IP Services Gateway Configuration

This chapter describes how to configure the IPSG.

This chapter covers the following topics:

Configuration Requirements for the IPSG

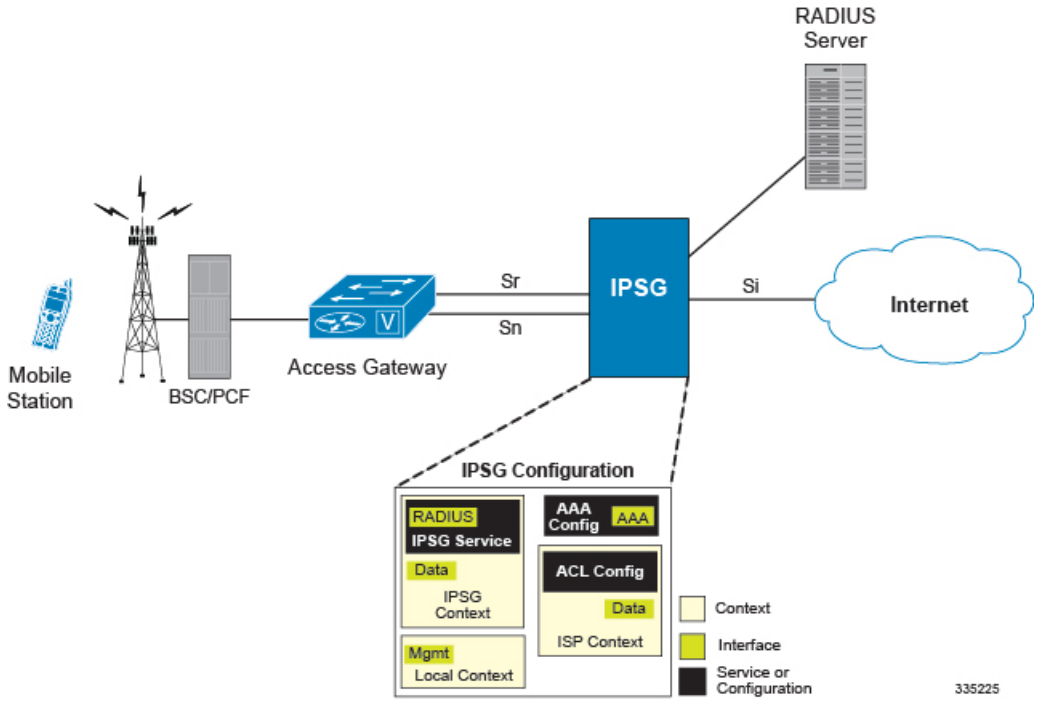
This section provides a high-level description of the configuration requirements of the IPSG.

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 Enhanced Charging Service (ECS) configuration.

Figure 1: 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 Enhanced 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
- Enhanced 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*.

IPSG RADIUS Dictionaries

The following table provides information on the different IPSG RADIUS dictionaries and the corresponding usage:

Table 1: IPSG RADIUS Dictionaries

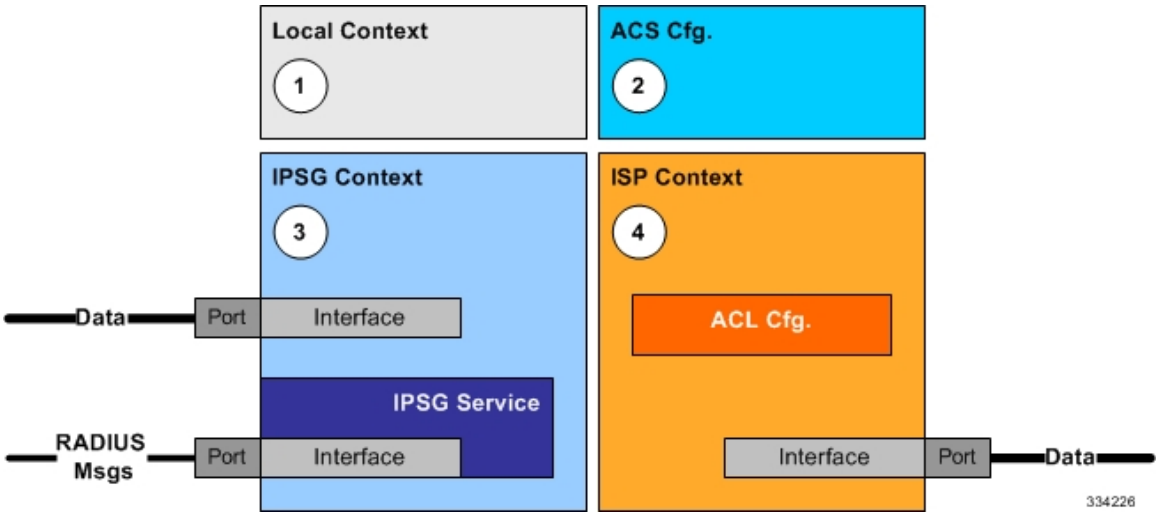
Dictionary	Mandatory Attributes	Session Identity
starent-vsa1	User-Name Acct-Status-Type Acct-Sess-Id Called-Station-Id Framed-IP-Address	User-Name Framed-IP-Address

Dictionary	Mandatory Attributes	Session Identity
custom28	Acct-Status-Type Acct-Sess-Id Called-Station-Id Framed-IP-Address Calling-Station-Id	Calling-station-Id Framed-IP-Address
custom54	Acct-Status-Type Acct-Sess-Id Called-Station-Id Framed-IP-Address Calling-Station-Id	Calling-station-id Framed-IP-Address

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 2: 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 Service Administration Guide*.

Step 3 Configure the system to perform as an IPSG by applying the example configurations presented in IPSG Context and Service Configuration, on page 5.

Step 4 Configure the Service Provider context by applying the example configuration presented in ISP Context Configuration, on page 7.

Step 5 Bind interfaces to ports as described in the *System Administration Guide*.

Step 6 Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

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, on page 5
- Option 2: RADIUS Server with Proxy Mode Configuration, on page 5
- Option 3: RADIUS Snoop Mode Configuration, on page 6

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 *System 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 ipsg_service_name mode radius-server
               bind address ipv4/ipv6_address
               radius dictionary dictionary_name
               radius accounting client ipv4/ipv6_address [ encrypted ] key
key [ dictionary dictionary_name ] [ disconnect-message [ dest-port port_number
 ] ]
               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 ipsg_service_name mode radius-server
               bind address ipv4/ipv6_address
               radius dictionary dictionary_name
               radius accounting client ipv4/ipv6_address [ encrypted ] key
key [ dictionary dictionary_name ] [ disconnect-message [ dest-port port_number
 ] ]
# IPSG Authentication Proxy Configuration:
               bind authentication-proxy address ipv4/ipv6_address
               connection authorization [ encrypted ] password password
               radius dictionary dictionary_name
               radius accounting client ipv4/ipv6_address [ encrypted ] key
key [ dictionary dictionary_name ] [ disconnect-message [ dest-port port_number
 ] ]
               exit
          aaa group default
               radius attribute nas-ip-address address ipv4/ipv6_address
               radius dictionary dictionary_name
               radius server ipv4/ipv6_address [ encrypted ] key key port
port_number
               radius accounting server ipv4/ipv6_address [ encrypted ] key
key port port_number
               exit
# IPSG Accounting Proxy Configuration:
          ipsg-service ipsg_service_name mode radius-server
              bind accounting-proxy address ipv4/ipv6_address port port_number

               radius dictionary dictionary_name
               radius accounting client ipv4/ipv6_address [ encrypted ] key
secret_key [ dictionary dictionary_name ] [ disconnect-message [ dest-port
port_number ] ]
               exit
          aaa group default
               radius attribute nas-ip-address address ipv4/ipv6_address
               radius dictionary dictionary_name
               radius accounting server ipv4/ipv6_address [ encrypted ] key
key port port_number
               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 and GTP 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 ipsg_service_name mode radius-snoop
               bind
               connection authorization [ encrypted ] password password
               radius accounting server ipv4/ipv6_address
               radius dictionary dictionary_name
               end
```

ISP Context Configuration

To configure the ISP context:

Step 1 Create an ISP context as described in Creating the ISP Context, on page 7.

Step 2 Create an interface within the ISP context to connect to the data network as described in the *System 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 Administration 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_name
               redirect css service css_service_name any
               permit any
               exit
          aaa group default
               exit
          ip route {ipv4_address/mask | ipv6_address } next-hop
next_hop_ipv4/ipv6_address isp_data_interface_name
               end
```

Enhanced and Optional Configurations

This section provides information on enhanced and optional configurations:

Virtual APN Support Configuration

To configure Virtual APN Support use the following configuration:

```
configure
     context ipsg_context_name
          apn apn_name
             virtual-apn preference priority apn apn_name [ access-gw-address
 { ipv4/ipv6_address | ipv4/ipv6_address/mask } | [ msisdn-range { from
msisdn_start_range to msisdn_end_range } ] [ rat-type { eutran | gan | geran |
hspa | utran | wlan } ] ]
               exit
```

RADIUS Server and/or RADIUS Snoop mode

```
          ipsg-service ipsg_service_name mode radius-server
          ipsg-service ipsg_service_name mode radius-snoop
               profile { APN | subscriber }
               end
```

Notes:

- The IPSG Virtual APN feature allows operators to use a single APN to configure differentiated services. The APN selection is based on the APN supplied to the IPSG in conjunction with the following configurable parameters:
  - access-gw-address (for IPSG this means the RADIUS client
  - msisdn-range
  - rat-type
- For more information, refer to the **virtual-apn** CLI command in the *APN Configuration Mode Commands* chapter of the *Command Line Interface Reference*.

Gx Interface Configuration

For information on how to configure R7 Gx interface support, please refer to the *Configuring Rel. 7 Gx Interface* section of the *Gx Interface Support* appendix.

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

For information on how to configure Gy interface support, refer to the *Gy Interface Support* appendix.

Overlapping IP Support over VPN Configuration

To enable Overlapping IP Support over VPN, use the following configuration:

```
config
          context context_name
```

```
ipsg-service ipsg_service_name mode radius-server
     [ default | no ] overlapping-ip-address
end
```

Notes:

- This feature is disabled by default.

Radius Client IP Validation

To enable IPSG to validate RADIUS client IP address, use the following configuration:

```
config
          context context_name
               ipsg-service ipsg_service_name mode radius-server
                    [ default ] radius accounting validate-client-ip
               end
```

Notes:

- This feature is enabled by default.
- Use the **disable radius accounting validate-client-ip** command to disable IPSG from validating the RADIUS client IPs.

Responding to Accounting-Stop Messages for Non-Existing Sessions

To enable the IPSG service to respond to a RADIUS Accounting-Stop message for a session that does not exist anymore (For example: IPSG service is reset and all active sessions are lost), use the following configuration:

```
config
          context context_name
               ipsg-service ipsg_service_name mode radius-server
                    [ default | no ] respond-to-non-existing-session
               end
```

Notes:

- This feature is disabled by default.