Cisco ASR 5000 Series IP Services Gateway Administration Guide

Version 10.0

Last updated June 30, 2010

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-22961-01

Cisco ASR 5000 Series IP Services Gateway Administration Guide

CONTENTS

About this Guide v
Conventions Used vi
Contacting Customer Support viii
IP Services Gateway Overview 9
Introduction 10
Service Modes 11
RADIUS Server Mode 11
RADIUS Proxy 12
RADIUS Snoop Mode 12
In-line Services 14
Enhanced Charging Service 14
Content Filtering 14
Peer-to-Peer 14
Enhanced Feature Support 15
IMS Authorization Service 15
Content Service Steering 16
Multiple IPSG Services 16
Session Recovery 16
Configuring the IP Services Gateway 17
Configuration Requirements for the IPSG 18
Required Configuration File Components 19
Required Component Information 19
Configuring the IPSG 21
IPSG Context and Service Configuration 22
Option 1: RADIUS Server Mode Configuration 22
Option 2: RADIUS Server with Proxy Mode Configuration 22
Option 3: RADIUS Snoop Mode Configuration 24
Gx Interface Configuration 24
Gy Interface Configuration 25
ISP Context Configuration 26
Creating the ISP Context 26
Saving the Configuration 27
Verifying and Saving Your Configuration 29
Verifying the Configuration 30
Feature Configuration 30
Service Configuration 31
Context Configuration 32
System Configuration 32
Finding Configuration Errors 32
Saving the Configuration 34
Saving the Configuration on the Chassis 35
IPSG Engineering Rules 37
IPSG Context and Service Rules 38
IPSG RADIUS Messaging Rules 39

About this Guide

This document pertains to features and functionality that run on and/or that are related to the Cisco® ASR 5000 Chassis, formerly the Starent Networks ST40.

Conventions Used

The following tables describe the conventions used throughout this documentation.

Icon	Notice Type	Description
	Information Note	Provides information about important features or instructions.
	Caution	Alerts you of potential damage to a program, device, or system.
	Warning	Alerts you of potential personal injury or fatality. May also alert you of potential electrical hazards.
	Electro-Static Discharge (ESD)	Alerts you to take proper grounding precautions before handling a product.

Typeface Conventions	Description
Text represented as a `screen display`	This typeface represents displays that appear on your terminal screen, for example: `Login:`
Text represented as **`commands`**	This typeface represents commands that you enter, for example: **`show ip access-list`** This document always gives the full form of a command in lowercase letters. Commands are not case sensitive.
Text represented as a **`command`** *`variable`*	This typeface represents a variable that is part of a command, for example: **`show card`** *`slot_number`* slot_number is a variable representing the desired chassis slot number.
Text represented as menu or sub-menu names	This typeface represents menus and sub-menus that you access within a software application, for example: Click the File menu, then click New

Command Syntax Conventions	Description
{ **`keyword`** or *`variable`* }	Required keywords and variables are surrounded by grouped brackets. Required keywords and variables are those components that are required to be entered as part of the command syntax.

Command Syntax Conventions	Description
[**keyword** or *variable*]	Optional keywords or variables, or those that a user may or may not choose to use, are surrounded by square brackets.
|	With some commands there may be a group of variables from which the user chooses one. These are called alternative variables and are documented by separating each variable with a vertical bar (also known as a pipe filter). Pipe filters can be used in conjunction with required or optional keywords or variables. For example: **{ nonce | timestamp }** OR [**count** *number_of_packets* | **size** *number_of_bytes*]

Contacting Customer Support

Use the information in this section to contact customer support.

For New Customers: Refer to the support area of http://www.cisco.com for up-to-date product documentation or to submit a service request. A valid username and password is required to this site. Please contact your local sales or service representative for additional information.

For Existing Customers with support contracts through Starent Networks: Refer to the support area of https://support.starentnetworks.com/ for up-to-date product documentation or to submit a service request. A valid username and password is required to this site. Please contact your local sales or service representative for additional information.

IMPORTANT: For warranty and repair information, please be sure to include the Return Material Authorization (RMA) tracking number on the outside of the package.

Chapter 1
IP Services Gateway Overview

This chapter provides an overview of the IP Services Gateway (IPSG).

This chapter covers the following topics:

- Introduction
- Service Modes
- In-line Services
- Enhanced Feature Support

Introduction

The IP Services Gateway (IPSG) is a stand-alone device capable of providing managed services to IP flows. The IPSG is situated on the network side of legacy, non-service capable GGSNs, PDSNs, HAs, and other subscriber management devices. The IPSG can provide per-subscriber services such as enhanced charging, stateful firewall, traffic performance optimization, and others.

The IPSG allows the carrier to roll out advanced services without requiring a replacement of the HA, PDSN, GGSN, or other access gateways and eliminates the need to add multiple servers to support additional services.


IMPORTANT: The IPSG is a license-dependent feature.

Service Modes

The IPSG supports the following service modes:

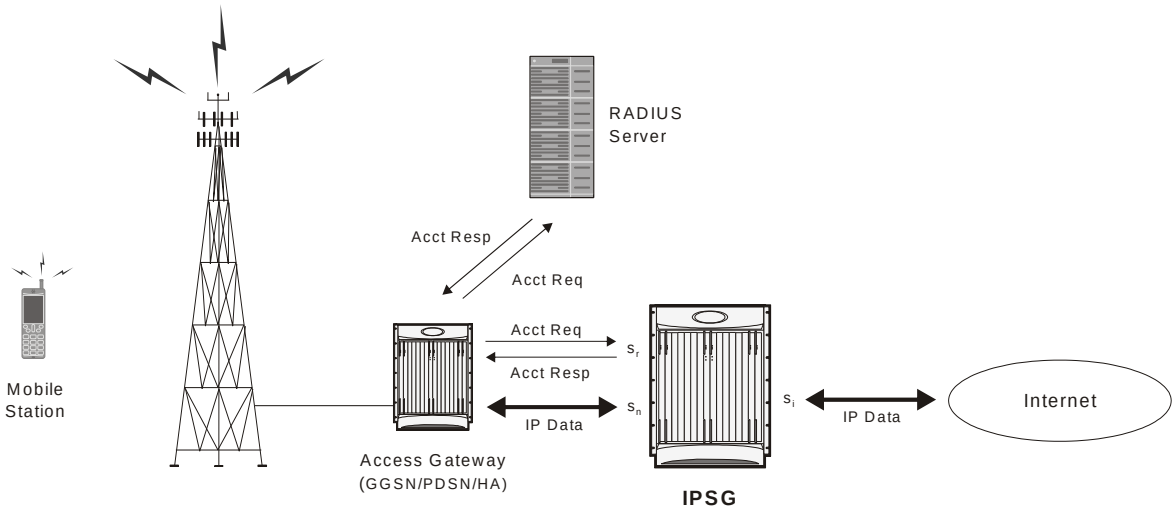
- RADIUS Server Mode
- RADIUS Snoop Mode

RADIUS Server Mode

When configured in RADIUS server mode, the IPSG inspects identical RADIUS accounting request packets sent to the RADIUS accounting server and the IPSG simultaneously.

As shown in the following figure, the IPSG inspects the RADIUS accounting request, extracts the required user information, then sends a RADIUS accounting response message back to the access gateway. The IPSG has three reference points: sn, si, and sr. The sn interface transmits/receives data packets to/from the access gateway (GGSN, HA, PDSN, etc.). The si interface transmits/receives data packets to/from the Internet or a packet data network. The sr interface receives RADIUS accounting requests from the access gateway. The system inspects the accounting request packets and extracts information to be used to determine the appropriate service(s) to apply to the flow.

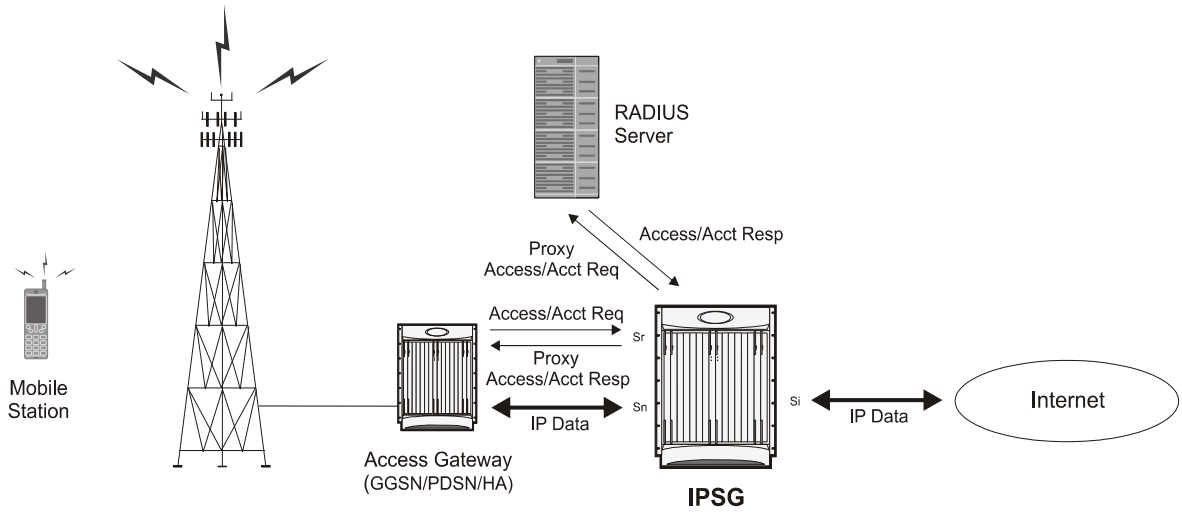
Figure 1. IPSG Message/Data Flow (RADIUS Server Mode)



RADIUS Proxy

In the event that the Access Gateway is incapable of sending two separate RADIUS Start message, the IPSG can be configured as a RADIUS Proxy. As shown in the following figure, the IPSG receives an IPSG RADIUS proxy Access request, then generates the Authentication and Accounting requests to the AAA Server.

Figure 2. IPSG Message/Data Flow (RADIUS Server Mode - RADIUS Proxy)

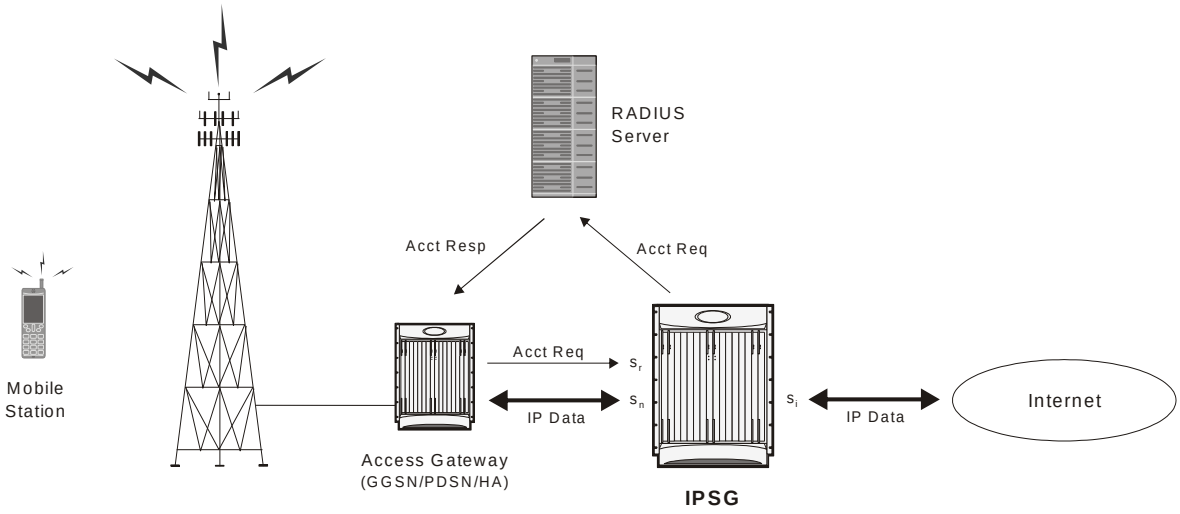


RADIUS Snoop Mode

When configured in RADIUS snoop mode, the IPSG simply inspects RADIUS accounting request packets sent to a RADIUS server through the IPSG.

As shown in the following figure, the IPSG has three reference points: sn, si, and sr. The sn interface transmits/receives data packets to/from the access gateway (GGSN, HA, PDSN, etc.). The si interface transmits/receives data packets to/from the Internet or a packet data network. The sr interface receives RADIUS accounting requests from the access gateway. The system inspects the accounting request packets and extracts information to be used to determine the appropriate service(s) to apply to the flow. Information is not extracted from the RADIUS accounting responses so they are sent directly to the access gateway by the RADIUS Server, but can also be sent back through the IPSG.

Figure 3. IPSG Message/Data Flow (RADIUS Snoop Mode)



In-line Services

As described previously, the IPSG provides a method of inspecting RADIUS packets to discover user identity for the purpose of applying enhanced services to the subsequent data flow. Internal applications such as the Enhanced Charging Service, Content Filtering, and Peer-to-Peer Detection are primary features that take advantage of the IPSG service.

Enhanced Charging Service

Enhanced Charging Service (ECS)/Active Charging Service (ACS) is the primary vehicle performing packet inspection and applying rules to the session which includes the delivery of enhanced services.

For more information, refer to the *Enhanced Charging Service Administration Guide*.

Content Filtering

Content Filtering is an in-line service feature that filters HTTP and WAP requests from mobile subscribers based on the URLs in the requests. This enables operators to filter and control the content that an individual subscriber can access, so that subscribers are inadvertently not exposed to universally unacceptable content and/or content inappropriate as per the subscribers' preferences.

For more information, refer to the *Content Filtering Services Administration Guide*.

Peer-to-Peer

Peer-to-Peer is an in-line service feature that detects peer-to-peer protocols in real time and applies actions such as permitting, blocking, charging, bandwidth control, and TOS marking.

For more information, refer to the *Peer-to-Peer Detection Administration Guide*.

Enhanced Feature Support

This section describes the enhanced features supported by IPSG.

IMS Authorization Service

To support roaming IMS subscribers in a GPRS/UMTS network, the IPSG must be able to charge only for the amount of resources consumed by the particular IMS application and bandwidth used. The IPSG must also allow for the provisioning and control of the resources used by the IMS subscriber. To facilitate this, the IPSG supports the R7 Gx interface to a Policy Control and Charging Rule Function (PCRF).

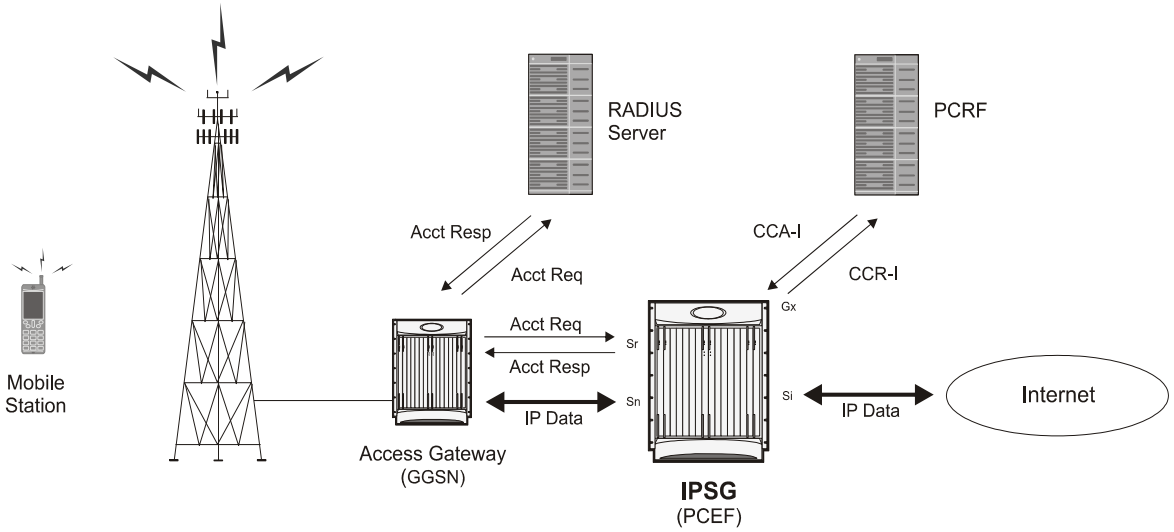
For detailed information on the Gx Interface support, refer to the *Gx Interface Support* chapter of the *System Enhanced Feature Configuration Guide*.

Note the following for IPSG:

- Only single bearer/session concept is supported. Multiple bearer concept is not applicable.
- Only PCRF binding is applicable. PCEF binding is not applicable.

The following figure shows the interface and basic message flow of the Gx interface.

Figure 4. PSG Message/Data Flow (RADIUS Server Mode - IMS Auth Service)



IPSG also supports IMS Authorization Service Session Recovery with the following limitations:

- Active calls only
- The number of rules recovered is limited to the following:

  - 3 flow-descriptions per charging-rule-definition
  - 3 Charging-rule-definitions per PDP context
- The above are combined limits for opened/closed gates and for uplink and downlink rules. IMSA sessions with rules more than the above are not recoverable.

Content Service Steering

Content Service Steering (CSS), defines how traffic is handled by the system based on the content of the data presented by a mobile subscriber. CSS can be used to direct traffic to in-line services that are internal to the system. CSS controls how subscriber data is forwarded to a particular in-line service, but does not control the content.

IPSG supports steering subscriber sessions to Content Filtering Service based on their policy setting. If a subscriber does not have a policy setting (ACL name) requiring Content Filtering, their session will bypass the Content Filtering Service and will be routed on to the destination address.

If subscriber policy entitlements indicate filtering is required for a subscriber, CSS will be used to steer subscriber sessions to the Content Filtering in-line service.

If a subscriber is using a mobile application with protocol type not supported, their session will bypass the Content Filtering Service and will be efficiently routed on to destination address.

For more information regarding CSS, refer to the *Content Service Steering* chapter of the *System Enhanced Feature Configuration Guide*.

Multiple IPSG Services

Multiple IPSG services, can be configured on the system in different contexts. Both source and destination contexts should be different for the different IPSG services. Each such IPSG service functions independently as an IPSG.

Session Recovery

The Session Recovery feature provides seamless failover and reconstruction of subscriber session information in the event of a hardware or software fault within the system preventing a fully connected user session from being disconnected.

For more information on this feature, please refer to the *Session Recovery* chapter in the *System Enhanced Feature Configuration Guide*.

Inter-Chassis Session Recovery is not supported.

Chapter 2
Configuring the IP Services Gateway

This chapter describes how to configure the IPSG.

This chapter covers the following topics:

- Configuration Requirements for the IPSG
- Configuring the IPSG

Configuration Requirements for the IPSG

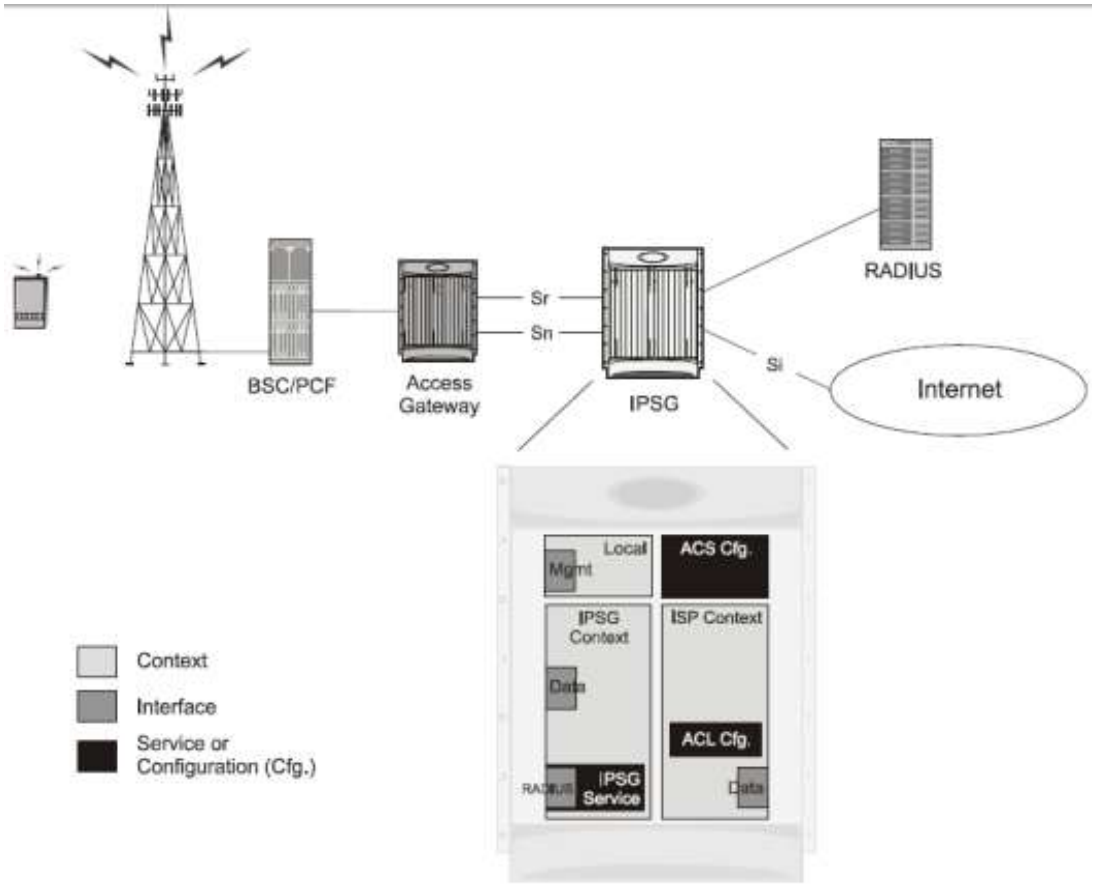
This section provides a high-level description of the configuration requirements of the IPSG.

The Snoop and Server methods use the same configuration components and differ only in how the IPSG service is configured.

The IPSG can be configured in various ways such as by creating a single context with interfaces for the RADIUS messages and both inbound and outbound data traffic. The following figure presents another method in which the IPSG context manages communication with the access gateway for both RADIUS messaging and inbound data traffic. The ISP context is responsible for all outbound data traffic.

The following figure also shows other important components such as IP access control lists (ACLs) in both contexts as well as an Active Charging Service (ACS) configuration.

Figure 5. IPSG Support



Required Configuration File Components

The following configuration components are required to complete an IPSG configuration file:

- IPSG License
- Card Activations
- Local Context Modifications
    - Network Management Interface
    - Remote Management
    - Administrative Users
- Global Active Charging Service Configuration
- IPSG Context
    - IPSG Service
    - RADIUS Server or Client Configuration
    - Interface for RADIUS messages to/from access gateway
    - Interface for data traffic to/from access gateway
- Service Provider Context
    - IP ACL Configuration
    - Interface for data traffic to/from access gateway
- Port Configuration (bindings)

Required Component Information

Prior to configuring the system, determine the following information:

- Context names
- Service names
- Active Charging Service
    - Rule definitions
    - Rulebase name
- IMS Auth Service
- RADIUS accounting client IP address, dictionary type, and shared secret (RADIUS Server Mode)
- RADIUS accounting server IP address and dictionary type (RADIUS Snoop Mode)
- All Interfaces and ports
    - Interface IP addresses
    - Interface names

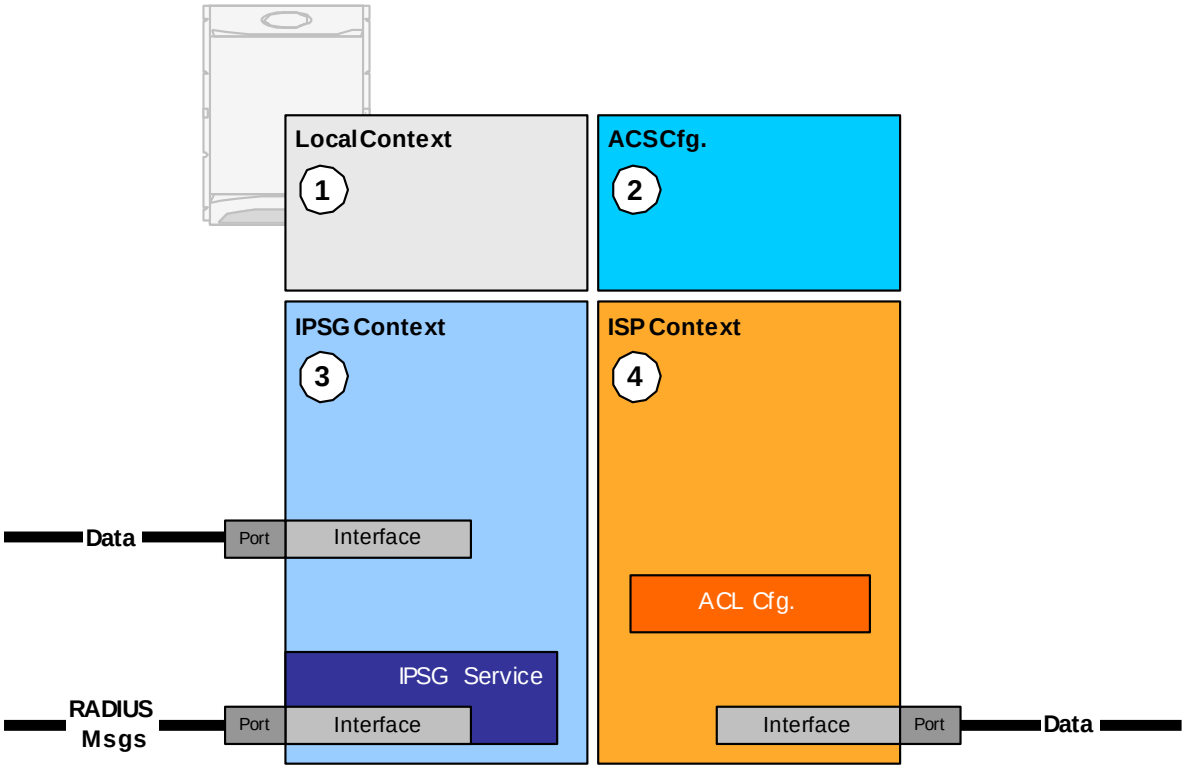
- Port names
- Port numbers

For a complete understanding of the required information for all configuration mode commands, refer to the *Command Line Interface Reference*.

Configuring the IPSG

This section describes how to configure the IPSG to accept RADIUS accounting requests (start messages) in order to extract user information used to apply other services. The following figure illustrates the required components within the system supporting IPSG.

Figure 6. IPSG Configuration Detail



To configure the system to perform as an IPSG:

Step 1 Set initial configuration parameters such as activating processing cards and modifying the local context by referring to procedures in the *System Administration Guide*.

Step 2 Configure the global active charging parameters as described in the *Enhanced Charging Services Administration Guide*.

Step 3 Configure the system to perform as an IPSG by applying the example configurations presented in the IPSG Context and Service Configuration section.

Step 4 Configure the Service Provider context by applying the example configuration presented in the ISP Context Configuration section.

Step 5 Bind interfaces to ports by referring to procedures in the *GGSN Administration Guide*.

Step 6 Save the configuration as described in the *Saving your Configuration* section.

IMPORTANT: Commands used in the configuration examples in this section provide base functionality to the extent that the most common or likely commands and/or keyword options are presented. In many cases, other optional commands and/or keyword options are available. Refer to the *Command Line Interface Reference* for complete information regarding all commands.

IPSG Context and Service Configuration

To configure IPSG context and service:

Step 1 Create an IPSG context and the IPSG service by applying the example configuration in one of the following sections as required:

- Option 1: RADIUS Server Mode Configuration
- Option 2: RADIUS Server with Proxy Mode Configuration
- Option 3: RADIUS Snoop Mode Configuration

Step 2 Create two interfaces within the IPSG context for communication with the access gateway by referring to the *Creating and Configuring Ethernet Interfaces and Ports* procedure in the *GGSN Administration Guide*.

Option 1: RADIUS Server Mode Configuration

To create an IPSG context and IPSG service in RADIUS Server Mode, use the following configuration:

```
configure

   context <ipsg_context_name>

      ipsg-service <service_name> mode radius-server

         bind address <ip_address>

         radius dictionary <dictionary>

         radius accounting client <ip_address> [ encrypted ] key <secret> [
dictionary <dictionary> ] [ disconnect-message [ dest-port <port_num> ] ]

         end
```

Option 2: RADIUS Server with Proxy Mode Configuration

To create an IPSG context and IPSG service in RADIUS Server Mode with IPSG authentication and accounting proxy configuration, use the following configuration:

```
configure

   context <ipsg_context_name>

      ipsg-service <service_name> mode radius-server

         bind address <ip_address>

         radius dictionary <dictionary>

         radius accounting client <ip_address> [ encrypted ] key <secret> [
dictionary <dictionary> ] [ disconnect-message [ dest-port <port_num> ] ]

# IPSG Authentication Proxy Configuration:

         bind authentication-proxy address <ip_address>

         connection authorization [ encrypted ] password <password>

         radius dictionary <dictionary>

         radius accounting client <ip_address> [ encrypted ] key <secret> [
dictionary <dictionary> ] [ disconnect-message [ dest-port <port_num> ] ]

         exit

      aaa group default

         radius attribute nas-ip-address address <ip_address>

         radius dictionary <dictionary>

         radius server <ip_address> [ encrypted ] key <key> port <port>

         radius accounting server <ip_address> [ encrypted ] key <key> port
<port>

         exit

# IPSG Accounting Proxy Configuration:

      ipsg-service <service_name> mode radius-server

         bind accounting-proxy address <ip_address> port <port>

         radius dictionary <dictionary>

         radius accounting client <ip_address> [ encrypted ] key <secret> [
dictionary <dictionary> ] [ disconnect-message [ dest-port <port_num> ] ]

         exit

      aaa group default

         radius attribute nas-ip-address address <ip_address>
```

```
        radius dictionary <dictionary>

        radius accounting server <ip_address> [ encrypted ] key <key> port
<port>

        end
```

Notes:

- If both IPSG Service and client/server dictionaries are configured, the client/server dictionary takes precedence over the IPSG Service dictionary.
- If both RADIUS server and client dictionaries are configured, the client dictionary takes precedence over the server dictionary.
- For basic AAA configurations please refer to the *AAA Interface Administration and Reference*.

Option 3: RADIUS Snoop Mode Configuration

To create an IPSG context and IPSG service in RADIUS Snoop Mode, use the following configuration:

```
configure

   context <ipsg_context_name>

      ipsg-service <service_name> mode radius-snoop

         bind

         connection authorization [ encrypted ] password <password>

         radius accounting server <ip_address>

         radius dictionary <dictionary>

         end
```

Gx Interface Configuration

For information on how to configure the R7 Gx interface, please refer to the *Configuring Rel. 7 Gx Interface* section of the *GX Interface Support* chapter in the *System Enhanced Feature Configuration Guide*.

Note the following for IPSG:

- Only single bearer/session concept is supported. Multiple bearer concept is not applicable.
- Only PCRF binding is applicable. PCEF binding is not applicable.

Gy Interface Configuration

To configure the Gy interface, use the following example:

```
configure
   context <ipsg_context_name>
      diameter endpoint <endpoint_name>
         origin realm <realm>
         origin host <host> address <ip_address>
         peer <peer> realm <realm> address <ip_address>
         exit
      exit
   active-charging service <service_name>
      credit-control
         diameter origin endpoint <endpoint_name>
         diameter peer-select peer <peer> realm <realm>
         diameter pending-timeout <timeout>
         diameter session failover
         trigger type cellid
         diameter dictionary <dictionary>
         failure-handling initial-request continue go-offline-after-tx-expiry
         failure-handling update-request continue
         failure-handling terminate-request continue
         exit
      exit
   context <ipsg_context_name>
      apn <apn_name>
         selection-mode sent-by-ms
         ims-auth-service <service>
         ip access-group <access_list> in
```

```
ip access-group <access_list> out
ip context-name <context_name>
active-charging rulebase <rulebase_name>
end
```

ISP Context Configuration

To configure the ISP context:

Step 1 Create an ISP context as described in the Creating the ISP Context section.

Step 2 Create an interface within the ISP context to connect to the data network as described in the *GGSN Administration Guide*.

Step 3 Create an IP access control list within the ISP context as described in the *IP Access Control Lists* chapter of the *System Enhanced Features Configuration Guide*.

Creating the ISP Context

To configure an ISP context, use the following configuration. Note that the following configuration also includes an IP route for data traffic through the IPSG context.

```
configure
   context <isp_context_name>
      subscriber default
         exit
      ip access-list <access_list>
         redirect css service <service> any
         permit any
         exit
      aaa group default
         exit
      ip route <ip_address/mask> <next_hop_address> <isp_data_intfc_name>
         end
```

Saving the Configuration

Refer to the *Verifying and Saving Your Configuration* chapter to save the IPSG configuration.

Chapter 3
Verifying and Saving Your Configuration

This chapter describes how to save the system configuration.

Verifying the Configuration

You can use a number of command to verify the configuration of your feature, service, or system. Many are hierarchical in their implementation and some are specific to portions of or specific lines in the configuration file.

Feature Configuration

In many configurations, specific features are set and need to be verified. Examples include APN and IP address pool configuration. Using these examples, enter the following commands to verify proper feature configuration:

show apn all

The output displays the complete configuration for the APN. In this example, an APN called apn1 is configured.

```
access point name (APN): apn1

authentication context: test

pdp type: ipv4

Selection Mode: subscribed

ip source violation: Checked drop limit: 10

accounting mode: gtpp No early PDUs: Disabled

max-primary-pdp-contexts: 1000000 total-pdp-contexts: 1000000

primary contexts: not available total contexts: not available

local ip: 0.0.0.0

primary dns: 0.0.0.0 secondary dns: 0.0.0.0

ppp keep alive period : 0 ppp mtu : 1500

absolute timeout : 0 idle timeout : 0

long duration timeout: 0 long duration action: Detection

ip header compression: vj

data compression: stac mppc deflate compression mode: normal

min compression size: 128

ip output access-group: ip input access-group:

ppp authentication:

allow noauthentication: Enabled imsi

 authentication:Disabled
```

Enter the following command to display the IP address pool configuration:

show ip pool

The output from this command should look similar to the sample shown below. In this example, all IP pools were configured in the *isp1* context.

```
context : isp1:

+-----Type: (P) - Public (R) - Private

 | (S) - Static (E) - Resource

 |

 |+----State: (G) - Good (D) - Pending Delete (R)-Resizing

 ||

 ||++--Priority: 0..10 (Highest (0) .. Lowest (10))

 ||||

 ||||+-Busyout: (B) - Busyout configured

 |||| |||||| vvvvv Pool Name Start Address Mask/End Address Used Avail

 ----- --------- --------------- --------------- -------- --------

PG00 ipsec 12.12.12.0 255.255.255.0 0 254 PG00

pool1 10.10.0.0 255.255.0.0 0 65534 SG00

vpnpool 192.168.1.250 192.168.1.254 0 5 Total Pool Count: 5
```

IMPORTANT: Many features can be configured on the system. There are show commands specifically for these features. Refer to the *Command Line Interface Reference* for more information.

Service Configuration

Verify that your service was created and configured properly by entering the following command:

show *<service_type> <service_name>*

The output is a concise listing of the service parameter settings similar to the sample displayed below. In this example, a P-GW service called pgw is configured.

```
Service name : pgw1

Service-Id : 1

Context : test1
```

```
Status : STARTED

Restart Counter : 8

EGTP Service : egtp1

LMA Service : Not defined

Session-Delete-Delay Timer : Enabled

Session-Delete-Delay timeout : 10000(msecs)

PLMN ID List : MCC: 100, MNC: 99

Newcall Policy : None
```

Context Configuration

Verify that your context was created and configured properly by entering the following command:

show context name *<name>*

The output shows the active context. Its ID is similar to the sample displayed below. In this example, a context named *test1* is configured.

```
Context Name     ContextID     State

------------     ---------     -----

test1            2          Active
```

System Configuration

Verify that your entire configuration file was created and configured properly by entering the following command:

show configuration

This command displays the entire configuration including the context and service configurations defined above.

Finding Configuration Errors

Identify errors in your configuration file by entering the following command:

show configuration errors

This command displays errors it finds within the configuration. For example, if you have created a service named "service1", but entered it as "srv1" in another part of the configuration, the system displays this error.

You must refine this command to specify particular sections of the configuration. Add the **section** keyword and choose a section from the help menu:

show configuration errors section ggsn-service

or

show configuration errors section aaa-config

If the configuration contains no errors, an output similar to the following is displayed:

```
###############################################################################

Displaying Global
AAA-configuration errors
###############################################################################

Total 0 error(s) in this section !
```

Saving the Configuration

Save system configuration information to a file locally or to a remote node on the network. You can use this configuration file on any other systems that require the same configuration.

Files saved locally can be stored in the SPC's/SMC's CompactFlash or on an installed PCMCIA memory card on the SPC/SMC. Files that are saved to a remote network node can be transmitted using either FTP, or TFTP.

Saving the Configuration on the Chassis

These instructions assume that you are at the root prompt for the Exec mode:

```
[local]host_name#
```

To save your current configuration, enter the following command:

```
save configuration url [-redundant] [-noconfirm] [showsecrets] [verbose]
```

Keyword/Variable	Description
url	Specifies the path and name to which the configuration file is to be stored. *url* may refer to a local or a remote file. *url* must be entered using one of the following formats: • **{ /flash | /pcmcia1 | /pcmcia2 }** *[/dir] /file_name* • **file:/{ /flash | /pcmcia1 | /pcmcia2 }** *[/dir] /file_name* • **tftp://**{ *ipaddress*|*host_name*[*:port#*]} [*/directory*] */file_name* • **ftp://**[*username*[*:pwd*] *@*] { *ipaddress*|*host_name*} [*:port#*] [*/directory*] */file_name* • **sftp://**[*username*[:*pwd*] *@*] { *ipaddress*|*host_name*} [*:port#*] [*/directory*] */file_name* **/flash** corresponds to the CompactFlash on the SPC/SMC. **/pcmcia1** corresponds to PCMCIA slot 1. **/pcmcia2** corresponds to PCMCIA slot 2. *ipaddress* is the IP address of the network server. *host_name* is the network server's *hostname*. *port#* is the network server's logical port number. Defaults are: • tftp: 69 - data • ftp: 20 - data, 21 - control • sftp: 115 - data Note: *host_name* can only be used if the **networkconfig** parameter is configured for DHCP and the DHCP server returns a valid nameserv er.dx *username* is the username required to gain access to the server if necessary. *password* is the password for the specified username if required. */directory* specifies the directory where the file is located if one exists. */file_name* specifies the name of the configuration file to be saved. Note: Configuration files should be named with a .cfg extension.
-redundant	Optional: This keyword directs the system to save the CLI configuration file to the local device, defined by the url variable, and then automatically copy that same file to the like device on the Standby SPC/SMC, if available. Note: This keyword will only work for like local devices that are located on both the active and standby SPCs/SMCs. For example, if you save the file to the /pcmcia1 device on the active SPC/SMC, that same type of device (a PC-Card in Slot 1 of the standby SPC/SMC) must be available. Otherwise, a failure message is displayed. Note: If saving the file to an external network (non-local) device, the system disregards this keyword.

Keyword/Variable	Description
-noconfirm	Optional: Indicates that no confirmation is to be given prior to saving the configuration information to the specified filename (if one was specified) or to the currently active configuration file (if none was specified).
showsecrets	Optional: This keyword causes the CLI configuration file to be saved with all passwords in plain text, rather than their default encrypted format.
verbose	Optional: Specifies that every parameter that is being saved to the new configuration file should be displayed.

IMPORTANT: The **-redundant** keyword is only applicable when saving a configuration file to local devices .This command does not synchronize the local file system. If you have added, modified, or deleted other files or directories to or from a local device for the active SPC/SMC, then you must synchronize the local file system on both SPCs/SMCs.

To save a configuration file called system.cfg to a directory that was previously created called cfgfiles on the SPC's/SMC's CompactFlash, enter the following command:

```
save configuration /flash/cfgfiles/system.cfg
```

To save a configuration file called simple_ip.cfg to a directory called host_name_configs using an FTP server with an IP address of 192.168.34.156 on which you have an account with a username of administrator and a password of secure, use the following command:

```
save configuration
ftp://administrator:secure@192.168.34.156/host_name_configs/
simple_ip.cfg
```

To save a configuration file called init_config.cfg to the root directory of a TFTP server with a hostname of config_server, enter the following command:

save configuration *tftp://config_server/init_config.cfg*

Chapter 4
IPSG Engineering Rules

This appendix lists IPSG-specific engineering rules or guidelines that must be considered prior to configuring the system for your network deployment. General and network-specific rules are available in the appendix of the *System Administration and Configuration Guide* for the specific network type.

The following rules are covered in this appendix:

- IPSG Context and Service Rules
- IPSG RADIUS Messaging Rules

IPSG Context and Service Rules

- Only one IPSG service can be configured within a context.
- Single context configurations must have the ingress port identified using the **ingress-mode** command in the Ethernet Port Configuration Mode.
- In single context configurations, if data packets are received before a session is initiated, the packets could be routed to their destination without being processed. Use separate ingress and egress contexts to prevent this issue.

IPSG RADIUS Messaging Rules

- The sending of RADIUS accounting start messages to the RADIUS server is delayed by the IPSG until a session is successfully started.