in its authentication requests to a RADIUS server.

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

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

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

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

To specify that the GGSN 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 specify that the GGSN suppress the 3GPP-GPRS-Qos Profile in its authentication and accounting requests to a RADIUS server, use the following command beginning 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 specify that the GGSN 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 beginning 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 authentication and accounting requests to a RADIUS server.

Obtaining DNS and NetBIOS Address Information from a RADIUS Server

To obtain DNS address and NetBIOS address information from a RADIUS server, issue the following command in global configuration mode:

Command	Purpose
`Router(config)#radius-server vsa send [accounting	authentication]`	(Optional) Enables the GGSN to send and recognized 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 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 6-6.

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, then the GGSN rejects the PDP context request.

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, ISPs can partition AAA services base on VRF. This permits the GGSN to communicate directly with the customer RADIUS server associated with the customer 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.

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 10-16 (Required)
- Configuring a VRF-Aware Private RADIUS Server Group, page 10-16 (Required)
- Configuring Accounting, Authentication, and Authorization Using Named Method Lists, page 10-17 (Required)
- Configuring a VRF Routing Table, page 10-17 (Required)
- Configuring VRF on an Interface, page 10-18 (Required)
- Configuring VRF under an Access Point for Access to the Private RADIUS Server, page 10-18 (Required)
- Configuring a Route to the RADIUS Server Using VRF, page 10-19 (Optional)

Enabling AAA Globally

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

To enable AAA globally, use the following commands beginning 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** *group-name*	Groups different RADIUS server hosts into distinct lists and distinct methods. • *group-name*—Character string used to name the group of servers.
Step 2	Router(config-sg-radius)# **server-private** *ip-address* **auth-port** *port_num* **acct-port** *port_num* **key** *string*	Configures the IP address of the private RADIUS server for the group server. • *ip-address*—Specifies the IP address of the private RADIUS server host. • **auth-port** *port_num*—Specifies a port solely for authentication. • **acct-port** *port_num*—Specifies a port solely for accounting. • *string*—(Optional) Specifies the authentication and encryption key for all RADIUS communications between the router and the RADIUS server. **Note** If private server parameters are not specified, global configurations are used. If global configurations are not specified, default values are used.
Step 3	Router(config-sg-radius)# **ip vrf forwarding** *vrf-name*	Configures the VRF reference of the AAA RADIUS server group. • *vrf-name*—Name assigned to a VRF.

Configuring Accounting, Authentication, and Authorization Using Named Method Lists

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

Step 4	Router(config)# **aaa authentication ppp** {**default** | *list-name*} *method1* [*method2*...]	Creates a local authentication method list, with the following options: • **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 5	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 6	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 command 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 configure VRF on a physical interface to the PDN using Fast Ethernet over the Gi interface, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# interface type slot/port`	Defines a physical interface on the GGSN, where *type* is **fastethernet**, and *slot/port* is the hardware slot and port on the interface.
Step 2	`Router(config-if)# ip vrf forwarding vrf-name`	Associates a VRF with an interface or subinterface. **Note** The *vrf-name* argument should match the name of the VRF that you configured using the **ip vrf** command in the "Configuring Accounting, Authentication, and Authorization Using Named Method Lists" section on page 10-17. **Note** The IP address defined on the interface will get removed when you associate a VRF with the interface. Therefore, you will need to reconfigure the IP address for the interface.
Step 3	`Router(config-if)# ip address ip-address mask`	Specifies an IP address for the interface, where: • *ip-address*—Specifies the IP address of the interface in dotted decimal format. • *mask*—Specifies a subnet mask in dotted decimal format.

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

To configure VRF under an access point to use to access a RADIUS server, use the following commands beginning in access-point list configuration mode:

	Command	Purpose
Step 1	`Router(config-ap-list)# access-point access-point-index`	Specifies an index number for a new access point definition, or references an existing access point definition, and enters access point configuration mode.
Step 2	`Router(config-access-point)# access-point-name apn-name`	Specifies the network (or domain) name for a PDN that users can access from the GGSN at a defined access point. **Note** The *apn-name* must match the APN that has been provisioned at the MS, HLR, and DNS server.

	Command	Purpose
Step 3	`Router(config-access-point)# aaa-group authentication server-group`	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: - **authentication**—Assigns the selected server group for authentication services on the APN. - *server-group*—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 4	`Router(config-access-point)# access-mode non-transparent`	Specifies for the GGSN to act as a proxy for authentication.
Step 5	`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.
Step 6	`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. **Note** The *vrf-name* argument should match the name of the VRF that you configured using the **ip vrf** command in the "Configuring Accounting, Authentication, and Authorization Using Named Method Lists" section on page 10-17.

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
Router(config)# **ip route vrf** *vrf-name prefix mask* [*next-hop-address*] [*interface* {*interface-number*}] [**global**] [*distance*] [**permanent**] [**tag** *tag*]	Configures a static IP route, where: • *vrf-name*—Specifies the name of the VPN routing/forwarding instance (VRF) for the static route. • *prefix*—Specifies the IP route prefix for the destination. • *mask*—Specifies the prefix mask for the destination. • *next-hop-address*—Specifies the IP address of the next hop that can be used to reach the destination network. • *interface interface-number*—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. • *distance*—Specifies an administrative distance for the route. • **tag** *tag*—Specifies a tag value that can be used as a “match” value for controlling redistribution via route maps. • **permanent**—Specifies that the route will not be removed, even if the interface shuts down.

Verifying a Static Route Using VRF

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

```
Router# 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 process-id [vrf vrf-name]`	Enables OSPF routing, and enters router configuration mode, where, • *process-id*—Specifies an internally used identification parameter for an OSPF routing process. The *process-id* is locally assigned and can be any positive integer. A unique value is assigned for each OSPF routing process. • **vrf** *vrf-name*—Specifies the name of the VPN routing/forwarding instance.

Configuring IPSec Network Security

In Cisco IOS Release 12.1(5)T and later, the GGSN software supports the IP security protocol for data authentication, confidentiality, encryption and integrity. IPSec data security can be implemented between the GGSN and another router on the PDN.

Note To support IPSec on the GGSN, you must install an ISA card on your router.

Configuring IPSec network security includes the following tasks:

- Configuring an IKE Policy, page 10-21 (Required)
- Configuring Pre-Shared Keys, page 10-23 (Required, when pre-shared authentication is configured)
- Configuring Transform Sets, page 10-24 (Optional)
- Configuring Crypto Map Entries that Use IKE to Establish Security Associations, page 10-24 (Optional)

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

For an example, see the "IPSec Configuration Example" section on page 10-31.

Configuring an IKE Policy

You can create multiple Internet Key Exchange (IKE) policies, each with a different combination of parameter values. For each policy that you create, you assign a unique priority (1 through 10,000, with 1 being the highest priority).

You can configure multiple policies on each peer—but at least one of these policies must contain exactly the same encryption, hash, authentication, and Diffie-Hellman parameter values as one of the policies on the remote peer. For example, you can configure multiple policies on the GGSN to correlate with the policies for different PDNs.

To configure an IKE policy on the GGSN and corresponding PDN, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# **crypto isakmp policy** *priority*	Identifies the IKE policy, where *priority* is an integer (from 1 to 10,000) that uniquely identifies the policy. This command enters you into ISAKMP policy configuration mode.
Step 2	Router(config-isakmp)# **encryption des**	Specifies the encryption algorithm, where: • **des**—Specifies 56-bit Data Encryption Standard (DES)-Cipher Block Chaining (CBC). This is the default value. **Note** Triple DES, or 168-bit DES encryption is supported in the Cisco IOS software. It can be configured by using this command and specifying the **3des** optional keyword. GGSN Release 1.4 in Cisco IOS Release 12.2 does not support the **3des** optional keyword.
Step 3	Router(config-isakmp)# **hash** {**sha** | **md5**}	Specifies the hash algorithm, where: • **sha**—Specifies the Secure Hash Algorithm (SHA)-1. This is the default value. • **md5**—Specifies the Message Digest 5 hash algorithm.
Step 4	Router(config-isakmp)# **authentication** {**rsa-sig** | **rsa-encr** | **pre-share**}	Specifies the authentication method, where: • **rsa-sig**—Specifies the public key encryption system developed by Ron Rivest, Adi Shamir, and Leonard Adleman, which provides non-repudiation. This is the default value. • **rsa-encr**—Specifies RSA encrypted nonces, which provide repudiation. • **pre-share**—Specifies a pre-shared key that does not require use of a certification authority. Pre-shared keys might be easier to configure in a small network with less than 10 nodes. RSA signatures can be considered more secure than pre-shared keys. If you configure **pre-share** authentication, then you must configure the pre-shared keys on both the local and remote peer (GGSN and PDN).

	Command	Purpose
Step 5	`Router(config-isakmp)# group {1 | 2}`	Specifies the Diffie-Hellman group identifier, where: • **1**—Specifies 768-bit Diffie-Hellman. This is the default value. • **2**—Specifies 1024-bit Diffie-Hellman. **Note** The 1024-bit Diffie-Hellman option is harder to crack, but requires more CPU time to execute.
Step 6	`Router(config-isakmp)# lifetime seconds`	Specifies the security association's lifetime (in seconds). The default value is 86,400 seconds (1 day).

For more information about the meaning of the IKE policy parameters, refer to the *Cisco IOS Security Configuration Guide* and *Cisco IOS Security Command Reference* publications.

Configuring Pre-Shared Keys

When you configure the **pre-share** authentication method for your IKE policy, you also must configure the pre-shared keys on the GGSN and remote peer, or PDN.

To configure pre-shared keys on the GGSN and corresponding PDN, use one of the following commands beginning in global configuration mode:

Command	Purpose

`Router(config)# crypto isakmp key keystring address peer-address`
or
`Router(config)# crypto isakmp key keystring hostname peer-hostname`
	Specifies the shared key to be used between a local peer (GGSN) and particular remote peer (PDN).
	If the remote peer, or PDN, specifies the ISAKMP identity with an address, use the **address** keyword; otherwise use the **hostname** keyword.
	When configuring the pre-shared keys on the GGSN, use the address or hostname of the PDN. When configuring the pre-shared keys on the PDN, use the address or hostname of the GGSN.

Configuring Transform Sets

A transform set represents a certain combination of security protocols and algorithms. During the IPSec security association negotiation, the peers agree to use a particular transform set for protecting a particular data flow.

To configure a transform set on the GGSN and corresponding PDN, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)#` **`crypto ipsec transform-set`** *`transform-set-name transform1`* `[`*`transform2`* `[`*`transform3`*`]]`	Defines a transform set and enters crypto transform configuration mode. There are complex rules defining which entries you can use for the transform arguments. For more information, refer to the *Cisco IOS Security Configuration Guide* and *Cisco IOS Security Command Reference* publications.
Step 2	`Router(config-crypto-transform)#` **`mode`** `[`**`tunnel`** `|` **`transport`**`]`	(Optional) Changes the mode associated with the transform set. The following options are available: • **tunnel**—Protects (encrypts, authenticates) and encapsulates the entire original IP packet • **transport**—Protects (encrypts, authenticates) and encapsulates the payload or data portion of the IP packet. **Note** The mode setting is applicable only to traffic whose source and destination addresses are the IPSec peer addresses; it is ignored for all other traffic.

Configuring Crypto Map Entries that Use IKE to Establish Security Associations

When you use IKE to establish security associations, you can specify a list of acceptable settings to be used during IPSec peer negotiation using a crypto map entry.

To configure crypto map entries on the GGSN and corresponding PDN, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)#` **`crypto map`** *`map-name seq-num`* **`ipsec-isakmp`**	Creates or modifies a crypto map entry and enters crypto map configuration mode.
Step 2	`Router(config-crypto-map)#` **`match address`** *`access-list-id`*	Names an extended access list. This access list determines which traffic should be protected by IPSec and which traffic should not be protected by IPSec in the context of the current crypto map entry.
Step 3	`Router(config-crypto-map)#` **`set peer`** `{`*`hostname`* `|` *`ip-address`*`}`	Specifies a remote IPSec peer. This is the peer to which IPSec-protected traffic can be forwarded.

	Command	Purpose
Step 4	`Router(config-crypto-map)#` **`set transform-set`** *`transform-set-name1`* `[`*`transform-set-name2...transform-set-name6`*`]`	Specifies which transform sets are allowed for this crypto map entry. List multiple transform sets in order of priority (highest priority first).

Step 5	`Router(config-crypto-map)#` **`set security-association lifetime seconds`** *`seconds`*
	`and/or`
	`set security-association lifetime kilobytes kilobytes`
		(Optional) Specifies a security association lifetime for the crypto map entry, if you want the security associations for the current crypto map entry to be negotiated using different IPSec security association lifetimes than the global lifetimes.

Step 6	`Router(config-crypto-map)#` **`set security-association level per-host`**	(Optional) Specifies that separate security associations should be established for each source/destination pair. **Note** Use this command with care, as multiple streams between given subnets can rapidly consume resources.
Step 7	`Router(config-crypto-map)#` **`set pfs`** `[`**`group1`** `|` **`group2`**`]`	(Optional) Specifies that IPSec should ask for perfect forward secrecy (PFS) when requesting new security associations for the current crypto map entry, or should demand PFS in requests received from the IPSec peer.
Step 8	`Router(config-crypto-map)#` **`exit`**	Exits crypto map configuration mode.
Step 9	`Router(config)#` **`interface fastethernet`** *`slot/port`*	Accesses the Gi interface to which you want to apply the cryto map.
Step 10	`Router(config-if)#` **`crypto map`** *`map-name`*	Applies the crypto map set to the interface.

Securing the GGSN Mobile (Gn) Interface

With GGSN 3.0 on Cisco IOS Release 12.2(8) B or later, features have been added to provide additional security for the GGSN mobile interface against attacks that can lead to illegal access to a network or even network downtime.

Configuring Address Verification

Use the **security verify source** 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** command is 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 accounts it as an illegal packet in its PDP context and APN. Configuring the **security verify source** access point configuration command protects the GGSN from faked user identities.

Use the **security verify destination** access point configuration command to have the GGSN verify the destination addresses of upstream TPDUs 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. In addition, the verification of destination addresses does not apply to GTP-PPP regeneration or GTP-PPP with L2TP.

To configure address verification for a GGSN access point, use the following commands beginning 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 TPDUs received from a Gn interface.

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

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) Specifies that mobile-to-mobile traffic be redirected to an external device.

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

Configuration Examples

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

AAA Security Configuration Example

The following example shows how to enable AAA security globally on the router, and 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 foo group foo
!
! 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 foo group foo
```

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 "foo" for this radius host only
!
radius-server host 10.100.0.2 auth-port 1645 acct-port 1646 key foo
!
! 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: foo, foo1, foo2, and foo3, 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: foo2 for authentication, and foo3 for accounting.

At access-point 1, which is enabled for authentication, the default global authentication server group of foo2 is overridden and the server group named foo 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 foo3 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 foo3 is overridden and the server group named foo1 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 foo
 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 foo1
 server 10.10.0.1 auth-port 1645 acct-port 1646
aaa group server radius foo2
 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 foo3
 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 foo group foo
aaa authentication ppp foo2 group foo2
aaa authorization network foo group foo
aaa accounting network foo start-stop group foo
aaa accounting network foo1 start-stop group foo1
aaa accounting network foo2 start-stop group foo2
aaa accounting network foo3 start-stop group foo3
!
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 foo
!
 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 foo1
!
 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 foo2
gprs default aaa-group accounting foo3
!
! 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 using the **no gtp response-message wait-accounting** command:

```
! Enables AAA globally
!
aaa new-model
!
! Defines AAA server group
!
aaa group server radius foo
 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 foo group foo
aaa authorization network foo group foo
aaa accounting network foo start-stop group foo
!
gprs access-point-list gprs
 access-point 1
  access-mode non-transparent
  access-point-name www.pdn1.com
  aaa-group authentication foo
!
! 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 foo
!
! 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
```

IPSec Configuration Example

IP Security Protocol is configured between two peers to establish data security services. For GPRS/UMTS, IPSec configuration is applicable between the GGSN and a router on a PDN. The following example shows configuration of IPSec on the GGSN and an associated PDN, including the complete global and GGSN configuration commands:

GGSN configuration

```
!
hostname ggsn1
!
! IPSec configuration for GGSN
crypto isakmp policy 1
  authentication pre-share
  group 2
!
! 10.58.0.8 is address of peer, or PDN
!
crypto isakmp key sharedkey address 10.58.0.8
crypto ipsec transform-set auth2 esp-des esp-sha-hmac
crypto map test 10 ipsec-isakmp
  set peer 10.58.0.8
  set transform-set auth2
  match address 133
!
! ISA card is required for IPSec support
!
controller ISA 1/1
!
interface loopback 1
  ip address 10.7.7.7 255.255.255.0
!
interface FastEthernet0/0
  description CONNECT TO sgsn-a
  ip address 10.56.0.7 255.255.0.0
!
interface FastEthernet4/0
  description CONNECT TO Gi
  ip address 10.58.0.7 255.255.0.0
  crypto map test
!
interface Virtual-Template1
  ip unnumber loopback 1
  encapsulation gtp
  ip mroute-cache
  gprs access-point-list gprs
router eigrp 10
  network 10.56.0.0
  network 10.58.0.0
!
!
!
!  10.2.0.0 is the network for Mobile Nodes
!
access-list 133 permit ip 10.2.0.0 0.0.255.255 10.59.0.0 0.0.255.255
!
!
gprs access-point-list gprs
  access-point 1
    access-point-name gprs.cisco.com
  exit
```

PDN configuration

```
!
hostname pdn1a
!
!
! IPSec configuration on the PDN
!
crypto isakmp policy 1
  authentication pre-share
  group 2
!
! 10.58.0.7 is address of peer, or GGSN
!
crypto isakmp key sharedkey address 10.58.0.7
crypto ipsec transform-set auth2 esp-des esp-sha-hmac
crypto map test 10 ipsec-isakmp
  set peer 10.58.0.7
  set transform-set auth2
  match address 144
!
!
controller ISA 1/1
!
interface FastEthernet0/0
  description CONNECT TO Intranet
  ip address 10.59.0.8 255.255.0.0
!
interface FastEthernet4/0
  description CONNECT TO Gi
  ip address 10.58.0.8 255.255.0.0
  crypto map test

!
!
! ISA card is required for IPSec support
router eigrp 10
  network 10.2.0.0
  network 10.58.0.0
  network 10.59.0.0
!
!
access-list 144 permit ip 10.59.0.0 0.0.255.255 10.2.0.0 0.0.255.255
!
!
```

Address Verification and Mobile-to-Mobile Traffic Redirection Example

The following example shows how to enable address verification on the router and specify that mobile-to-mobile traffic be redirected to an external device:

```
! Defines PLMN address ranges
gprs plmn ip address 1.1.1.1 1.1.1.99
gprs plmn ip address 1.1.2.1 1.1.2.49
!
! Enters access-point configuration mode
! and turns on source and destination address
! verification and mobile-to-mobile traffic redirection
!
gprs access-point-list gprs
     access-point 1
         access-point-name www.abc.com
         security verify source
         security verify destination
         redirection intermobile ip 10.1.1.1
!
```

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:

```
! Enables AAA globally
aaa new-model
!
! Configures a VRF-Aware Private RADIUS Server Group named vrf_aware_radius
!
aaa group server radius vrf_aware_radius
 server-private 99.100.0.2 auth-port 1645 acct-port 1646 key cisco
 ip vrf forwarding vpn4
!
! Configures Authentication, Authorization, and Accounting using named method lists
!
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
!
! Configures a VRF routing table
!
ip vrf vpn4
 rd 104:1
!
! Configures VRF on an interface
!
interface FastEthernet0/0
 ip vrf forwarding vpn4   <=== new
 ip address 99.108.0.4 255.255.255.0
!
! Configures VRF on an access point for access to the server
!
access-point 17
   access-point-name radius_vrf
   access-mode non-transparent
   aaa-group authentication vrf_aware_radius
   aaa-group accounting vrf_aware_radius
   ip-address-pool radius-client
   vrf vpn4
   exit
```