CHAPTER 12

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 SAMI.

For information about configuring IPSec on the Cisco 7600 series router platform, see *IPSEC VPN Acceleration Services Module Installation and Configuration Not*e.

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, see *Cisco IOS Security Configuration Guide* and *Cisco IOS Security Command Reference* publications. For information about IPSec security services on Cisco 7600 platform, see *IPSec VPN Acceleration Services Module Installation and Configuration Note*.

For complete descriptions of the GGSN commands in this chapter, see *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 12-2
- Configuring AAA Security Globally, page 12-4 (Required)
- Configuring RADIUS Server Communication Globally, page 12-5 (Required)
- Configuring RADIUS Server Communication at the GGSN Configuration Level, page 12-6 (Required)
- Configuring Additional RADIUS Services, page 12-10 (Optional)
- Securing the GGSN Gn Interface, page 12-28 (Optional)
- Segregating GRX Traffic on the Gn/Gp Interface, page 12-31
- Configuring Simultaneous Broadcast and Wait Accounting, page 12-32 (Optional)
- Periodic Accounting Timer, page 12-34 (Optional)
- Implementing Lawful Intercept Support on the Cisco GGSN (Optional)
- Configuration Examples, page 12-45

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.

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

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** command in global configuration mode.
- 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 not a global configuration command for enabling or disabling authentication.
- Configure AAA accounting and authentication using the **aaa accounting** and **aaa authentication** commands in global configuration mode.

Note For more information about AAA and RADIUS global configuration commands, see *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: • **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, see *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 GGSN, 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 hostname of the remote RADIUS server host. The following options are available: • **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, see *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 12-46.

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 12-6 (Required)
- Specifying an AAA Server Group for All Access Points, page 12-7 (Optional)
- Specifying an AAA Server Group for a Particular Access Point, page 12-8 (Optional)
- Configuring AAA Accounting Services at an Access Point, page 12-8 (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` *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 9-7.

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 for all GGSN access points to use.

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 an AAA server group to use 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 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} 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 an AAA server group to use 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 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** command in global configuration mode.
- Define a server group with the IP addresses of the RADIUS servers in that group by using the **aaa group server** command in global configuration mode.

- Configure the following AAA services:
  - AAA authentication using the **aaa authentication** command in global configuration mode
  - AAA authorization using the **aaa authorization** command in global configuration mode
  - AAA accounting using the **aaa accounting** command in global configuration mode
- 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 *Cisco IOS Security Command Reference.*

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

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** command in access-point configuration mode.

Configuring Interim Accounting on an Access Point

Using the **aaa-accounting** command in access-point configuration mode with an **interim** keyword option specified, you can configure the GGSN to send Interim-Update Accounting requests to the AAA server.

Note Interim accounting support requires that accounting services be enabled for the APN and that the **aaa accounting update newinfo** command in global configuration mode 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 | periodic` *minutes* `| periodic radius}]`	Configures accounting services on an access point on the GGSN, with the following options: • **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. • **interim periodic** *minutes*—(Optional) Enables interim periodic accounting records to be sent to an accounting server on regular configured intervals. • **interim periodic radius—**(Optional) Enables GGSN to accept the periodic accounting value (Attribute 85) sent by RADIUS.

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 12-11
- Configuring the Vendor-Specific Attribute in Access Requests to the RADIUS Server, page 12-13
- Suppressing Attributes for RADIUS Authentication, page 12-14
- Obtaining DNS and NetBIOS Address Information from a RADIUS Server, page 12-16
- Configuring the RADIUS Packet of Disconnect, page 12-16
- Configuring the GGSN to Wait for a RADIUS Response, page 12-18
- Configuring Access to a RADIUS Server Using VRF, page 12-19
- Configuring RADIUS Change of Authorization Support, page 12-28

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 12-11
- Configuring the MSISDN IE, page 12-11
- Configuring the NAS-Identifier, page 12-11
- Configuring the Charging ID in the Acct-Session-ID Attribute, page 12-12
- Configuring the MSISDN in the User-Name Attribute, page 12-12

Configuring the CHAP Challenge

To specify to always include the Challenge Handshake Authentication Protocol (CHAP) challenge 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 to include the NAS-Identifier 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` *format*	Specifies that the GGSN sends the RADIUS attribute 32 (NAS-Identifier) in access requests where *format* 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 in global configuration mode.

To specify to include the NAS-Identifier 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` *format*	Specifies that the GGSN sends the NAS-Identifier in access requests at an APN where *format* 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 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 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 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 12-1 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 12-1 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 gateway GPRS support node-call detail records (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** command in global configuration mode.

Table 12-1 3GPP VSA Sub-Attributes (continued)

Number	Vendor-Proprietary Attribute	Description
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** command in global configuration mode.
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
`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, see *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 12-14
- Suppressing the 3GPP-IMSI VSA Sub-Attribute for RADIUS Authentication, page 12-15
- Suppressing the 3GPP-GPRS-QoS Profile VSA Sub-Attribute for RADIUS Authentication, page 12-15
- Suppressing the 3GPP-GPRS-SGSN-Address VSA Sub-Attribute for RADIUS Authentication, page 12-15

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 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** command in access point configuration mode.

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 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** command in access point configuration mode.

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** command in access point configuration mode.

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 9-7.

Configuring the RADIUS Packet of Disconnect

The RADIUS Packet of Disconnect (PoD) feature is a method for terminating a user session after the session is 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 is accepted by the RADIUS access-accept packet. For example, with 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
`Router(config)# aaa pod server [port port-number] [auth-type {any| all| session-key}] server-key [encryption-type] string`	Enables inbound user sessions to be disconnected when specific session attributes are presented. • **port** *port-number*—(Optional) Network access server User Datagram Protocol (UDP) port 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. – **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. **Note** When configuring a PoD on the GGSN, we recommend that you do not configure the **auth-type** keyword option. • **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** command in global configuration mode. To disable this behavior for a particular APN, use the **no gtp response-message wait-accounting** command in access-point configuration mode.

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 12-24.

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, define AAA servers in a single global pool that is 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 and 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, see *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 12-20 (Required)
- Configuring a VRF-Aware Private RADIUS Server Group, page 12-21 (Required)
- Configuring Authentication, Authorization, and Accounting Using Named Method Lists, page 12-22 (Required)
- Configuring a VRF Routing Table, page 12-22 (Required)
- Configuring VRF on an Interface, page 12-22 (Required)
- Configuring VRF Under an Access Point for Access to the Private RADIUS Server, page 12-23 (Required)
- Configuring a Route to the RADIUS Server Using VRF, page 12-27 (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 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 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: • **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 is 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 3-2.

For more information about configuring interfaces, see *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 slot/port.subinterface-number`	Specifies the subinterface on which IEEE 802.1Q will be used.
Step 2	`Router(config-if)# encapsulation dot1q vlanid`	Defines the encapsulation format as IEEE 802.1Q (dot1q), and specifies the VLAN identifier.
Step 3	`Router(config-if)# ip address ip-address mask`	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.

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** command in access point configuration mode.

Note 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 list-name`	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 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 3	`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 is provisioned at the MS, HLR, and DNS server.

	Command	Purpose
Step 4	`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 use 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.
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. **Note** The *vrf-name* 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 12-22.
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` *list-name*	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` *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 3	`Router(config-access-point)# access-point name` *apn-name*	Specifies the access point network ID, which is commonly an Internet domain name. **Note** The *apn-name* must match the APN that is 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: • **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.
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.

	Command	Purpose
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: • **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** command in access point configuration mode and that a local pool is configured using the **ip local pool** command in global configuration mode. • **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 hostname) 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
`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 (VRF) instance 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. • **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 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 RADIUS Change of Authorization Support

The RADIUS Change of Authorization (CoA) message contains information for dynamically changing session authorizations. The CoA message is received on port 1700.

The Cisco GGSN uses the base Cisco IOS AAA to support the RADIUS CoA message, as defined by RFC 3576. In addition, the Cisco GGSN also utilizes an additional 3GPP QoS attribute that indicates the updated QoS, and the Acct-Session-ID that identifies the PDP context.

The QoS vendor-specific attribute (VSA) is a string with bytes encoded with QoS attributes (as defined by 3GPP TS 24.008). The Accounting-session-id is a string that uses the standard attribute type 44.

For detailed information about AAA and RADIUS, see *Cisco IOS Security Configuration Guide, Release 12.4*.

To ensure that an interim accounting record is generated as a part of the CoA procedure, confirm the following exists:

- Globally, the **aaa accounting update newinfo** command in global configuration mode is configured.
- Under the APN, the **aaa-accounting** command in access-point configuration mode is configured with the **interim update** keyword option specified.

Securing the GGSN 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 12-29
- Configuring Mobile-to-Mobile Traffic Redirection, page 12-30
- Redirecting All Traffic, page 12-30

Configuring Address Verification

Use the **security verify source** (IPv4 address verification) and **ipv6 security verify source** (IPv6 address verification) commands in access point configuration mode 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 under 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** commands in access point configuration mode protects the GGSN from faked user identities.

Use the **security verify destination** command in access point configuration mode (IPv4 address verification only) 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 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 TPDUs received from a Gn interface.

Note Both the verification of IPv4 destination addresses and source addresses can be configured under 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 SAMI, 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 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.

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 commands in access-point configuration mode:

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

Segregating GRX Traffic on the Gn/Gp Interface

The Cisco GGSN receives traffic from the SGSN on the Gn/Gp interface. The Gn traffic is from SGSNs within the same PLMN, and the Gp traffic is from SGSNs within different PLMNs coming via GPRS Roaming Exchange (GRX) to the GGSN.

To ensure privacy and security, the Cisco GGSN supports Virtual Private Network (VPN) routing and forwarding (VRF) instances on the Gn/Gp interface so that you can segregate GRX traffic to be a part of separate routing tables.

When configuring a Gn VRF virtual template interface to segregate GRX traffic, note the following:

- You must configure the default GTP virtual template (Virtual-Template 1), and never unconfigured it as long as **service gprs ggsn** is configured. You must assign a valid IP address to the default GTP virtual template (Virtual-Template 1) by using either the **ip address** or **ip unnumbered** command. Do not use the default GTP Virtual-Template in a VRF.
- You must configure a separate GTP virtual template interface for each VRF.
- Never place two virtual templates with GTP encapsulation under the same VRF.
- Unless a charging source interface is configured, use the same IP address for all loopback interfaces create for and associated with the GTP virtual template interfaces to ensure that CDRs for a PDP context contain the same GGSN address.
- Configure all GTP virtual template interfaces with the same access point list name.

To create a Gn VRF virtual template interface, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# interface virtual-template number`	Creates a virtual template interface, where *number* identifies the virtual template interface. This command takes you to interface configuration mode.
Step 2	`Router(config-if)# description description`	Description of the interface.
Step 3	`Router(config-if)# ip vrf forwarding vrf-name`	Associates a VRF instance with an interface.
Step 4	`Router(config-if)# ip unnumber loopback number`	Assigns a previously defined loopback IP address to the GTP virtual template interface.
Step 5	`Router(config-if)# encapsulation gtp`	Specifies GTP as the encapsulation type for packets transmitted over the virtual template interface.
Step 6	`Router(config-if)# gprs access-point-list list-name`	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.

The following is an example Gn VRF virtual template interface configuration:

```
ip vrf example
   rd 60:110
!
interface Loopback0
   ip address 172.0.0.100 255.255.0.0
!
interface Loopback52
   ip vrf forwarding example
   ip address 172.0.0.100 255.255.0.0
!
interface Virtual-Template1
   ip unnumbered Loopback0
   encapsulation gtp
   gprs access-point-list MWAM
!
interface Virtual-Template30
   ip vrf forwarding example
   ip unnumbered Loopback52
   encapsulation gtp
   gprs access-point-list MWAM
!
```

To remove the Gn VRF virtual template interface configuration using the **no** form of the **interface virtual-template** command in global configuration mode and specify the number of the Gn VRF virtual template interface.

Configuring Simultaneous Broadcast and Wait Accounting

With Cisco GGSN Release 8.0 and later, broadcast and wait accounting can be configured to work together. The wait accounting feature is configured at the APN level, while broadcast accounting is specified at the AAA method level.

Broadcast accounting sends start, stop and interim accounting records to all the server groups configured in a method list. Within a server group, the accounting records are sent to the first active server. If the active server cannot be reached, then the accounting records are sent to the next server within a group.

In addition, one or more server groups within a method list can be configured as “mandatory,” meaning that a server from that server group has to respond to the Accounting Start message. The APN-level wait accounting ensures that an accounting response is received from all mandatory server groups before the PDP context is established.

The advantages of broadcast and wait accounting together include:

- Accounting records are sent to multiple servers and once the entry is made, the user can start using different services.
- Records are sent to multiple AAA servers serve for redundancy purposes.
- A PDP context is established only when a valid Accounting Start record is received by all essential servers, avoiding information loss.
- Broadcast records can be sent to as many as 10 server groups within a method-list.

When configuring broadcast and wait accounting together:

- Under the method list configuration, the **mandatory** keyword is available only if broadcast accounting is configured.
- If wait accounting is not required, broadcast accounting to all server groups is available without any mandatory groups defined.

- If you do not specify any mandatory server groups when configuring broadcast accounting, wait accounting will function as it does in Cisco GGSN Release 7.0 and prior releases.
- Wait accounting does not apply to PPP PDP contexts.
- A PDP is successfully created only when a Accounting response is received from all the mandatory servers.
- The periodic timer starts when an Accounting Response (PDP creation) is received.

Note More than one server-group can be defined as a mandatory server-group in a method list.

To configure broadcast and wait accounting on the GGSN, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# aaa accounting network methodlist-name`	Enables authentication, authorization, and accounting (AAA) accounting of requested services for billing or security purposes when you use RADIUS.
Step 2	`Router(cfg-acct-mlist)# action-type {start-stop | stop-only | none}`	Type of action to be performed on accounting records. Possible values are: • **start-stop**—Sends a "start" accounting notice at the beginning of a process and a "stop" accounting notice at the end of a process. • **stop-only**—Sends a "stop" accounting notice at the end of the requested user process. • **none**—Disables accounting services on this line or interface.
Step 3	`Router(cfg-acct-mlist)# broadcast`	(Optional) Enables sending accounting records to multiple AAA servers. Simultaneously sends accounting records to the first server in each group. If the first server is unavailable, switchover occurs using the backup servers defined within that group.
Step 4	`Router(cfg-acct-mlist)# group {server-group} [mandatory]`	Specifies the server group. Optionally, specify mandatory to define this server group as mandatory. If a server group is mandatory, a server from the server group has to respond to the Accounting Start message. **Note** Up to 10 server groups can be defined within a method list.
Step 5	`Router(cfg-acct-mlist)# exit`	Exits from accounting method list mode.
Step 1	`Router(config)# gprs access-point-list list_name`	Configures an access point list that you use to define public data network (PDN) access points on the GGSN.
Step 2	`Router(config-ap-list)#access-point access-point-index`	Specifies an access point number and enters access point configuration mode.

	Command	Purpose
Step 3	`Router(config-access-point)#`**`aaa-group accounting`** *`method-list name`*	Specifies an accounting server group.
Step 4	`Router(config-access-point)#` **`gtp-response-message wait-accounting`**	Configure APN to wait for a RADIUS accounting response before sending a Create PDP Context response to the SGSN.

Periodic Accounting Timer

The Cisco IOS software supports a global AAA configuration command that enables the sending of periodic accounting records for AAA sessions. However, the GGSN does not use this configuration to send periodic accounting records for PDP contexts.

With Cisco GGSN Release 8.0 and later, the periodic accounting timer interval value is obtained using one of the following:

- Configured periodic timer at an APN level
- Configured periodic timer at the GGSN global configuration level
- An accounting-interim interval attribute in access-accept messages

When these configurations exist, “interim” type accounting records are sent at the configured interval for the applicable PDP contexts. The following precedence applies:

- The APN-level configuration
- GGSN global configuration
- Attribute 85 (in access-accept messages)

Note If the value is obtained through Attribute 85 in an access-accept message, the GGSN verifies that the minimum and maximum values are within range configured on the GGSN, and if not, the attribute is ignored. In addition, if accounting is not enabled on the APN, Attribute 85 is ignored.

When the GGSN sends an interim update accounting (IAU) record, the periodic timer is reset so that next periodic accounting record will be sent after the periodic interval expires, starting from the instance when the IAU record is sent.

This limits the RADIUS accounting traffic as both types of records contain the same information. However, after a switchover, the records sent out will be aligned with the original START record.

Caution If the **aaa accounting update periodic** command is configured on the GGSN, and GGSN-level periodic accounting is not configured, the GGSN will send interim accounting records after the Accounting Start message is sent to AAA server. This might have adverse effects on the GGSN, therefore ensure that the **aaa accounting update periodic** command has not been configured.

When configuring periodic accounting timers on the GGSN:

- Timers are supported for PPP-Regen, IPv4, and IPv6 PDP’s. Timers do not apply to do PPP PDPs.
- The send/receive byte counts for a PDP is reset to 0 upon switchover.

- Redundant systems should have their clocks synchronized with a mechanism such as NTP to ensure that their timer intervals to be accurate
- Periodic accounting on a redundant configuration maintains intervals across switchovers.
- A timer is initiated only on successful PDP creation, for example, with wait accounting, after a successful accounting response is received.

Configuring a Default GGSN Periodic Accounting Timer

To enable a default periodic accounting value for all APNs, use the following command in global configuration mode:

Command	Purpose
`Router(config)# gprs default aaa-accounting interim periodic` *minutes*	Configures a default periodic accounting timer on the GGSN. The valid values are 15 to 71582. The default is no periodic accounting timer is configured globally.

Configuring an APN-Level Periodic Accounting Timer

To configure the periodic accounting timer under an APN, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# gprs access-point-list` *list_name*	Configures an access point list.
Step 2	`Router(config-ap-list)#access-point` *access-point-index*	Specifies an access point number and enters access point configuration mode.
Step 3	`Router(config-access-point)#aaa-accounting interim periodic` *minutes*	Configures a periodic accounting timer under an APN. The valid values are 15 to 71582. The default is no periodic accounting timer is configured at the APN level.
Step 4	`Router(config-access-point)#aaa-accounting interim periodic radius`	Enables the APN to accept the periodic accounting value (Attribute 85) sent by RADIUS.

Note AAA global configuration value (**aaa accounting update periodic** *minutes*) will be ignored always. Also, unless APN accounting is enabled, the periodic accounting will not take effect regardless of how it is configured.

Implementing Lawful Intercept Support on the Cisco GGSN

This section provides information about Lawful Intercept and contains the following subsections:

- Lawful Intercept Overview, page 12-36
- Network Components Used for Lawful Intercept, page 12-37
- Lawful Intercept Processing, page 12-38
- Lawful Intercept MIBs, page 12-39
- Lawful Intercept Topology, page 12-40
- Configuring Lawful Intercept Support, page 12-40

Caution This section does not address legal obligations for the implementation of lawful intercept. As a service provider, you are responsible to ensure that your network complies with applicable lawful intercept statutes and regulations. We recommend that you seek legal advice to determine your obligations.

Lawful Intercept Overview

Lawful intercept is a process that enables a Law Enforcement Agency (LEA) to perform electronic surveillance on an individual (a target) as authorized by a judicial or administrative order. To facilitate the lawful intercept process, certain legislation and regulations require service providers (SPs) and Internet service providers (ISPs) to implement their networks to explicitly support authorized electronic surveillance.

The surveillance is performed through the use of wiretaps on traditional telecommunications and Internet services in voice, data, and multiservice networks. The LEA delivers a request for a wiretap to the target's service provider, who is responsible for intercepting data communication to and from the individual. The service provider uses the target's IP address or session to determine which of its edge routers handles the target's traffic (data communication). The service provider then intercepts the target's traffic as it passes through the router, and sends a copy of the intercepted traffic to the LEA without the target's knowledge.

The Lawful Intercept feature supports the Communications Assistance for Law Enforcement Act (CALEA), which describes how service providers in the United States must support lawful intercept. Currently, lawful intercept is defined by the following standards:

- Telephone Industry Association (TIA) specification J-STD-025
- Packet Cable Electronic Surveillance Specification (PKT-SP-ESP-101-991229)

For information about the Cisco lawful intercept solution, contact your Cisco account representative.

Lawful intercept support on the Cisco GGSN provides the following benefits:

- Allows multiple LEAs to run a lawful intercept on the same target without each other's knowledge.
- Does not affect subscriber services on the GGSN.
- Supports wiretaps in both the input and output direction.
- Supports wiretaps of Layer 3 and Layer 2 traffic.
- Cannot be detected by the target. Neither the network administrator nor the calling parties is aware that packets are being copied or that the call is being tapped.
- ***Uses Simple Network Management Protocol Version 3 (SNMPv3) and security features such as the View-based Access Control Model (SNMP-VACM-MIB) and User-based Security Model (SNMP-USM-MIB) to restrict access to lawful intercept information and components.***
- Hides information about lawful intercepts from all but the most privileged users. An administrator must set up access rights to enable privileged users to access lawful intercept information.
- Provides two secure interfaces for performing an intercept: one for setting up the wiretap and one for sending the intercepted traffic to the LEA.

Network Components Used for Lawful Intercept

The following network components are used for lawful intercepts:

- **Mediation Device—**A mediation device (supplied by a third-party vendor) handles most of the processing for the lawful intercept. The mediation device:
  - Provides the interface used to set up and provision the lawful intercept.
  - Generates requests to other network devices to set up and run the lawful intercept.
  - Converts the intercepted traffic into the format required by the LEA (which can vary from country to country) and sends a copy of the intercepted traffic to the LEA without the target's knowledge.

Note If multiple LEAs are performing intercepts on the same target, the mediation device must make a copy of the intercepted traffic for each LEA. The mediation device is also responsible for restarting any lawful intercepts that are disrupted due to a failure.

- **Intercept Access Point**—An intercept access point (IAP) is a device that provides information for the lawful intercept. There are two types of IAPs:
  - Identification (ID) IAP—A device, such as an authentication, authorization, and accounting (AAA) server, that provides intercept-related information (IRI) for the intercept (for example, the target's username and system IP address). The IRI helps the service provider determine which content IAP (router) the target's traffic passes through.
  - Content IAP—A device, such as a Cisco 7600 series router, that the target's traffic passes through. The content IAP:

    - Intercepts traffic to and from the target for the length of time specified in the court order. The router continues to forward traffic to its destination to ensure that the wiretap is undetected.

    - Creates a copy of the intercepted traffic, encapsulates it in User Datagram Protocol (UDP) packets, and forwards the packets to the mediation device without the target's knowledge.

    Note The content IAP sends a single copy of intercepted traffic to the mediation device. If multiple LEAs are performing intercepts on the same target, the mediation device must make a copy of the intercepted traffic for each LEA.

- **Collection Function**—The collection function is a program that stores and processes traffic intercepted by the service provider. The program runs on equipment at the LEA.

Lawful Intercept Processing

After acquiring a court order or warrant to perform surveillance, the LEA delivers a surveillance request to the target's service provider. Service provider personnel use an admin function that runs on the mediation device to configure a lawful intercept to monitor the target's electronic traffic for a specific period of time (as defined in the court order).

After the intercept is configured, user intervention is no longer required. The admin function communicates with other network devices to set up and execute the lawful intercept. The following sequence of events occurs during a lawful intercept:

1. The admin function contacts the ID IAP for intercept-related information (IRI), such as the target's username and the IP address of the system, to determine which content IAP (router) the target's traffic passes through.
2. After identifying the router that handles the target's traffic, the admin function sends SNMPv3 get and set requests to the router's MIBs to set up and activate the lawful intercept. The GGSN lawful intercept MIBs include the CISCO-TAP2-MIB and the CISCO-MOBILITY-TAP-MIB.
3. During the lawful intercept, the router:
   a. Examines incoming and outgoing traffic and intercepts any traffic that matches the specifications of the lawful intercept request.
   b. Creates a copy of the intercepted traffic and forwards the original traffic to its destination so the target does not suspect anything.
   c. Encapsulates the intercepted traffic in UDP packets and forwards the packets to the mediation device without the target's knowledge.

   Note The process of intercepting and duplicating the target's traffic adds no detectable latency in the traffic stream.

4. The mediation device converts the intercepted traffic into the required format and sends it to a collection function running at the LEA. Here, the intercepted traffic is stored and processed.

   Note If the router intercepts traffic that is not allowed by the judicial order, the mediation device filters out the excess traffic and sends the LEA only the traffic allowed by the judicial order.

5. When the lawful intercept expires, the router stops intercepting the target's traffic.

Lawful Intercept MIBs

To perform lawful intercept, the GGSN uses the following MIBs:

- **CISCO-TAP2-MIB**—The CISCO-TAP2-MIB contains SNMP management objects that control lawful intercepts on the router. The mediation device uses the MIB to configure and run lawful intercepts on targets whose traffic passes through the router. The MIB is bundled with Cisco software images that support lawful intercept.

  The CISCO-TAP2-MIB contains several tables that provide information for lawful intercepts that are running on the router:

  – cTap2MediationTable—Contains information about each mediation device that is currently running a lawful intercept on the router. Each table entry provides information that the router uses to communicate with the mediation device (for example, the device's address, the interfaces to send intercepted traffic over, and the protocol to transmit the intercepted traffic).

  – cTap2StreamTable—Contains information used to identify the traffic to intercept. Each table entry contains a pointer to a filter that is used to identify the traffic stream associated with the target of a lawful intercept. Traffic that matches the filter is intercepted, copied, and sent to the corresponding mediation device application (cTap2MediationContentId).

  – The table also contains counts of the number of packets that were intercepted, and counts of dropped packets that should have been intercepted, but were not.

  – cTap2DebugTable—Contains debug information for troubleshooting lawful intercept errors.

  The CISCO-TAP2-MIB also contains several SNMP notifications for lawful intercept events. For detailed descriptions of MIB objects, see the MIB itself.

  The admin function (running on the mediation device) issues SNMPv3 **set** and **get** requests to the router's CISCO-TAP2-MIB to set up and initiate a lawful intercept. To do this, the admin function performs the following actions:

  a. Creates a cTap2MediationTable entry to define how the router is to communicate with the mediation device executing the intercept.

     Note The cTap2MediationNewIndex object provides a unique index for the mediation table entry.

  b. Creates an entry in the cTap2StreamTable to identify the traffic stream to intercept.

  c. Creates an entry in the cmTapStreamTable and sets the cmTapStreamStatus to active (1).

  d. Sets cTap2StreamInterceptEnable to true(1) to start the intercept. The router intercepts traffic in the stream until the intercept expires (cTap2MediationTimeout).

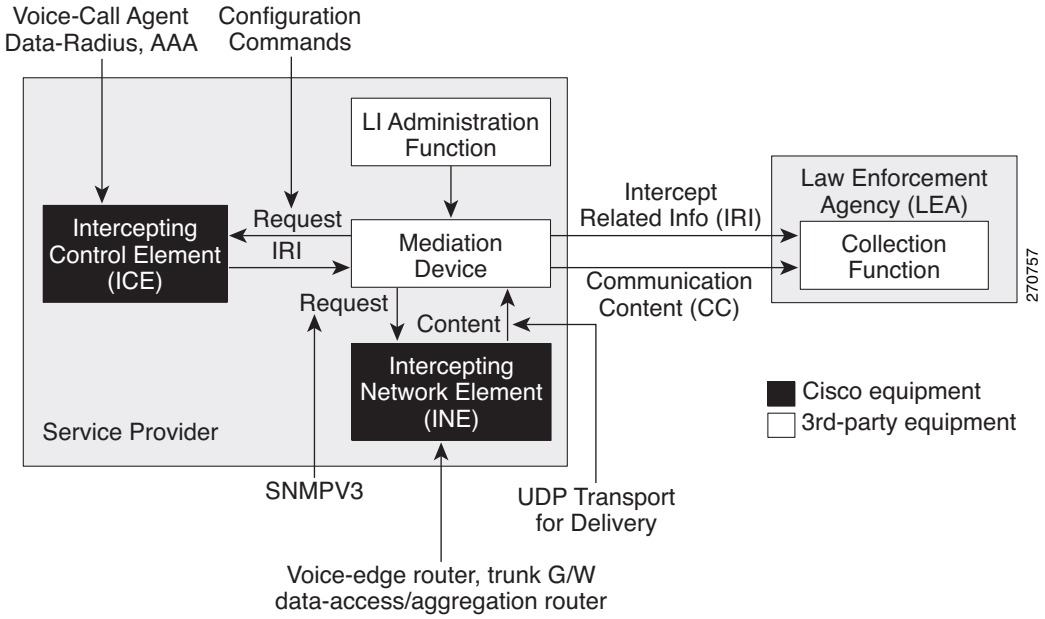
- **CISCO-MOBILITY-TAP-MIB—**The CISCO-MOBILITY-TAP-MIB contains the SNMP management objects to configure and execute wiretaps on mobility gateway traffic.

  The CISCO-MOBILITY-TAP-MIB contains the cmtapStreamTable (the Mobility Stream table) that lists the data streams to be intercepted. The same data stream might be required by multiple taps. This table essentially provides options for packet selection, only some of which might be used. For example, if all of the traffic to or from a subscriber is to be intercepted, an entry listing would be configured listing the SubscriberID along with the SubscriberIDType corresponding to the stream to be intercepted. (More details can be found in CISCO-MOBILITY-TAP-MIB.)

Lawful Intercept Topology

The following illustration shows intercept access points and interfaces in a lawful intercept topology for both voice and data interception (Figure 1).

Figure 12-1 Lawful Intercept Topologies



Configuring Lawful Intercept Support

This section contains the following information:

- Prerequisites, page 12-41
- Security Considerations, page 12-41
- Configuration Guidelines and Limitations, page 12-41
- Accessing the Lawful Intercept MIBs, page 12-42
- Configuring SNMPv3, page 12-43

- Creating a Restricted SNMP View of Lawful Intercept MIBs, page 12-43
- Configuring the Cisco GGSN to Send SNMP Notifications for Lawful Intercept, page 12-45

Prerequisites

To configure support for lawful intercept, the following prerequisites must be met:

- You must be logged in to the GGSN with the highest access level (level 15). To log in with level-15 access, enter the **enable** command and specify the highest-level password defined for the router.
- You must issue commands in global configuration mode. Enter **config** to enter global configuration mode.
- (Optional) It might be helpful to use a loopback interface for the interface through which the GGSN communicates with the mediation device.
- The mediation device must be provisioned. For detailed information, see the vendor documentation associated with your mediation device. For a list of Cisco-preferred mediation device equipment suppliers, see http://www.cisco.com/wwl/regaffairs/lawful_intercept/index.html.

Security Considerations

Consider the following security issues as you configure the GGSN for lawful intercept support:

- SNMP notifications for lawful intercept must be sent to User Datagram Protocol (UDP) port 161 on the mediation device, not port 162 (which is the Simple Network Management Protocol (SNMP) default). See the "Configuring the Cisco GGSN to Send SNMP Notifications for Lawful Intercept" section on page 12-45 for instructions.
- The only users who should be allowed to access the lawful intercept MIBs are the mediation device and system administrators who need to know about lawful intercepts on the router. In addition, these users must have authPriv or authNoPriv access rights to access the lawful intercept MIBs. Users with NoAuthNoPriv access cannot access the lawful intercept MIBs.
- The default SNMP view excludes the following MIBs:

  CISCO-TAP2-MIB
  CISCO-MOBILITY-TAP-MIB

Configuration Guidelines and Limitations

This section and the sections that follow describe the general limitations and configuration guidelines for lawful intercept, Cisco GGSN-specific guidelines, and per-subscriber guidelines.

- To maintain GGSN performance, lawful intercept is limited to no more than 0.2% of active sessions. For example, if the GGSN is handling 4000 sessions, 8 of those sessions can be intercepted.
- **General Configuration Guidelines**—For the GGSN to communicate with the mediation device to execute a lawful intercept, the following configuration requirements must be met:
  - The domain name for both the GGSN and the mediation device must be registered in the Domain Name System (DNS).
  - In DNS, the router IP address is typically the address of the FastEthernet0/0/0 interface on the router.
  - The mediation device must have an access function (AF) and an access function provisioning interface (AFPI).

  - You must add the mediation device to the SNMP user group that has access to the CISCO-TAP2-MIB view. Specify the username of the mediation device as the user to add to the group.
  - When you add the mediation device as a CISCO-TAP2-MIB user, you can include the mediation device's authorization password if you want. The password must be at least eight characters in length.
- **MIB Guidelines**—The following Cisco MIBs are used for lawful intercept processing. Include these MIBs in the SNMP view of lawful intercept MIBs to enable the mediation device to configure and execute wiretaps on traffic that flows through the router.
  - CISCO-TAP2-MIB—Required for both types of lawful intercepts: regular and broadband.
  - CISCO-MOBILITY-TAP-MIB—Required for wiretaps on mobility gateway traffic.
- **Cisco GGSN Configuration Guidelines and Limitations**—The following is a list of configuration guidelines for regular lawful intercept on the Cisco GGSN:
  - Lawful intercept can intercept traffic at a rate of 6000 packets per second (pps) without affecting the packet forwarding rate. This intercept rate includes all active intercepts and assumes that packets are 150 to 200 bytes long. If the intercept rate exceeds 6000 pps, the packet forwarding rate will decrease slightly because lawful intercept is processor intensive.
  - Lawful intercept is not supported on Layer 2 interfaces. However, lawful intercept can intercept traffic on VLANs that run over the Layer 2 interface if the VLAN interface is a Layer 3 interface and traffic is routed by the VLAN interface.
  - Packets that are subject to hardware rate limiting are processed by lawful intercept as follows:
  - Packets that are dropped by the rate limiter are not intercepted or processed.
  - Packets that are passed by the rate limiter are intercepted and processed.
  - If multiple law enforcement agencies (LEAs) are using a single mediation device and each is executing a wiretap on the same target, the router sends a single packet to the mediation device. It is up to the mediation device to duplicate the packet for each LEA.
  - Lawful intercept on the GGSN is based on the subscriber IMSI value as described in CISCO-MOBILITY-MIB.

Accessing the Lawful Intercept MIBs

Due to its sensitive nature, the Cisco lawful intercept MIBs are only available in software images that support the lawful intercept feature. These MIBs are not accessible through the Network Management Software MIBs Support page (http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml).

Restricting Access to the Lawful Intercept MIBs

Only the mediation device and users who need to know about lawful intercepts should be allowed to access the lawful intercept MIBs. To restrict access to these MIBs, you must:

1. Create a view that includes the Cisco lawful intercept MIBs.
2. Create an SNMP user group that has read-and-write access to the view. Only users assigned to this user group can access information in the MIBs.

3. Add users to the Cisco lawful intercept user groups to define who can access the MIBs and any information related to lawful intercepts. Be sure to add the mediation device as a user in this group; otherwise, the router cannot perform lawful intercepts.

Note Access to the Cisco lawful intercept MIB view should be restricted to the mediation device and to system administrators who need to be aware of lawful intercepts on the router. To access the MIB, users must have level-15 access rights on the router.

Configuring SNMPv3

To perform the following procedures, SNMPv3 must be configured on the GGSN. For information about how to configure SNMPv3, and for detailed information about the commands described in the sections that follow, see the following Cisco documents:

- *Cisco IOS Configuration Fundamentals Configuration Guide*, Part 3: System Management, "Configuring SNMP Support" section, available at the following URL:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/ffun_c/fcfprt3/fcf014.htm

- *Cisco IOS Configuration Fundamentals and Network Management Command Reference*, available at the following URL:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/fun_r/cfr_1g11.htm

Creating a Restricted SNMP View of Lawful Intercept MIBs

To create and assign users to an SNMP view that includes the Cisco lawful intercept MIBs, perform the following procedure at the CLI, in global configuration mode with level-15 access rights. For command examples, see the "Configuration Example" section on page 12-44.

Note The command syntax in the following steps includes only those keywords required to perform each task. For details on command syntax, see the documents listed in the previous section ("Configuring SNMPv3").

Step 1 Make sure that SNMPv3 is configured on the GGSN. For instructions, see the documents listed in the "Configuring SNMPv3" section on page 12-43.

Step 2 Create an SNMP view that includes the CISCO-TAP2-MIB (where *view_name* is the name of the view to create for the MIB). This MIB is required for both regular and broadband lawful intercept.

```
Router(config)# snmp-server view view_name ciscoTap2MIB included
```

Step 3 Add the following MIB to the SNMP view to configure support for wiretaps on mobility gateway streams (where *view_name* is the name of the view you created in Step 2).

```
Router(config)# snmp-server view view_name ciscoMobilityTapMIB included
```

Step 4 Create an SNMP user group (*groupname*) that has access to the lawful intercept MIB view and define the group's access rights to the view.

```
Router(config)# snmp-server group groupname v3 auth read view_name write view_name
notify notify-view
```

Step 5 Add users to the user group you just created (where *username* is the user, *groupname* is the user group, and *auth_password* is the authentication password):

```
Router(config)# snmp-server user username groupname v3 auth md5 auth_password
```

Note Both the **priv** and **auth** keyword options are valid options when adding users.

Note Be sure to add the mediation device to the SNMP user group; otherwise, the router cannot perform lawful intercepts. Access to the lawful intercept MIB view should be restricted to the mediation device and to system administrators who need to know about lawful intercepts on the router.

Step 6 Specify the host from which the user will be allowed to connect:

```
Router(config)# snmp-server host ip-address version 3 auth user-name
```

Step 7 Specify the engine identifier:

```
Router(config)# snmp-server engineID local engine-ID
```

The mediation device is now able to access the lawful intercept MIBs, and issue SNMP **set** and **get** requests to configure and run lawful intercepts on the router.

For instructions on how to configure the router to send SNMP notifications to the mediation device, see the "Configuring the Cisco GGSN to Send SNMP Notifications for Lawful Intercept" section on page 12-45.

Configuration Example

The following commands show an example of how to enable the mediation device to access the lawful intercept MIBs.

```
Router(config)# snmp-server view tapV ciscoTap2MIB included
Router(config)# snmp-server view tapV ciscoMobilityTapMIB included
Router(config)# snmp-server group tapGrp v3 auth read tapV write tapV notify tapV
Router(config)# snmp-server user ss8user tapGrp v3 auth md5 ss8passwd
Router(config)# snmp-server host 172.10.10.1 version 3 auth ss8usr
Router(config)# snmp-server engineID local 0123467891
```

1. Create a view (tapV) that includes the appropriate lawful intercept MIBs (CISCO-TAP2-MIB and CISCO-MOBILITY-TAP-MIB).
2. Create a user group (tapGrp) that has read, write, and notify access to MIBs in the tapV view.
3. Add the mediation device (ss8user) to the user group, and specify MD5 authentication with a password (ss8passwd).
4. (Optional) Assign a 24-character SNMP engine ID (for example, 123400000000000000000000) to the router for administration purposes. If you do not specify an engine ID, one is automatically generated. You can omit the trailing zeros from the engine ID, as shown in the last line of the example above.

Note Changing an engine ID has consequences for SNMP user passwords and community strings.

Configuring the Cisco GGSN to Send SNMP Notifications for Lawful Intercept

SNMP automatically generates notifications for lawful intercept events (see Table 12-2). This is because the default value of the cTap2MediationNotificationEnable object is true(1).

To configure the GGSN to send lawful intercept notifications to the mediation device, issue the following commands in global-configuration mode with level-15 access rights (where *MD-ip-address* is the IP address of the mediation device and *community-string* is the password-like community string to send with the notification request):

```
Router(config)# snmp-server host MD-ip-address community-string udp-port 161 snmp
```

- For lawful intercept, **udp-port** must be 161 and not 162 (the SNMP default).

Table 12-2 lists the SNMP notifications generated for lawful intercept events.

Table 12-2 SNMP Notifications for Lawful Intercept Events

Notification	Description
cTap2MIBActive	The router is ready to intercept packets for a traffic stream configured in the CISCO-TAP2-MIB.
cTap2MediationTimedOut	A lawful intercept was terminated (for example, because cTap2MediationTimeout expired).
cTap2MediationDebug	Debugging information for events related to cTap2MediationTable entries.
cTap2StreamDebug	Debugging information for events related to cTap2StreamTable entries.
cTap2Switchover	A redundant, active route processor (RP) is going into standby mode and the standby is the active RP.

Disabling SNMP Notifications

You can disable SNMP notifications on the GGSN as follows:

- To disable all SNMP notifications, issue the **no snmp-server enable traps** command.
- To disable lawful intercept notifications, use SNMPv3 to set the CISCO-TAP2-MIB object cTap2MediationNotificationEnable to false(2). To re-enable lawful intercept notifications through SNMPv3, reset the object to true(1).

Configuration Examples

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

- AAA Security Configuration Example, page 12-46
- RADIUS Server Global Configuration Example, page 12-46
- RADIUS Server Group Configuration Example, page 12-46
- RADIUS Response Message Configuration Example, page 12-48
- Address Verification and Mobile-to-Mobile Traffic Redirection Example, page 12-49
- “Periodic Accounting Timer Example” section on page 12-52

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, see *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, see *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 is 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 SAMI 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
!
...
```

Periodic Accounting Timer Example

The following example shows a period accounting timer configured at the APN level and globally.

```
gprs default aaa-accounting interim periodic 60
!
gprs access-point-list APLIST
  access-point 100
   access-point-name peracct.com
   access-mode non-transparent
   aaa-accounting interim update
   aaa-accounting interim periodic 15
   aaa-group authentication radaccess
   aaa-group accounting default
   ip-address-pool radius-client
   gtp response-message wait-accounting
!
```