PDN Gateway Configuration

This chapter provides configuration information for the PDN Gateway (P-GW).

Important Information about all commands in this chapter can be found in the *Command Line Interface Reference*.

Because each wireless network is unique, the system is designed with a variety of parameters allowing it to perform in various wireless network environments. In this chapter, only the minimum set of parameters are provided to make the system operational. Optional configuration commands specific to the P-GW product are located in the *Command Line Interface Reference*.

The following procedures are located in this chapter:

Configuring the System as a Standalone eGTP P-GW

This section provides a high-level series of steps and the associated configuration file examples for configuring the system to perform as an eGTP P-GW in a test environment. For a complete configuration file example, refer to the *Sample Configuration Files* appendix. Information provided in this section includes the following:

Information Required

The following sections describe the minimum amount of information required to configure and make the P-GW operational on the network. To make the process more efficient, it is recommended that this information be available prior to configuring the system.

There are additional configuration parameters that are not described in this section. These parameters deal mostly with fine-tuning the operation of the P-GW in the network. Information on these parameters can be found in the appropriate sections of the *Command Line Interface Reference*.

Required Local Context Configuration Information

The following table lists the information that is required to configure the local context on an P-GW.

Table 1: Required Information for Local Context Configuration

Required Information	Description
Management Interface Configuration	
Interface name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured.
IP address and subnet	IPv4 addresses assigned to the interface. Multiple addresses and subnets are needed if multiple interfaces will be configured.
Physical port number	The physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides followed by the number of the physical connector on the card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Gateway IP address	Used when configuring static IP routes from the management interface(s) to a specific network.
Security administrator name	The name or names of the security administrator with full rights to the system.
Security administrator password	Open or encrypted passwords can be used.
Remote access type(s)	The type of remote access protocol that will be used to access the system, such as SSH.

Required P-GW Context Configuration Information

The following table lists the information that is required to configure the P-GW context on a P-GW.

Table 2: Required Information for P-GW Context Configuration

Required Information	Description
P-GW context name	An identification string from 1 to 79 characters (alpha and/or numeric) by which the P-GW context will be recognized by the system.
Accounting policy name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the accounting policy will be recognized by the system. The accounting policy is used to set parameters for the Rf (off-line charging) interface.
S5/S8 Interface Configuration (To/from S-GW)	

Required Information	Description
Interface name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured.
IP address and subnet	IPv4 or IPv6 addresses assigned to the interface. Multiple addresses and subnets are needed if multiple interfaces will be configured.
Physical port number	The physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides followed by the number of the physical connector on the card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Gateway IP address	Used when configuring static IP routes from the interface(s) to a specific network.
GTP-U Service Configuration	
GTP-U service name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the GTP-U service will be recognized by the system.
IP address	S5/S8 interface IPv4 address.
P-GW Service Configuration	
P-GW service name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the P-GW service will be recognized by the system. Multiple names are needed if multiple P-GW services will be used.
PLMN ID	MCC number: The mobile country code (MCC) portion of the PLMN's identifier (an integer value between 100 and 999). MNC number: The mobile network code (MNC) portion of the PLMN's identifier (a 2 or 3 digit integer value between 00 and 999).
eGTP Service Configuration	
eGTP Service Name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the eGTP service will be recognized by the system.

Required PDN Context Configuration Information

The following table lists the information that is required to configure the PDN context on a P-GW.

Table 3: Required Information for PDN Context Configuration

Required Information	Description
PDN context name	An identification string from 1 to 79 characters (alpha and/or numeric) by which the PDN context is recognized by the system.

Required Information	Description
IP Address Pool Configuration	
IPv4 address pool name and range	An identification string between 1 and 31 characters (alpha and/or numeric) by which the IPv4 pool is recognized by the system. Multiple names are needed if multiple pools will be configured. A range of IPv4 addresses defined by a starting address and an ending address.
IPv6 address pool name and range	An identification string between 1 and 31 characters (alpha and/or numeric) by which the IPv6 pool is recognized by the system. Multiple names are needed if multiple pools will be configured. A range of IPv6 addresses defined by a starting address and an ending address.
Access Control List Configuration	
IPv4 access list name	An identification string between 1 and 47 characters (alpha and/or numeric) by which the IPv4 access list is recognized by the system. Multiple names are needed if multiple lists will be configured.
IPv6 access list name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the IPv6 access list is recognized by the system. Multiple names are needed if multiple lists will be configured.
Deny/permit type	The types are: • any • by host IP address • by IP packets • by source ICMP packets • by source IP address masking • by TCP/UDP packets
Readdress or redirect type	The types are • readdress server • redirect context • redirect css delivery-sequence • redirect css service • redirect nexthop
SGi Interface Configuration (To/from IPv4 PDN)	

Required Information	Description
Interface name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface is recognized by the system. Multiple names are needed if multiple interfaces will be configured.
IP address and subnet	IPv4 addresses assigned to the interface. Multiple addresses and subnets are needed if multiple interfaces will be configured.
Physical port number	The physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides followed by the number of the physical connector on the card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Gateway IP address	Used when configuring static IP routes from the interface(s) to a specific network.
SGi Interface Configuration (To/from IPv6 PDN)	
Interface name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface is recognized by the system. Multiple names are needed if multiple interfaces will be configured.
IP address and subnet	IPv6 addresses assigned to the interface. Multiple addresses and subnets are needed if multiple interfaces will be configured.
Physical port number	The physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides followed by the number of the physical connector on the card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Gateway IP address	Used when configuring static IP routes from the interface(s) to a specific network.

Required AAA Context Configuration Information

The following table lists the information that is required to configure the AAA context on a P-GW.

Table 4: Required Information for AAA Context Configuration

Required Information	Description
Gx Interface Configuration (to PCRF)	
Interface name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface is recognized by the system. Multiple names are needed if multiple interfaces will be configured.

Required Information	Description
IP address and subnet	IPv4 or IPv6 addresses assigned to the interface. Multiple addresses and subnets are needed if multiple interfaces will be configured.
Physical port number	The physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides followed by the number of the physical connector on the card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Gateway IP address	Used when configuring static IP routes from the interface(s) to a specific network.
Gx Diameter Endpoint Configuration	
End point name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the Gx Diameter endpoint configuration is recognized by the system.
Origin realm name	An identification string between 1 through 127 characters. The realm is the Diameter identity. The originator's realm is present in all Diameter messages and is typically the company or service name.
Origin host name	An identification string from 1 to 255 characters (alpha and/or numeric) by which the Gx origin host is recognized by the system.
Origin host address	The IP address of the Gx interface.
Peer name	The Gx endpoint name described above.
Peer realm name	The Gx origin realm name described above.
Peer address and port number	The IP address and port number of the PCRF.
Route-entry peer	The Gx endpoint name described above.
Gy Interface Configuration (to on-line charging server)	
Interface name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface is recognized by the system. Multiple names are needed if multiple interfaces will be configured.
IP address and subnet	IPv4 or IPv6 addresses assigned to the interface. Multiple addresses and subnets are needed if multiple interfaces will be configured.
Physical port number	The physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides followed by the number of the physical connector on the card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.

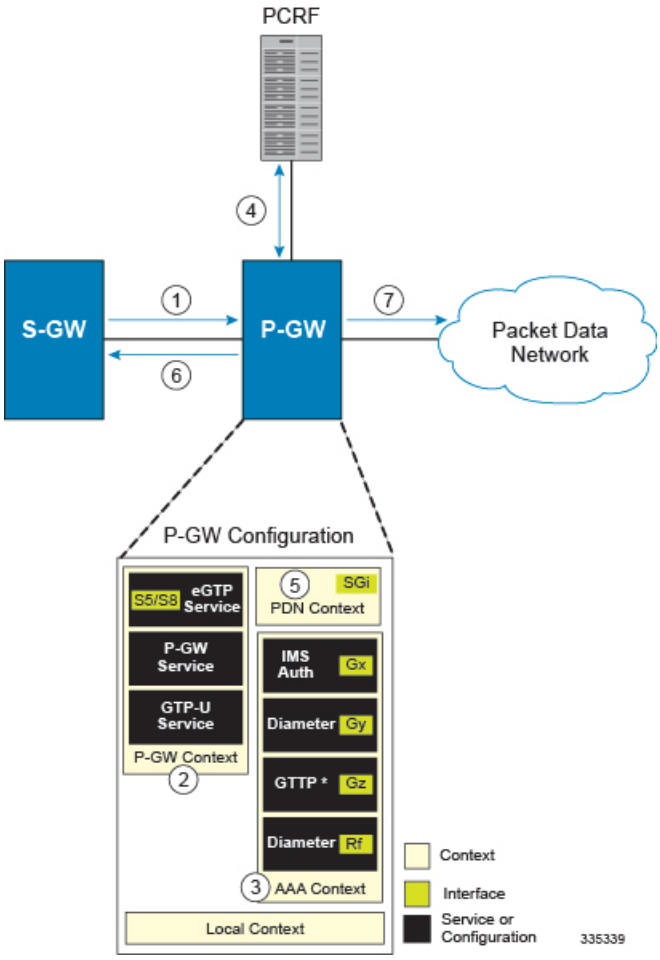
Required Information	Description
Gateway IP address	Used when configuring static IP routes from the interface(s) to a specific network.
Gy Diameter Endpoint Configuration	
End point name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the Gy Diameter endpoint configuration is recognized by the system.
Origin realm name	An identification string between 1 through 127 characters. The realm is the Diameter identity. The originator's realm is present in all Diameter messages and is typically the company or service name.
Origin host name	An identification string from 1 to 255 characters (alpha and/or numeric) by which the Gy origin host is recognized by the system.
Origin host address	The IP address of the Gy interface.
Peer name	The Gy endpoint name described above.
Peer realm name	The Gy origin realm name described above.
Peer address and port number	The IP address and port number of the OCS.
Route-entry peer	The Gy endpoint name described above.
Gz Interface Configuration (to off-line charging server)	
Interface name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface is recognized by the system. Multiple names are needed if multiple interfaces will be configured.
IP address and subnet	IPv4 addresses assigned to the interface. Multiple addresses and subnets are needed if multiple interfaces will be configured.
Physical port number	The physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides followed by the number of the physical connector on the card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Gateway IP address	Used when configuring static IP routes from the interface(s) to a specific network.
Rf Interface Configuration (to off-line charging server)	
Interface name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface is recognized by the system. Multiple names are needed if multiple interfaces will be configured.

Required Information	Description
IP address and subnet	IPv4 or IPv6 addresses assigned to the interface. Multiple addresses and subnets are needed if multiple interfaces will be configured.
Physical port number	The physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides followed by the number of the physical connector on the card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Gateway IP address	Used when configuring static IP routes from the interface(s) to a specific network.
Rf Diameter Endpoint Configuration	
End point name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the Rf Diameter endpoint configuration is recognized by the system.
Origin realm name	An identification string between 1 through 127 characters. The realm is the Diameter identity. The originator's realm is present in all Diameter messages and is typically the company or service name.
Origin host name	An identification string from 1 to 255 characters (alpha and/or numeric) by which the Rf origin host is recognized by the system.
Origin host address	The IP address of the Rf interface.
Peer name	The Rf endpoint name described above.
Peer realm name	The Rf origin realm name described above.
Peer address and port number	The IP address and port number of the OFCS.
Route-entry peer	The Rf endpoint name described above.

How This Configuration Works

The following figure and supporting text describe how this configuration with a single source and destination context is used by the system to process a subscriber call originating from the GTP LTE network.

Figure 1: GTP P-GW Configuration Elements

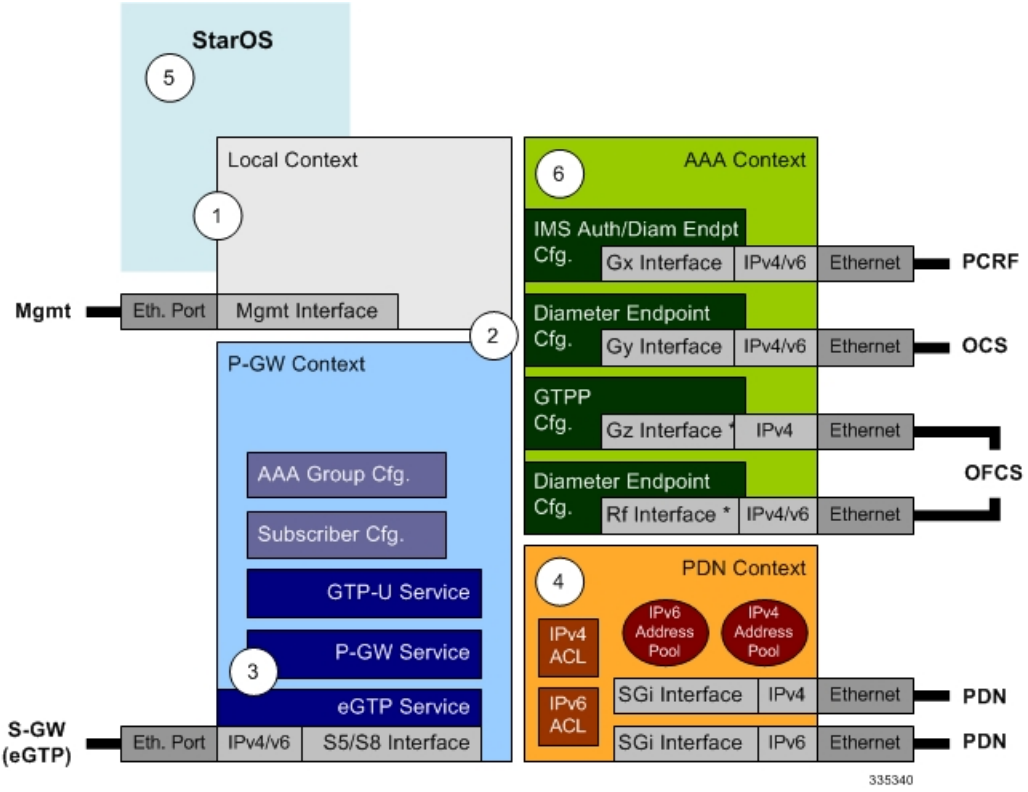


1. The S-GW establishes the S5/S8 connection by sending a Create Session Request message to the P-GW including an Access Point name (APN).
2. The P-GW service determines which context to use to provide AAA functionality for the session. This process is described in the *How the System Selects Contexts* section located in the *Understanding the System Operation and Configuration* chapter of the *System Administration Guide*.
3. The P-GW uses the configured Gx Diameter endpoint to establish the IP-CAN session.
4. The P-GW sends a CC-Request (CCR) message to the PCRF to indicate the establishment of the IP-CAN session and the PCRF acknowledges with a CC-Answer (CCA).
5. The P-GW uses the APN configuration to select the PDN context. IP addresses are assigned from the IP pool configured in the selected PDN context.
6. The P-GW responds to the S-GW with a Create Session Response message including the assigned address and additional information.
7. The S5/S8 data plane tunnel is established and the P-GW can forward and receive packets to/from the PDN.

eGTP P-GW Configuration

To configure the system to perform as a standalone eGTP P-GW:

Figure 2: eGTP P-GW Configurables



Procedure

Step 1 Set system configuration parameters such as activating PSCs by applying the example configurations found in the *System Administration Guide*.

Step 2 Set initial configuration parameters such as creating contexts and services by applying the example configurations found in the Initial Configuration, on page 11.

Step 3 Configure the system to perform as an eGTP P-GW and set basic P-GW parameters such as eGTP interfaces and IP routes by applying the example configurations presented in the P-GW Service Configuration, on page 15.

Step 4 Configure the PDN context by applying the example configuration in the P-GW PDN Context Configuration, on page 15.

Step 5 Enable and configure the active charging service for Gx interface support by applying the example configuration in the Active Charging Service Configuration, on page 16.

Step 6 Create a AAA context and configure parameters for policy by applying the example configuration in the Policy Configuration, on page 18.

Step 7 Verify and save the configuration by following the steps found in Verifying and Saving the Configuration, on page 20.

Initial Configuration

Procedure

Step 1 Set local system management parameters by applying the example configuration in Modifying the Local Context, on page 11.

Step 2 Create the context where the eGTP service will reside by applying the example configuration in Creating and Configuring an eGTP P-GW Context, on page 11.

Step 3 Create and configure APNs in the P-GW context by applying the example configuration in Creating and Configuring APNs in the P-GW Context, on page 12.

Step 4 Create and configure AAA server groups in the P-GW context by applying the example configuration in Creating and Configuring AAA Groups in the P-GW Context, on page 13.

Step 5 Create an eGTP service within the newly created context by applying the example configuration in Creating and Configuring an eGTP Service, on page 14.

Step 6 Create and configure a GTP-U service within the P-GW context by applying the example configuration in Creating and Configuring a GTP-U Service, on page 14.

Step 7 Create a context through which the interface to the PDN will reside by applying the example configuration in Creating a P-GW PDN Context, on page 14.

Modifying the Local Context

Use the following example to set the default subscriber and configure remote access capability in the local context:

```
configure
  context local
    interface <lcl_cntxt_intrfc_name>
      ip address <ip_address> <ip_mask>
        exit
      server ftpd
        exit
      server telnetd
        exit
      subscriber default
        exit
      administrator <name> encrypted password <password> ftp
      ip route <ip_addr/ip_mask> <next_hop_addr> <lcl_cntxt_intrfc_name>
      exit
  port ethernet <slot#/port#>
    no shutdown
    bind interface <lcl_cntxt_intrfc_name> local
    end
```

Creating and Configuring an eGTP P-GW Context

Use the following example to create a P-GW context, create an S5/S8 IPv4 interface (for data traffic to/from the S-GW), and bind the S5/S8 interface to a configured Ethernet port:

```
configure
  gtpp single-source
  context <pgw_context_name> -noconfirm
    interface <s5s8_interface_name>
      ip address <ipv4_address>
      exit
    gtpp group default
      gtpp charging-agent address <gz_ipv4_address>
      gtpp echo-interval <seconds>
      gtpp attribute diagnostics
      gtpp attribute local-record-sequence-number
      gtpp attribute node-id-suffix <string>
      gtpp dictionary <name>
      gtpp server <ipv4_address> priority <num>
      gtpp server <ipv4_address> priority <num> node-alive enable
      exit
    policy accounting <rf_policy_name> -noconfirm
      accounting-level {level_type}
      accounting-event-trigger interim-timeout action stop-start
      operator-string <string>
      cc profile <index> interval <seconds>
      exit
    exit
  subscriber default
    exit
  port ethernet <slot_number/port_number>
    no shutdown
    bind interface <s5s8_interface_name> <pgw_context_name>
    end
```

Notes:

- **gtpp single-source** is enabled to allow the system to generate requests to the accounting server using a single UDP port (by way of a AAA proxy function) rather than each AAA manager generating requests on unique UDP ports.
- The S5/S8 (P-GW to S-GW) interface IP address can also be specified as an IPv6 address using the **ipv6 address** command.
- Set the accounting policy for the Rf (off-line charging) interface. The accounting level types are: flow, PDN, PDN-QCI, QCI, and subscriber. Refer to the *Accounting Profile Configuration Mode Commands* chapter in the *Command Line Interface Reference* for more information on this command.
- Set the GTPP group setting for Gz accounting.

Creating and Configuring APNs in the P-GW Context

Use the following configuration to create an APN:

```
configure
  context <pgw_context_name> -noconfirm
    apn <name>
      accounting-mode radius-diameter
      associate accounting-policy <rf_policy_name>
```

```
ims-auth-service <gx_ims_service_name>
aaa group <rf-radius_group_name>
dns primary <ipv4_address>
dns secondary <ipv4_address>
ip access-group <name> in
ip access-group <name> out
mediation-device context-name <pgw_context_name>
ip context-name <pdn_context_name>
ipv6 access-group <name> in
ipv6 access-group <name> out
active-charging rulebase <name>
end
```

Notes:

- The IMS Authorization Service is created and configured in the AAA context.
- Multiple APNs can be configured to support different domain names.
- The **associate accounting-policy** command is used to associate a pre-configured accounting policy with this APN. Accounting policies are configured in the P-GW context. An example is located in the Creating and Configuring an eGTP P-GW Context, on page 11.

Use the following configuration to create an APN that includes Gz interface parameters:

```
configure
  context <pgw_context_name> -noconfirm
    apn <name>
      bearer-control-mode mixed
      selection-mode sent-by-ms
      accounting-mode gtpp
      gtpp group default accounting-context <aaa_context_name>
      ims-auth-service <gx_ims_service_name>
      ip access-group <name> in
      ip access-group <name> out
      ip context-name <pdn_context_name>
      active-charging rulebase <gz_rulebase_name>
      end
```

Notes:

- The IMS Authorization Service is created and configured in the AAA context.
- Multiple APNs can be configured to support different domain names.
- The accounting-mode GTPP and GTPP group commands configure this APN for Gz accounting.

Creating and Configuring AAA Groups in the P-GW Context

Use the following example to create and configure AAA groups supporting RADIUS and Rf accounting:

```
configure
  context <pgw_context_name> -noconfirm
    aaa group <rf-radius_group_name>
      radius attribute nas-identifier <id>
      radius accounting interim interval <seconds>
```

```
      radius dictionary <name>
      radius mediation-device accounting server <address> key <key>
      diameter authentication dictionary <name>
      diameter accounting dictionary <name>
      diameter accounting endpoint <rf_cfg_name>
      diameter accounting server <rf_cfg_name> priority <num>
      exit
   aaa group default
      radius attribute nas-ip-address address <ipv4_address>
      radius accounting interim interval <seconds>
      diameter authentication dictionary <name>
      diameter accounting dictionary <name>
      diameter accounting endpoint <rf_cfg_name>
      diameter accounting server <rf_cfg_name> priority <num>
      end
```

Creating and Configuring an eGTP Service

Use the following configuration example to create the eGTP service:

```
configure
   context <pgw_context_name>
      egtp-service <egtp_service_name> -noconfirm
         interface-type interface-pgw-ingress
         validation mode default
         associate gtpu-service <gtpu_service_name>
         gtpc bind address <s5s8_interface_address>
         end
```

Notes:

- Co-locating a P-GW service on the same ASR 5500 requires that the **gtpc bind address** command uses the same IP address the P-GW service is bound to.

Creating and Configuring a GTP-U Service

Use the following configuration example to create the GTP-U service:

```
configure
   context <pgw_context_name>
      gtpu-service <gtpu_service_name> -noconfirm
         bind ipv4-address <s5s8_interface_address>
         end
```

Notes:

- The **bind** command can also be specified as an IPv6 address using the **ipv6-address** command.

Creating a P-GW PDN Context

Use the following example to create a P-GW PDN context and Ethernet interface, and bind the interface to a configured Ethernet port.

```
configure
   context <pdn_context_name> -noconfirm
```

```
interface <sgi_ipv4_interface_name>
   ip address <ipv4_address>
interface <sgi_ipv6_interface_name>
   ipv6 address <address>
   end
```

P-GW Service Configuration

Procedure

Step 1 Configure the P-GW service by applying the example configuration in the Configuring the P-GW Service, on page 15.

Step 2 Specify an IP route to the eGTP Serving Gateway by applying the example configuration in the Configuring a Static IP Route, on page 15.

Configuring the P-GW Service

Use the following example to configure the P-GW service:

```
configure
   context <pgw_context_name>
      pgw-service <pgw_service_name> -noconfirm
           plmn id mcc <id> mnc <id>
           associate egtp-service <egtp_service_name>
           associate qci-qos-mapping <name>
           end
```

Notes:

- QCI-QoS mapping configurations are created in the AAA context. Refer to the Configuring QCI-QoS Mapping, on page 20 for more information.
- Co-locating a P-GW service on the same ASR 5500 requires the configuration of the **associate pgw-service** *name* command within the P-GW service.

Configuring a Static IP Route

Use the following example to configure an IP Route for control and user plane data communication with an eGTP Serving Gateway:

```
configure
   context <pgw_context_name>
      ip route <sgw_ip_addr/mask> <sgw_next_hop_addr> <pgw_intrfc_name>
      end
```

P-GW PDN Context Configuration

Use the following example to configure an IP Pool and APN, and bind a port to the interface in the PDN context:

```
configure
   context <pdn_context_name> -noconfirm
```

```
    interface <sgi_ipv4_interface_name>
      ip address <ipv4_address>
      exit
    interface <sgi_ipv6_interface_name>
      ip address <ipv6_address>
      exit
    ip pool <name> range <start_address end_address> public <priority>
    ipv6 pool <name> range <start_address end_address> public <priority>
    subscriber default
      exit
    ip access-list <name>
      redirect css service <name> any
      permit any
      exit
    ipv6 access-list <name>
      redirect css service <name> any
      permit any
      exit
      aaa group default
      exit
    exit
  port ethernet <slot_number/port_number>
    no shutdown
    bind interface <sgi_ipv4_interface_name> <pdn_context_name>
    exit
  port ethernet <slot_number/port_number>
    no shutdown
    bind interface <sgi_ipv6_interface_name> <pdn_context_name>
    end
```

Active Charging Service Configuration

Use the following example to enable and configure active charging:

```
configure
  require active-charging optimized-mode
  active-charging service <name>
    ruledef <name>
      <rule>
        .
        .
      <rule>
      exit
    ruledef default
      ip any-match = TRUE
      exit
    ruledef icmp-pkts
      icmp any-match = TRUE
      exit
    ruledef qci3
       icmp any-match = TRUE
      exit
```

```
ruledef static
  icmp any-match = TRUE
  exit
charging-action <name>
  <action>
    .
    .
  <action>
  exit
charging-action icmp
  billing-action egcdr
  exit
charging-action qci3
  content-id <id>
  billing-action rf
  qos-class-identifier <id>
  allocation-retention-priority <priority>
  tft packet-filter qci3
  exit
charging-action static
  service-identifier <id>
  billing-action rf
  qos-class-identifier <id>
  allocation-retention-priority <priority>
  tft packet-filter qci3
  exit
packet-filter <packet_filter_name>
  ip remote-address = { <ipv4/ipv6_address> | <ipv4/ipv6_address/mask> }
  ip remote-port { = <port_number> | range <start_port_number> to
<end_port_number> }
  exit
rulebase default
          exit
rulebase <name>
  <rule_base>
    .
    .
  <rule_base>
  exit
rulebase <gx_rulebase_name>
  dynamic-rule order first-if-tied
  egcdr tariff minute <minute> hour <hour>(optional)
  billing-records egcdr
  action priority 5 dynamic-only ruledef qci3 charging-action qci3
  action priority 100 ruledef static charging-action static
  action priority 500 ruledef default charging-action icmp
  action priority 570 ruledef icmp-pkts charging-action icmp
  egcdr threshold interval <interval>
  egcdr threshold volume total <bytes>
  end
```

Notes:

- A rulebase is a collection of rule definitions and associated charging actions.
- As depicted above, multiple rule definitions, charging actions, and rule bases can be configured to support a variety of charging scenarios.
- Charging actions define the action to take when a rule definition is matched.
- Routing and/or charging rule definitions can be created/configured. The maximum number of routing rule definitions that can be created is 256. The maximum number of charging rule definitions is 2048.
- The billing-action egcdr command in the charging-action *qc13*, *icmp*, and *static* examples is required for Gz accounting.
- The Gz rulebase example supports the Gz interface for offline charging. The **billing-records egcdr** command is required for Gz accounting. All other commands are optional.

Important If uplink packet is coming on the dedicated bearer, only rules installed on the dedicated bearer are matched. Static rules are not matched and packets failing to match the same will be dropped.

Policy Configuration

Procedure

Step 1 Configure the policy and accounting interfaces by applying the example configuration in the Creating and Configuring the AAA Context, on page 18.

Step 2 Create and configure QCI to QoS mapping by applying the example configuration in the Configuring QCI-QoS Mapping, on page 20.

Creating and Configuring the AAA Context

Use the following example to create and configure a AAA context including diameter support and policy control, and bind Ethernet ports to interfaces supporting traffic between this context and a PCRF, an OCS, and an OFCS:

```
configure
   context <aaa_context_name> -noconfirm
      interface <gx_interface_name>
         ipv6 address <address>
         exit
      interface <gy_interface_name>
         ipv6 address <address>
         exit
      interface <gz_interface_name>
         ip address <ipv4_address>
         exit
      interface <rf_interface_name>
         ip address <ipv4_address>
         exit
```

```
    subscriber default
      exit
    ims-auth-service <gx_ims_service_name>
      p-cscf discovery table <#> algorithm round-robin
      p-cscf table <#> row-precedence <#> ipv6-address <pcrf_ipv6_adr>
      policy-control
        diameter origin endpoint <gx_cfg_name>
        diameter dictionary <name>
        diameter host-select table <#> algorithm round-robin
        diameter host-select row-precedence <#> table <#> host <gx_cfg_name>

        exit
      exit
    diameter endpoint <gx_cfg_name>
      origin realm <realm_name>
      origin host <name> address <aaa_ctx_ipv6_address>
      peer <gx_cfg_name> realm <name> address <pcrf_ipv4_or_ipv6_addr>
      route-entry peer <gx_cfg_name>
      exit
    diameter endpoint <gy_cfg_name>
      origin realm <realm_name>
      origin host <name> address <gy_ipv6_address>
      connection retry-timeout <seconds>
      peer <gy_cfg_name> realm <name> address <ocs_ipv4_or_ipv6_addr>
      route-entry peer <gy_cfg_name>
      exit
    diameter endpoint <rf_cfg_name>
      use-proxy
      origin realm <realm_name>
      origin host <name> address <rf_ipv4_address>
      peer <rf_cfg_name> realm <name> address <ofcs_ipv4_or_ipv6_addr>
      route-entry peer <rf_cfg_name>
      exit
    exit
  port ethernet <slot_number/port_number>
    no shutdown
    bind interface <gx_interface_name> <aaa_context_name>
    exit
  port ethernet <slot_number/port_number>
    no shutdown
    bind interface <gy_interface_name> <aaa_context_name>
    exit
  port ethernet <slot_number/port_number>
    no shutdown
    bind interface <gz_interface_name> <aaa_context_name>
    exit
  port ethernet <slot_number/port_number>
    no shutdown
    bind interface <rf_interface_name> <aaa_context_name>
    end
```

Notes:

- The **p-cscf table** command under **ims-auth-service** can also specify an IPv4 address to the PCRF.
- The Gx interface IP address can also be specified as an IPv4 address using the **ip address** command.
- The Gy interface IP address can also be specified as an IPv4 address using the **ip address** command.
- The Rf interface IP address can also be specified as an IPv6 address using the **ipv6 address** command.

Configuring QCI-QoS Mapping

Use the following example to create and map QCI values to enforceable QoS parameters:

```
configure
  qci-qos-mapping <name>
    qci 1 user-datagram dscp-marking <hex>
    qci 3 user-datagram dscp-marking <hex>
    qci 9 user-datagram dscp-marking <hex>
    end
```

Notes:

- The P-GW does not support non-standard QCI values unless a valid license key is installed.

  QCI values 1 through 9 are standard values defined in 3GPP TS 23.203; the P-GW supports these standard values.

  From 3GPP Release 8 onwards, operator-specific/non-standard QCIs can be supported and carriers can define QCI 128- 254.

- The above configuration only shows one keyword example. Refer to the *QCI - QOS Mapping Configuration Mode Commands* chapter in the *Command Line Interface Reference* for more information on the **qci** command and other supported keywords.

Verifying and Saving the Configuration

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*.

DHCP Service Configuration

The system can be configured to use the Dynamic Host Control Protocol (DHCP) to assign IP addresses for PDP contexts. IP address assignment using DHCP is done using the following method, as configured within an APN:

DHCP-proxy: The system acts as a proxy for client (MS) and initiates the DHCP Discovery Request on behalf of client (MS). Once it receives an allocated IP address from DHCP server in response to DHCP Discovery Request, it assigns the received IP address to the MS. This allocated address must be matched with the an address configured in an IP address pool on the system. This complete procedure is not visible to MS.

As the number of addresses in memory decreases, the system solicits additional addresses from the DHCP server. If the number of addresses stored in memory rises above the configured limit, they are released back to the DHCP server.

There are parameters that must first be configured that specify the DHCP servers to communicate with and how the IP address are handled. These parameters are configured as part of a DHCP service.

Important This section provides the minimum instruction set for configuring a DHCP service on system for DHCP-based IP allocation. For more information on commands that configure additional DHCP server parameters and working of these commands, refer to the *DHCP Service Configuration Mode Commands* chapter of *Command Line Interface Reference*.

These instructions assume that you have already configured the system level configuration as described in *System Administration Guide* and P-GW service as described in *eGTP P-GW Configuration* section of this chapter.

To configure the DHCP service:

Procedure

Step 1 Create the DHCP service in system context and bind it by applying the example configuration in the DHCP Service Creation, on page 21.

Step 2 Configure the DHCP servers and minimum and maximum allowable lease times that are accepted in responses from DHCP servers by applying the example configuration in the DHCP Server Parameter Configuration, on page 21.

Step 3 Verify your DHCP Service configuration by following the steps in the DHCPv6 Service Configuration Verification, on page 27.

Step 4 Save your configuration as described in the *Verifying and Saving Your Configuration* section.

DHCP Service Creation

Use the following example to create the DHCP service to support DHCP-based address assignment:

```
configure
   context <dest_ctxt_name>
      dhcp-service <dhcp_svc_name>
        bind address <ip_address> [nexthop-forwarding-address <nexthop_ip_address>
 [mpls-label input <in_mpls_label_value> output <out_mpls_label_value1>
[out_mpls_label_value2]]]
         end
```

Notes:

- To ensure proper operation, DHCP functionality should be configured within a destination context.
- Optional keyword **nexthop-forwarding-address** <*nexthop_ip_address*> **[mpls-label input** <*in_mpls_label_value*> **output** <*out_mpls_label_value1*> **[** *out_mpls_label_value2* **]]** applies DHCP over MPLS traffic.

DHCP Server Parameter Configuration

Use the following example to configure the DHCP server parameters to support DHCP-based address assignment:

```
configure
   context <dest_ctxt_name>
```

```
dhcp-service <dhcp_svc_name>
   dhcp server <ip_address> [priority <priority>
   dhcp server selection-algorithm {first-server | round-robin}
   lease-duration min <minimum_dur> max <max_dur>
   dhcp deadtime <max_time>
   dhcp detect-dead-server consecutive-failures <max_number>
   max-retransmissions <max_number>
   retransmission-timeout <dur_sec>
   end
```

Notes:

- Multiple DHCP services can be configured. Each service can have multiple DHCP servers configured by entering **dhcp server** command multiple times. A maximum of 225 DHCP services can be configured with maximum of 8 DHCP servers configurations per DHCP service.
- The **dhcp detect-dead-server** command and **max-retransmissions** command work in conjunction with each other.
- The retransmission-timeout command works in conjunction with **max-retransmissions** command.

DHCP Service Configuration Verification

Procedure

Step 1 Verify that your DHCP servers configured properly by entering the following command in Exec Mode:

show dhcp service all

This command produces an output similar to that displayed below where DHCP name is *dhcp1*:

```
Service name:                       dhcp1
Context:                                isp
Bind:                                   Done
Local IP Address:                       150.150.150.150
Next Hop Address:                       192.179.91.3
              MPLS-label:
               Input:                   5000
         Output:                        1566    1899
Service Status:                         Started
Retransmission Timeout:                 3000 (milli-secs)
Max Retransmissions:                    2
Lease Time:                             600 (secs)
Minimum Lease Duration:                 600 (secs)
Maximum Lease Duration:                 86400 (secs)
DHCP Dead Time:                         120 (secs)
DHCP Dead consecutive Failure:          5
DHCP T1 Threshold Timer:                50
DHCP T2 Threshold Timer:                88
DHCP Client Identifier:                 Not Used
DHCP Algorithm:                         Round Robin
DHCP Servers configured:
 Address: 150.150.150.150               Priority: 1
DHCP server rapid-commit:               disabled
DHCP client rapid-commit:               disabled
DHCP chaddr validation:                 enabled
```

Step 2 Verify the DHCP service status by entering the following command in Exec Mode:

```
show dhcp service status
```

DHCPv6 Service Configuration

The system can be configured to use the Dynamic Host Control Protocol (DHCP) for IPv6 to enable the DHCP servers to pass the configuration parameters such as IPv6 network addresses to IPv6 nodes. DHCPv6 configuration is done within an APN.

These instructions assume that you have already configured the system level configuration as described in *System Administration Guide* and APN as described in P-GW PDN Context Configuration, on page 41.

To configure the DHCPv6 service:

Procedure

Step 1 Create the DHCPv6 service in system context and bind it by applying the example configuration in the DHCPv6 Service Creation, on page 23.

Step 2 Configure the DHCPv6 server and other configurable values for Renew Time, Rebind Time, Preferred Lifetime, and Valid Lifetime by applying the example configuration in the DHCPv6 Server Parameter Configuration, on page 24.

Step 3 Configure the DHCPv6 client and other configurable values for Maximum Retransmissions, Server Dead Tries, and Server Resurrect Time by applying the example configuration in the DHCPv6 Client Parameter Configuration, on page 24.

Step 4 Configure the DHCPv6 profile by applying the example configuration in the DHCPv6 Profile Configuration, on page 25.

Step 5 Associate the DHCPv6 profile configuration with the APN by applying the example configuration in the Associate DHCPv6 Configuration, on page 26.

Step 6 Verify your DHCPv6 Service configuration by following the steps in the DHCPv6 Service Configuration Verification, on page 27.

Step 7 Save your configuration as described in the *Verifying and Saving Your Configuration* chapter.

DHCPv6 Service Creation

Use the following example to create the DHCPv6 service to support DHCP-based address assignment:

```
configure
   context <dest_ctxt_name>
      dhcpv6-service <dhcpv6_svc_name>
         bind address <ipv6_address> port <port>
         end
```

Notes:

- To ensure proper operation, DHCPv6 functionality should be configured within a destination context.

- The Port specifies the listen port and is used to start the DHCPv6 server bound to it. It is optional and if unspecified, the default port is 547.

Note Use only link-local and unicast addresses for the DHCPv6 interface

DHCPv6 Server Parameter Configuration

Use the following example to configure the DHCPv6 server parameters to support DHCPv6-based address assignment:

```
configure
   context <dest_ctxt_name>
      dhcpv6-service <dhcpv6_svc_name>
         dhcpv6-server
         renew-time <renewal_time>
         rebind-time <rebind_time>
         preferred-lifetime <pref_lifetime>
         valid-lifetime <valid_lifetime>
         end
```

Notes:

- Multiple DHCP can be configured by entering **dhcp server** command multiple times. A maximum of 256 services (regardless of type) can be configured per system.
- **renew-time** configures the renewal time for prefixes assigned by dhcp-service. Default is 900 seconds.
- **rebind-time** configures the rebind time for prefixes assigned by dhcp-service. Default is 900 seconds.
- **preferred-lifetime** configures the preferred lifetime for prefixes assigned by dhcp-service. Default is 900 seconds.
- **valid-lifetime** configures the valid lifetime for prefixes assigned by dhcp-service. Default is 900 seconds.

DHCPv6 Client Parameter Configuration

Use the following example to configure the DHCPv6 client parameters to support DHCPv6-based address assignment:

```
configure
   context <dest_ctxt_name>
      dhcpv6-service <dhcpv6_svc_name>
         dhcpv6-client
            server-ipv6-address <ipv6_addr> port <port> priority <priority>
            max-retransmissions <max_number>
            server-dead-time <dead_time>
            server-resurrect-time <revive_time>
            end
```

Notes:

- DHCPv6 client configuration requires an IPv6 address, port, and priority. The port is used for communicating with the DHCPv6 server. If not specified, default port 547 is used. The Priority parameter defines the priority in which servers should be tried out.
- **max-retransmissions** configures the max retransmission that DHCPV6-CLIENT will make towards DHCPV6-SERVER. Default is 20.
- **server-dead-time**: PDN DHCPV6-SERVER is considered to be dead if it does not respond after given tries from client. Default is 5.
- **server-resurrect-time**: PDN DHCPV6-SERVER is considered alive after it has been dead for given seconds. Default is 20.

DHCPv6 Profile Configuration

Use the following example to configure the DHCPv6 profile:

```
configure
  context <dest_ctxt_name>
    dhcp-server-profile <server_profile>
      enable rapid-commit-dhcpv6
     process dhcp-option-from { AAA | LOCAL | PDN-DHCP } priority <priority>

      dhcpv6-server-preference <pref_value>
      enable dhcpv6-server-unicast
      enable dhcpv6-server-reconf
      exit
    dhcp-client-profile <client_profile>
      dhcpv6-client-unicast
      client-identifier { IMSI | MSISDN }
      enable rapid-commit-dhcpv6
      enable dhcp-message-spray
      request dhcp-option dns-address
      request dhcp-option netbios-server-address
      request dhcp-option sip-server-address
      end
```

Notes:

- **dhcp-server-profile** command creates a server profile and then enters the DHCP Server Profile configuration mode.
- **enable rapid-commit-dhcpv6** command enables rapid commit on the DHCPv6 server. By default it is disabled. This is done to ensure that if there are multiple DHCPv6 servers in a network, with rapid-commit-option, they would all end up reserving resources for the UE.
- **process dhcp-option-from** command configures in what order the configuration options should be processed for a given client request. For a given client configuration, values can be obtained from either AAA, PDN-DHCP-SERVER, or LOCAL. By default, AAA is preferred over PDN-DHCP, which is preferred over LOCAL configuration.
- **dhcpv6-server-preference**: According to RFC-3315, DHCPv6-CLIENT should wait for a specified amount of time before considering responses to its queries from DHCPv6-SERVERS. If a server responds with a preference value of 255, DHCPv6-CLIENT need not wait any longer. Default value is 0 and it may have any configured integer between 1 and 255.

- **enable dhcpv6-server-unicast** command enables server-unicast option for DHCPv6. By default, it is disabled.
- **enable dhcpv6-server-reconf** command configures support for reconfiguration messages from the server. By default, it is disabled.
- **dhcpv6-client-unicast** command Enables client to send messages on unicast address towards the server.
- **dhcp-client-profile** command creates a client profile and then enters the DHCP Client Profile configuration mode.
- **client identifier** command configures the client-identifier, which is sent to the external DHCP server. By default, IMSI is sent. Another available option is MSISDN.
- **enable rapid-commit-dhcpv6** command configures the rapid commit for the client. By default, rapid-commit option is enabled for both DHCPv4 & DHCPv6.
- **enable dhcp-message-spray** command enables dhcp-client to spray a DHCP message to all configured DHCP servers in the PDN. By default this is disabled. With Rapid-Commit, there can only be one server to which this can be sent.
- **request dhcp-option** command configures DHCP options which can be requested by the dhcp-client. It supports the following options:
  - dns-address
  - netbios-server-address
  - sip-server-address

Associate DHCPv6 Configuration

Use the following example to associate the DHCPv6 profile with an APN:

```
configure
   context dest_ctxt_name
      apn apn_name
         dhcpv6 service-name dhcpv6_svc_name server-profile server_profile
client-profile client_profile
         dhcpv6 ip-address-pool-name dhcpv6_ip_pool allow-static-allocation
         dhcpv6 context-name <dest_ctxt>
         end
```

NOTES:

- **dhcpv6 service-name** *dhcpv6_svc_name* **server-profile** *server_profile* **client-profile** *client_profile*: Allows the system to enter the DHCPv6 Server Configuration Mode where parameters are configured for the DHCPv6 server.
- **dhcpv6 service-name** *dhcpv6_svc_name* **client-profile** *client_profile*: Allows the system to enter the DHCPv6 Client Configuration Mode where parameters are configured for the DHCPv6 client.
- **dhcpv6 ip-address-pool-name** *dhcpv6_ip_pool* **allow-static-allocation**: Associates the DHCPv6 profile with an APN.

Note Use the **allow-static-allocation** parameter only when configuring the IPv6 pool.

DHCPv6 Service Configuration Verification

Procedure

Step 1 Verify that your DHCPv6 servers configured properly by entering the following command in Exec Mode:

show dhcpv6-service all

This command produces an output similar to that displayed below where DHCPv6 service name is *dhcp6-service*:

```
Service name:                dhcpv6-service
Context:                             A
Bind Address:                        2092::192:90:92:40
Bind :                               Done
Service Status:                      Started
Server Dead Time:                    120 (secs)
Server Dead consecutive Failure:5
Server Select Algorithm:             First Server
Server Renew Time:                   400 (secs)
Server Rebind Time:                  500 (secs)
Server Preferred Life Time:          600 (secs)
Server Valid Life Time:              700 (secs)
Max Retransmissions:                 3 (secs)
Server Dead Tries:                   4 (secs)
Server Resurrect Time:               10 (secs)
ipv6_nd_flag:                        O_FLAG
DHCPv6 Servers configured:
          Address:                   2092::192:90:92:40 Priority: 1    enabled
```

Step 2 Verify the DHCPv6 service status by entering the following command in Exec Mode:

show dhcpv6 status service *dhcpv6_service_name*

Configuring the System as a Standalone PMIP P-GW in an LTE-SAE Network

This section provides a high-level series of steps and the associated configuration file examples for configuring the system to perform as a P-MIP P-GW in an LTE-SAE test environment. For a complete configuration file example, refer to the *Sample Configuration Files* appendix. Information provided in this section includes the following:

Information Required

The following sections describe the minimum amount of information required to configure and make the P-GW operational on the network. To make the process more efficient, it is recommended that this information be available prior to configuring the system.

There are additional configuration parameters that are not described in this section. These parameters deal mostly with fine-tuning the operation of the P-GW in the network. Information on these parameters can be found in the appropriate sections of the *Command Line Interface Reference*.

Required Local Context Configuration Information

The following table lists the information that is required to configure the local context on an P-GW.

Table 5: Required Information for Local Context Configuration

Required Information	Description
Management Interface Configuration	
Interface name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured.
IP address and subnet	IPv4 addresses assigned to the interface. Multiple addresses and subnets are needed if multiple interfaces will be configured.
Physical port number	The physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides followed by the number of the physical connector on the card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Gateway IP address	Used when configuring static IP routes from the management interface(s) to a specific network.
Security administrator name	The name or names of the security administrator with full rights to the system.
Security administrator password	Open or encrypted passwords can be used.
Remote access type(s)	The type of remote access protocol that will be used to access the system, such as SSH.

Required P-GW Context Configuration Information

The following table lists the information that is required to configure the P-GW context on a P-GW.

Table 6: Required Information for P-GW Context Configuration

Required Information	Description
P-GW context name	An identification string from 1 to 79 characters (alpha and/or numeric) by which the P-GW context will be recognized by the system.
Accounting policy name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the accounting policy will be recognized by the system. The accounting policy is used to set parameters for the Rf (off-line charging) interface.
S5/S8 Interface Configuration (To/from S-GW)	
Interface name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured.
IP address and subnet	IPv4 addresses assigned to the interface. Multiple addresses and subnets are needed if multiple interfaces will be configured.
Physical port number	The physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides followed by the number of the physical connector on the card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Gateway IP address	Used when configuring static IP routes from the interface(s) to a specific network.
P-GW Service Configuration	
P-GW service name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the P-GW service will be recognized by the system. Multiple names are needed if multiple P-GW services will be used.
LMA Service Configuration	
LMA Service Name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the LMA service will be recognized by the system.

Required PDN Context Configuration Information

The following table lists the information that is required to configure the PDN context on a P-GW.

Table 7: Required Information for PDN Context Configuration

Required Information	Description
P-GW context name	An identification string from 1 to 79 characters (alpha and/or numeric) by which the P-GW context is recognized by the system.
IP Address Pool Configuration	

Required Information	Description
IPv4 address pool name and range	An identification string between 1 and 31 characters (alpha and/or numeric) by which the IPv4 pool is recognized by the system. Multiple names are needed if multiple pools will be configured. A range of IPv4 addresses defined by a starting address and an ending address.
IPv6 address pool name and range	An identification string between 1 and 31 characters (alpha and/or numeric) by which the IPv6 pool is recognized by the system. Multiple names are needed if multiple pools will be configured. A range of IPv6 addresses defined by a starting address and an ending address.
Access Control List Configuration	
IPv4 access list name	An identification string between 1 and 47 characters (alpha and/or numeric) by which the IPv4 access list is recognized by the system. Multiple names are needed if multiple lists will be configured.
IPv6 access list name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the IPv6 access list is recognized by the system. Multiple names are needed if multiple lists will be configured.
Deny/permit type	The types are: • any • by host IP address • by IP packets • by source ICMP packets • by source IP address masking • by TCP/UDP packets
Readdress or redirect type	The types are • readdress server • redirect context • redirect css delivery-sequence • redirect css service • redirect nexthop
SGi Interface Configuration (To/from IPv4 PDN)	
Interface name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface is recognized by the system. Multiple names are needed if multiple interfaces will be configured.

Required Information	Description
IP address and subnet	IPv4 addresses assigned to the interface. Multiple addresses and subnets are needed if multiple interfaces will be configured.
Physical port number	The physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides followed by the number of the physical connector on the card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Gateway IP address	Used when configuring static IP routes from the interface(s) to a specific network.
SGi Interface Configuration (To/from IPv6 PDN)	
Interface name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface is recognized by the system. Multiple names are needed if multiple interfaces will be configured.
IP address and subnet	IPv6 addresses assigned to the interface. Multiple addresses and subnets are needed if multiple interfaces will be configured.
Physical port number	The physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides followed by the number of the physical connector on the card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Gateway IP address	Used when configuring static IP routes from the interface(s) to a specific network.

Required AAA Context Configuration Information

The following table lists the information that is required to configure the AAA context on a P-GW.

Table 8: Required Information for AAA Context Configuration

Required Information	Description
Gx Interface Configuration (to PCRF)	
Interface name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface is recognized by the system. Multiple names are needed if multiple interfaces will be configured.
IP address and subnet	IPv4 or IPv6 addresses assigned to the interface. Multiple addresses and subnets are needed if multiple interfaces will be configured.

Required Information	Description
Physical port number	The physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides followed by the number of the physical connector on the card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Gateway IP address	Used when configuring static IP routes from the interface(s) to a specific network.
Gx Diameter Endpoint Configuration	
End point name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the Gx Diameter endpoint configuration is recognized by the system.
Origin realm name	An identification string between 1 through 127 characters. The realm is the Diameter identity. The originator's realm is present in all Diameter messages and is typically the company or service name.
Origin host name	An identification string from 1 to 255 characters (alpha and/or numeric) by which the Gx origin host is recognized by the system.
Origin host address	The IP address of the Gx interface.
Peer name	The Gx endpoint name described above.
Peer realm name	The Gx origin realm name described above.
Peer address and port number	The IP address and port number of the PCRF.
Route-entry peer	The Gx endpoint name described above.
S6b Interface Configuration (to 3GPP AAA server)	
Interface name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface is recognized by the system. Multiple names are needed if multiple interfaces will be configured.
IP address and subnet	IPv4 or IPv6 addresses assigned to the interface. Multiple addresses and subnets are needed if multiple interfaces will be configured.
Physical port number	The physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides followed by the number of the physical connector on the card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Gateway IP address	Used when configuring static IP routes from the interface(s) to a specific network.
S6b Diameter Endpoint Configuration	

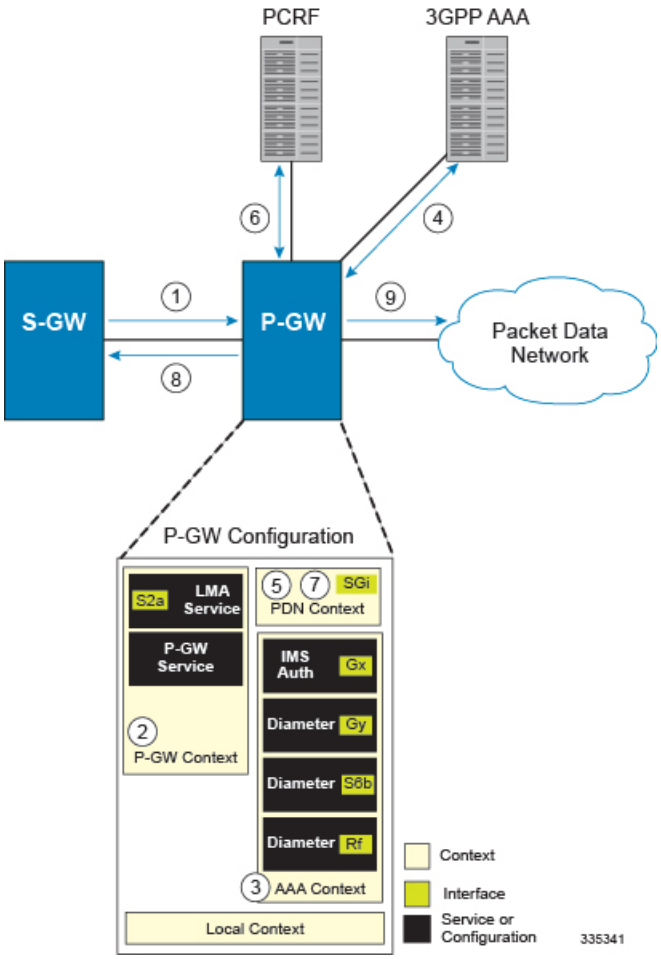
Required Information	Description
End point name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the S6b Diameter endpoint configuration is recognized by the system.
Origin realm name	An identification string between 1 through 127 characters. The realm is the Diameter identity. The originator's realm is present in all Diameter messages and is typically the company or service name.
Origin host name	An identification string from 1 to 255 characters (alpha and/or numeric) by which the S6b origin host is recognized by the system.
Origin host address	The IP address of the S6b interface.
Peer name	The S6b endpoint name described above.
Peer realm name	The S6b origin realm name described above.
Peer address and port number	The IP address and port number of the AAA server.
Route-entry peer	The S6b endpoint name described above.
Gy Interface Configuration (to on-line charging server)	
Interface name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface is recognized by the system. Multiple names are needed if multiple interfaces will be configured.
IP address and subnet	IPv4 or IPv6 addresses assigned to the interface. Multiple addresses and subnets are needed if multiple interfaces will be configured.
Physical port number	The physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides followed by the number of the physical connector on the card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Gateway IP address	Used when configuring static IP routes from the interface(s) to a specific network.
Gy Diameter Endpoint Configuration	
End point name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the Gy Diameter endpoint configuration is recognized by the system.
Origin realm name	An identification string between 1 through 127 characters. The realm is the Diameter identity. The originator's realm is present in all Diameter messages and is typically the company or service name.
Origin host name	An identification string from 1 to 255 characters (alpha and/or numeric) by which the Gy origin host is recognized by the system.
Origin host address	The IP address of the Gy interface.

Required Information	Description
Peer name	The Gy endpoint name described above.
Peer realm name	The Gy origin realm name described above.
Peer address and port number	The IP address and port number of the AAA server.
Route-entry peer	The Gy endpoint name described above.
Rf Interface Configuration (to off-line charging server)	
Interface name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface is recognized by the system. Multiple names are needed if multiple interfaces will be configured.
IP address and subnet	IPv4 or IPv6 addresses assigned to the interface. Multiple addresses and subnets are needed if multiple interfaces will be configured.
Physical port number	The physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides followed by the number of the physical connector on the card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Gateway IP address	Used when configuring static IP routes from the interface(s) to a specific network.
Rf Diameter Endpoint Configuration	
End point name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the Rf Diameter endpoint configuration is recognized by the system.
Origin realm name	An identification string between 1 through 127 characters. The realm is the Diameter identity. The originator's realm is present in all Diameter messages and is typically the company or service name.
Origin host name	An identification string from 1 to 255 characters (alpha and/or numeric) by which the Rf origin host is recognized by the system.
Origin host address	The IP address of the Rf interface.
Peer name	The Rf endpoint name described above.
Peer realm name	The Rf origin realm name described above.
Peer address and port number	The IP address and port number of the PCRF.
Route-entry peer	The Rf endpoint name described above.

How This Configuration Works

The following figure and supporting text describe how this configuration with a single source and destination context is used by the system to process a subscriber call originating from the PMIP LTE network.

Figure 3: Elements of the PMIP P-GW in the LTE Network



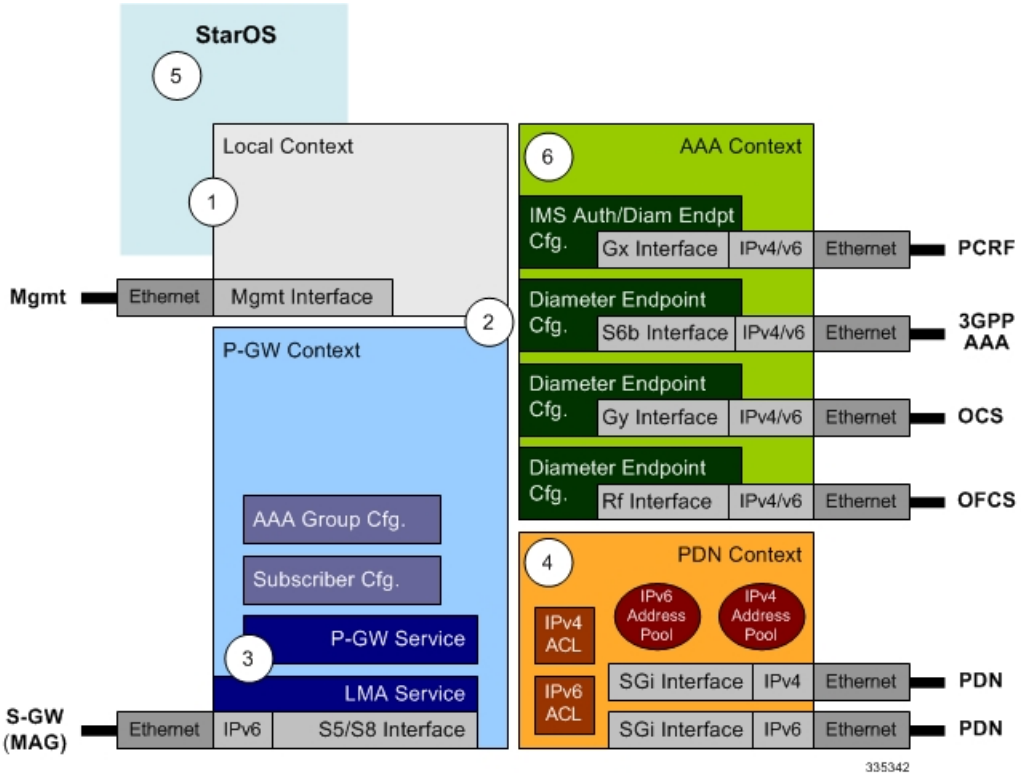
1. The S-GW establishes the S5/S8 connection by sending a Create Session Request message to the P-GW including an Access Point name (APN).
2. The P-GW service determines which context to use to provide AAA functionality for the session. This process is described in the *How the System Selects Contexts* section located in the *Understanding the System Operation and Configuration* chapter of the *System Administration Guide*.
3. The P-GW uses the configured Gx Diameter endpoint to establish the IP-CAN session.
4. The P-GW sends a CC-Request (CCR) message to the PCRF to indicate the establishment of the IP-CAN session and the PCRF acknowledges with a CC-Answer (CCA).
5. The P-GW uses the APN configuration to select the PDN context. IP addresses are assigned from the IP pool configured in the selected PDN context.

6. The P-GW responds to the S-GW with a Create Session Response message including the assigned address and additional information.
7. The S5/S8 data plane tunnel is established and the P-GW can forward and receive packets to/from the PDN.

P-MIP P-GW (LTE) Configuration

To configure the system to perform as a standalone P-MIP P-GW in an LTE-SAE network environment, review the following graphic and subsequent steps.

Figure 4: PMIP P-GW (LTE) Configurables



Procedure

Step 1 Set system configuration parameters such as activating PSCs by applying the example configurations found in the *System Administration Guide*.

Step 2 Set initial configuration parameters such as creating contexts and services by applying the example configurations found in the Initial Configuration, on page 37.

Step 3 Configure the system to perform as a PMIP P-GW and set basic P-GW parameters such as PMIP interfaces and an IP route by applying the example configurations presented in the P-GW Service Configuration, on page 40.

Step 4 Configure the PDN context by applying the example configuration in the P-GW PDN Context Configuration, on page 41.

Step 5 Enable and configure the active charging service for Gx interface support by applying the example configuration in the Active Charging Service Configuration, on page 41.

Step 6 Create a AAA context and configure parameters for AAA and policy by applying the example configuration in the AAA and Policy Configuration, on page 61.

Step 7 Verify and save the configuration by following the instructions in the Verifying and Saving the Configuration, on page 45.

Initial Configuration

Procedure

Step 1 Set local system management parameters by applying the example configuration in Modifying the Local Context, on page 37.

Step 2 Create the context where the P-GW service will reside by applying the example configuration in Creating and Configuring a P-MIP P-GW Context, on page 38.

Step 3 Create and configure APNs in the P-GW context by applying the example configuration in Creating and Configuring APNs in the P-GW Context, on page 38.

Step 4 Create and configure AAA server groups in the P-GW context by applying the example configuration in Creating and Configuring AAA Groups in the P-GW Context, on page 39.

Step 5 Create and configure a Local Mobility Anchor (LMA) service within the newly created context by applying example configuration in Creating and Configuring an LMA Service, on page 39.

Step 6 Create a context through which the interface to the PDN will reside by applying the example configuration in Creating a P-GW PDN Context, on page 40.

Modifying the Local Context

Use the following example to set the default subscriber and configure remote access capability in the local context:

```
configure
  context local
    interface <lcl_cntxt_intrfc_name>
      ip address <ip_address> <ip_mask>
        exit
      server ftpd
        exit
      server telnetd
        exit
      subscriber default
        exit
      administrator <name> encrypted password <password> ftp
      ip route <ip_addr/ip_mask> <next_hop_addr> <lcl_cntxt_intrfc_name>
      exit
  port ethernet <slot#/port#>
    no shutdown
```

```
bind interface <lcl_cntxt_intrfc_name> local
end
```

Creating and Configuring a P-MIP P-GW Context

Use the following example to create a P-GW context, create an S5/S8 IPv6 interface (for data traffic to/from the S-GW), and bind the S5/S8 interface to a configured Ethernet port:

```
configure
  context <pgw_context_name> -noconfirm
    interface <s5s8_interface_name> tunnel
      ipv6 address <ipv6_address>
      tunnel-mode ipv6ip
      source interface <name>
      destination address <ipv6 address>
      exit
    exit
  policy accounting <rf_policy_name> -noconfirm
    accounting-level {level_type}
    accounting-event-trigger interim-timeout action stop-start
    operator-string <string>
    exit
  subscriber default
    exit
    exit
  port ethernet <slot_number/port_number>
    no shutdown
    bind interface <s5s8_interface_name> <pgw_context_name>
    end
```

Notes:

- The S5/S8 (P-GW to S-GW) interface must be an IPv6 address.
- Set the accounting policy for the Rf (off-line charging) interface. The accounting level types are: flow, PDN, PDN-QCI, QCI, and subscriber. Refer to the *Accounting Profile Configuration Mode Commands* chapter in the *Command Line Interface Reference* for more information on this command.

Creating and Configuring APNs in the P-GW Context

Use the following configuration to create an APN:

```
configure
  context <pgw_context_name> -noconfirm
    apn <name>
      accounting-mode radius-diameter
      ims-auth-service <gx_ims_service_name>
      aaa group <rf-radius_group_name>
      dns primary <ipv4_address>
      dns secondary <ipv4_address>
      ip access-group <name> in
      ip access-group <name> out
      mediation-device context-name <pgw_context_name>
      ip context-name <pdn_context_name>
```

```
      ipv6 access-group <name> in
      ipv6 access-group <name> out
      active-charging rulebase <name>
      end
```

Notes:

- The IMS Authorization Service is created and configured in the AAA context.
- Multiple APNs can be configured to support different domain names.

Creating and Configuring AAA Groups in the P-GW Context

Use the following example to create and configure AAA groups supporting RADIUS and Rf accounting:

```
configure
  context <pgw_context_name> -noconfirm
    aaa group <rf-radius_group_name>
      radius attribute nas-identifier <id>
      radius accounting interim interval <seconds>
      radius dictionary <name>
      radius mediation-device accounting server <address> key <key>
      diameter authentication dictionary <name>
      diameter accounting dictionary <name>
      diameter authentication endpoint <s6b_cfg_name>
      diameter accounting endpoint <rf_cfg_name>
      diameter authentication server <s6b_cfg_name> priority <num>
      diameter accounting server <rf_cfg_name> priority <num>
      exit
    aaa group default
      radius attribute nas-ip-address address <ipv4_address>
      radius accounting interim interval <seconds>
      diameter authentication dictionary <name>
      diameter accounting dictionary <name>
      diameter authentication endpoint <s6b_cfg_name>
      diameter accounting endpoint <rf_cfg_name>
      diameter authentication server <s6b_cfg_name> priority <num>
      diameter accounting server <rf_cfg_name> priority <num>
      end
```

Creating and Configuring an LMA Service

Use the following configuration example to create the LMA service:

```
configure
  context <pgw_context_name>
    lma-service <lma_service_name> -noconfirm
      no aaa accounting
      revocation enable
      bind address <s5s8_ipv6_address>
      end
```

Notes:

- The **no aaa acounting** command is used to prevent duplicate accounting packets.

- Enabling revocation provides for MIP registration revocation in the event that MIP revocation is negotiated with a MAG and a MIP binding is terminated, the LMA can send a revocation message to the MAG.

Creating a P-GW PDN Context

Use the following example to create a P-GW PDN context and Ethernet interface, and bind the interface to a configured Ethernet port.

```
configure
   context <pdn_context_name> -noconfirm
      interface <sgi_ipv4_interface_name>
         ip address <ipv4_address>
      interface <sgi_ipv6_interface_name>
         ipv6 address <address>
         end
```

P-GW Service Configuration

Procedure

Step 1 Configure the P-GW service by applying the example configuration in the Configuring the P-GW Service, on page 40.

Step 2 Specify an IP route to the P-MIP Serving Gateway by applying the example configuration in the Configuring a Static IP Route, on page 41.

Configuring the P-GW Service

Use the following example to configure the P-GW service:

```
configure
   context <pgw_context_name>
      pgw-service <pgw_service_name> -noconfirm
         plmn id mcc <id> mnc <id>
         associate lma-service <lma_service_name>
         associate qci-qos-mapping <name>
         authorize external
         fqdn host <domain_name> realm <realm_name>
         end
```

Notes:

- QCI-QoS mapping configurations are created in the AAA context. Refer to the *Configuring QCI-QoS Mapping* section for more information.
- External authorization is performed by the 3GPP AAA server through the S6b interface. Internal authorization (APN) is default.
- The **fqdn host** command configures a Fully Qualified Domain Name for the P-GW service used in messages between the P-GW and a 3GPP AAA server over the S6b interface.

Configuring a Static IP Route

Use the following example to configure static IP routes for data traffic between the P-GW and the S-GW:

```
configure
   context <pgw_context_name>
      ipv6 route <ipv6_addr/prefix> next-hop <sgw_addr> interface
<pgw_sgw_intrfc_name>
      end
```

Notes:

- Static IP routing is not required for configurations using dynamic routing protocols.

P-GW PDN Context Configuration

Use the following example to configure an IP Pool and APN, and bind a port to the interface in the PDN context:

```
configure
   context <pdn_context_name> -noconfirm
      interface <pdn_sgi_ipv4_interface_name>
         ip address <ipv4_address>
         exit
      interface <pdn_sgi_ipv6_interface_name>
         ip address <ipv6_address>
         exit
      ip pool <name> range <start_address end_address> public <priority>
      ipv6 pool <name> range <start_address end_address> public <priority>
      subscriber default
      ip access-list <name>
         redirect css service <name> any
         permit any
         exit
      ipv6 access-list <name>
         redirect css service <name> any
         permit any
         exit
      aaa group default
         exit
      exit
   port ethernet <slot_number/port_number>
      no shutdown
      bind interface <pdn_ipv4_interface_name> <pdn_context_name>
      exit
   port ethernet <slot_number/port_number>
      no shutdown
      bind interface <pdn_ipv6_interface_name> <pdn_context_name>
      end
```

Active Charging Service Configuration

Use the following example to enable and configure active charging:

```
configure
  require active-charging optimized-mode
  active-charging service <name>
    ruledef <name>
      <rule>
        .
        .
      <rule>
      exit
    ruledef default
      ip any-match = TRUE
      exit
    ruledef icmp-pkts
      icmp any-match = TRUE
      exit
    ruledef qci3
       icmp any-match = TRUE
      exit
    ruledef static
      icmp any-match = TRUE
      exit
    charging-action <name>
      <action>
        .
        .
      <action>
      exit
    charging-action icmp
      billing-action egcdr
      exit
    charging-action qci3
      content-id <id>
      billing-action rf
      qos-class-identifier <id>
      allocation-retention-priority <priority>
      tft packet-filter qci3
      exit
    charging-action static
      service-identifier <id>
      billing-action rf
      qos-class-identifier <id>
      allocation-retention-priority <priority>
      tft packet-filter qci3
      exit
    packet-filter <packet_filter_name>
      ip remote-address = { <ipv4/ipv6_address> | <ipv4/ipv6_address/mask> }
      ip remote-port { = < port_number> | range <start_port_number> to
<end_port_number> }
      exit
    rulebase default
              exit
```

```
rulebase <name>
   <rule_base>
      .
      .
   <rule_base>
   end
```

Notes:

- A rulebase is a collection of rule definitions and associated charging actions.
- As depicted above, multiple rule definitions, charging actions, and rule bases can be configured to support a variety of charging scenarios.
- Routing and/or charging rule definitions can be created/configured. The maximum number of routing rule definitions that can be created is 256. The maximum number of charging rule definitions is 2048.
- Charging actions define the action to take when a rule definition is matched.

Important If uplink packet is coming on the dedicated bearer, only rules installed on the dedicated bearer are matched. Static rules are not matched and packets failing to match the same will be dropped.

AAA and Policy Configuration

Procedure

Step 1 Configure AAA and policy interfaces by applying the example configuration in the Creating and Configuring the AAA Context, on page 43.

Step 2 Create and configure QCI to QoS mapping by applying the example configuration in the Configuring QCI-QoS Mapping, on page 45 section.

Creating and Configuring the AAA Context

Use the following example to create and configure a AAA context including diameter support and policy control, and bind the port to interface supporting traffic between this context and a PCRF:

```
configure
   context <aaa_context_name> -noconfirm
      interface <s6b_interface_name>
         ip address <ipv4_address>
         exit
      interface <gx_interface_name>
         ipv6 address <address>
         exit
      interface <gy_interface_name>
         ipv6 address <address>
         exit
      interface <rf_interface_name>
```

```
      ip address <ipv4_address>
      exit
    subscriber default
      exit
    ims-auth-service <gx_ims_service_name>
      p-cscf discovery table <#> algorithm round-robin
      p-cscf table <#> row-precedence <#> ipv6-address <pcrf_adr>
      policy-control
        diameter origin endpoint <gx_cfg_name>
        diameter dictionary <name>
        diameter host-select table <#> algorithm round-robin
        diameter host-select row-precedence <#> table <#> host <gx_cfg_name>

        exit
      exit
    diameter endpoint <s6b_cfg_name>
      origin realm <realm_name>
      origin host <name> address <aaa_ctx_ipv4_address>
      peer <s6b_cfg_name> realm <name> address <aaa_ipv4_addr>
      route-entry peer <s6b_cfg_name>
      exit
    diameter endpoint <gx_cfg_name>
      origin realm <realm_name>
      origin host <name> address <aaa_ctx_ipv6_address>
      peer <gx_cfg_name> realm <name> address <pcrf_addr>
      route-entry peer <gx_cfg_name>
      exit
    diameter endpoint <gy_cfg_name>
      use-proxy
      origin realm <realm_name>
      origin host <name> address <gy_ipv6_address>
      connection retry-timeout <seconds>
      peer <gy_cfg_name> realm <name> address <ocs_ipv6_addr>
      route-entry peer <gy_cfg_name>
      exit
    diameter endpoint <rf_cfg_name>
      origin realm <realm_name>
      origin host <name> address <rf_ipv4_address>
      peer <rf_cfg_name> realm <name> address <ofcs_ipv4_addr>
      route-entry peer <rf_cfg_name>
      exit
    exit
  port ethernet <slot_number/port_number>
    no shutdown
    bind interface <s6b_interface_name> <aaa_context_name>
    exit
  port ethernet <slot_number/port_number>
    no shutdown
    bind interface <gx_interface_name> <aaa_context_name>
    exit
  port ethernet <slot_number/port_number>
    no shutdown
```

```
    bind interface <gy_interface_name> <aaa_context_name>
    exit
  port ethernet <slot_number/port_number>
    no shutdown
    bind interface <rf_interface_name> <aaa_context_name>
    end
```

Notes:

- The **p-cscf table** command under **ims-auth-service** can also specify an IPv4 address to the PCRF.
- The S6b interface IP address can also be specified as an IPv6 address using the **ipv6 address** command.
- The Gx interface IP address can also be specified as an IPv4 address using the **ip address** command.
- The Gy interface IP address can also be specified as an IPv4 address using the **ip address** command.
- The Rf interface IP address can also be specified as an IPv6 address using the **ipv6 address** command.

Configuring QCI-QoS Mapping

Use the following example to create and map QCI values to enforceable QoS parameters:

```
configure
  qci-qos-mapping <name>
    qci 1 user-datagram dscp-marking <hex>
    qci 3 user-datagram dscp-marking <hex>
    qci 9 user-datagram dscp-marking <hex>
    end
```

Notes:

- The P-GW does not support non-standard QCI values unless a valid license key is installed.

  QCI values 1 through 9 are standard values defined in 3GPP TS 23.203; the P-GW supports these standard values.

  From 3GPP Release 8 onwards, operator-specific/non-standard QCIs can be supported and carriers can define QCI 128- 254.

- The above configuration only shows one keyword example. Refer to the *QCI - QOS Mapping Configuration Mode Commands* chapter in the *Command Line Interface Reference* for more information on the **qci** command and other supported keywords.

Verifying and Saving the Configuration

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*.

Configuring the System as a Standalone PMIP P-GW Supporting an eHRPD Network

This section provides a high-level series of steps and the associated configuration file examples for configuring the system to perform as a P-MIP P-GW supporting an eHRPD test environment. For a complete configuration file example, refer to the *Sample Configuration Files* appendix. Information provided in this section includes the following:

Information Required

The following sections describe the minimum amount of information required to configure and make the P-GW operational on the network. To make the process more efficient, it is recommended that this information be available prior to configuring the system.

There are additional configuration parameters that are not described in this section. These parameters deal mostly with fine-tuning the operation of the P-GW in the network. Information on these parameters can be found in the appropriate sections of the *Command Line Interface Reference*.

Required Local Context Configuration Information

The following table lists the information that is required to configure the local context on an P-GW.

Table 9: Required Information for Local Context Configuration

Required Information	Description
Management Interface Configuration	
Interface name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured.
IP address and subnet	IPv4 addresses assigned to the interface. Multiple addresses and subnets are needed if multiple interfaces will be configured.
Physical port number	The physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides followed by the number of the physical connector on the card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Gateway IP address	Used when configuring static IP routes from the management interface(s) to a specific network.

Required Information	Description
Security administrator name	The name or names of the security administrator with full rights to the system.
Security administrator password	Open or encrypted passwords can be used.
Remote access type(s)	The type of remote access protocol that will be used to access the system, such as SSH.

Required P-GW Context Configuration Information

The following table lists the information that is required to configure the P-GW context on a P-GW.

Table 10: Required Information for P-GW Context Configuration

Required Information	Description
P-GW context name	An identification string from 1 to 79 characters (alpha and/or numeric) by which the P-GW context will be recognized by the system.
Accounting policy name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the accounting policy will be recognized by the system. The accounting policy is used to set parameters for the Rf (off-line charging) interface.
S2a Interface Configuration (To/from HSGW)	
Interface name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured.
IP address and subnet	IPv6 addresses assigned to the interface. Multiple addresses and subnets are needed if multiple interfaces will be configured.
Physical port number	The physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides followed by the number of the physical connector on the card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Gateway IP address	Used when configuring static IP routes from the interface(s) to a specific network.
P-GW Service Configuration	
P-GW service name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the P-GW service will be recognized by the system. Multiple names are needed if multiple P-GW services will be used.
PLMN ID	MCC number: The mobile country code (MCC) portion of the PLMN's identifier (an integer value between 100 and 999). MNC number: The mobile network code (MNC) portion of the PLMN's identifier (a 2 or 3 digit integer value between 00 and 999).

Required Information	Description
LMA Service Configuration	
LMA Service Name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the LMA service will be recognized by the system.

Required PDN Context Configuration Information

The following table lists the information that is required to configure the PDN context on a P-GW.

Table 11: Required Information for PDN Context Configuration

Required Information	Description
P-GW context name	An identification string from 1 to 79 characters (alpha and/or numeric) by which the P-GW context is recognized by the system.
IP Address Pool Configuration	
IPv4 address pool name and range	An identification string between 1 and 31 characters (alpha and/or numeric) by which the IPv4 pool is recognized by the system. Multiple names are needed if multiple pools will be configured. A range of IPv4 addresses defined by a starting address and an ending address.
IPv6 address pool name and range	An identification string between 1 and 31 characters (alpha and/or numeric) by which the IPv6 pool is recognized by the system. Multiple names are needed if multiple pools will be configured. A range of IPv6 addresses defined by a starting address and an ending address.
Access Control List Configuration	
IPv4 access list name	An identification string between 1 and 47 characters (alpha and/or numeric) by which the IPv4 access list is recognized by the system. Multiple names are needed if multiple lists will be configured.
IPv6 access list name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the IPv6 access list is recognized by the system. Multiple names are needed if multiple lists will be configured.
Deny/permit type	The types are: • any • by host IP address • by IP packets • by source ICMP packets • by source IP address masking • by TCP/UDP packets

Required Information	Description
Readdress or redirect type	The types are • readdress server • redirect context • redirect css delivery-sequence • redirect css service • redirect nexthop
SGi Interface Configuration (To/from IPv4 PDN)	
Interface name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface is recognized by the system. Multiple names are needed if multiple interfaces will be configured.
IP address and subnet	IPv4 addresses assigned to the interface. Multiple addresses and subnets are needed if multiple interfaces will be configured.
Physical port number	The physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides followed by the number of the physical connector on the card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Gateway IP address	Used when configuring static IP routes from the interface(s) to a specific network.
SGi Interface Configuration (To/from IPv6 PDN)	
Interface name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface is recognized by the system. Multiple names are needed if multiple interfaces will be configured.
IP address and subnet	IPv6 addresses assigned to the interface. Multiple addresses and subnets are needed if multiple interfaces will be configured.
Physical port number	The physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides followed by the number of the physical connector on the card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Gateway IP address	Used when configuring static IP routes from the interface(s) to a specific network.

Required AAA Context Configuration Information

The following table lists the information that is required to configure the AAA context on a P-GW.

Table 12: Required Information for AAA Context Configuration

Required Information	Description
Gx Interface Configuration (to PCRF)	
Interface name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface is recognized by the system. Multiple names are needed if multiple interfaces will be configured.
IP address and subnet	IPv4 or IPv6 addresses assigned to the interface. Multiple addresses and subnets are needed if multiple interfaces will be configured.
Physical port number	The physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides followed by the number of the physical connector on the card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Gateway IP address	Used when configuring static IP routes from the interface(s) to a specific network.
Gx Diameter Endpoint Configuration	
End point name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the Gx Diameter endpoint configuration is recognized by the system.
Origin realm name	An identification string between 1 through 127 characters. The realm is the Diameter identity. The originator's realm is present in all Diameter messages and is typically the company or service name.
Origin host name	An identification string from 1 to 255 characters (alpha and/or numeric) by which the Gx origin host is recognized by the system.
Origin host address	The IP address of the Gx interface.
Peer name	The Gx endpoint name described above.
Peer realm name	The Gx origin realm name described above.
Peer address and port number	The IP address and port number of the PCRF.
Route-entry peer	The Gx endpoint name described above.
S6b Interface Configuration (to 3GPP AAA server)	
Interface name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface is recognized by the system. Multiple names are needed if multiple interfaces will be configured.

Required Information	Description
IP address and subnet	IPv4 or IPv6 addresses assigned to the interface. Multiple addresses and subnets are needed if multiple interfaces will be configured.
Physical port number	The physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides followed by the number of the physical connector on the card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Gateway IP address	Used when configuring static IP routes from the interface(s) to a specific network.
S6b Diameter Endpoint Configuration	
End point name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the S6b Diameter endpoint configuration is recognized by the system.
Origin realm name	An identification string between 1 through 127 characters. The realm is the Diameter identity. The originator's realm is present in all Diameter messages and is typically the company or service name.
Origin host name	An identification string from 1 to 255 characters (alpha and/or numeric) by which the S6b origin host is recognized by the system.
Origin host address	The IP address of the S6b interface.
Peer name	The S6b endpoint name described above.
Peer realm name	The S6b origin realm name described above.
Peer address and port number	The IP address and port number of the AAA server.
Route-entry peer	The S6b endpoint name described above.
Rf Interface Configuration (to off-line charging server)	
Interface name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface is recognized by the system. Multiple names are needed if multiple interfaces will be configured.
IP address and subnet	IPv4 or IPv6 addresses assigned to the interface. Multiple addresses and subnets are needed if multiple interfaces will be configured.
Physical port number	The physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides followed by the number of the physical connector on the card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.

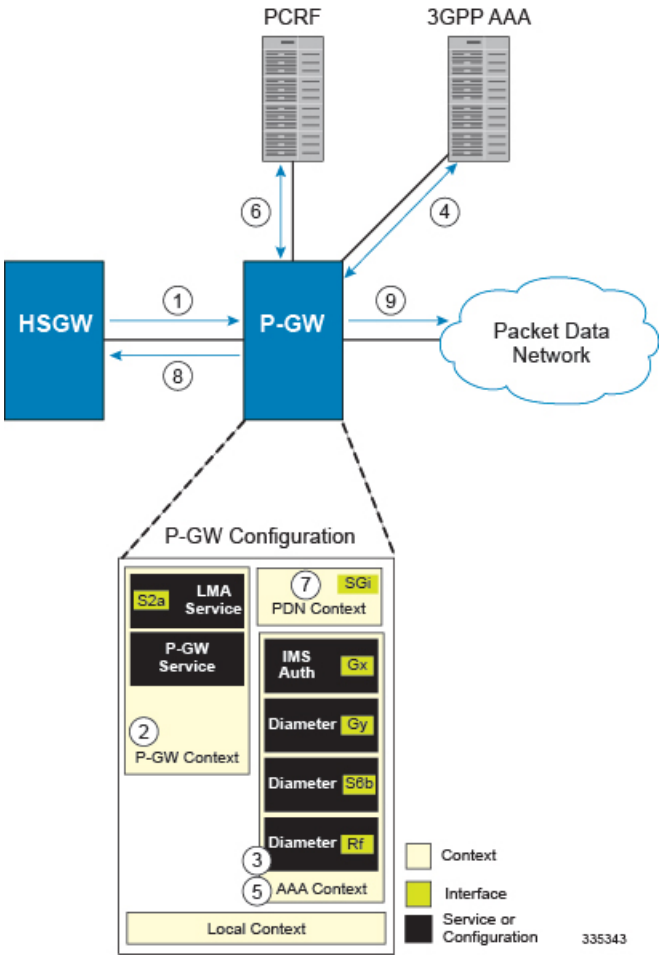
Required Information	Description
Gateway IP address	Used when configuring static IP routes from the management interface(s) to a specific network.
Rf Diameter Endpoint Configuration	
End point name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the Rf Diameter endpoint configuration is recognized by the system.
Origin realm name	An identification string between 1 through 127 characters. The realm is the Diameter identity. The originator's realm is present in all Diameter messages and is typically the company or service name.
Origin host name	An identification string from 1 to 255 characters (alpha and/or numeric) by which the Rf origin host is recognized by the system.
Origin host address	The IP address of the Rf interface.
Peer name	The Rf endpoint name described above.
Peer realm name	The Rf origin realm name described above.
Peer address and port number	The IP address and port number of the OFCS.
Route-entry peer	The Rf endpoint name described above.
Gy Interface Configuration (to on-line charging server)	
Interface name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface is recognized by the system. Multiple names are needed if multiple interfaces will be configured.
IP address and subnet	IPv4 or IPv6 addresses assigned to the interface. Multiple addresses and subnets are needed if multiple interfaces will be configured.
Physical port number	The physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides followed by the number of the physical connector on the card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Gateway IP address	Used when configuring static IP routes from the interface(s) to a specific network.
Gy Diameter Endpoint Configuration	
End point name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the Gy Diameter endpoint configuration is recognized by the system.
Origin realm name	An identification string between 1 through 127 characters. The realm is the Diameter identity. The originator's realm is present in all Diameter messages and is typically the company or service name.

Required Information	Description
Origin host name	An identification string from 1 to 255 characters (alpha and/or numeric) by which the Gy origin host is recognized by the system.
Origin host address	The IP address of the Gy interface.
Peer name	The Gy endpoint name described above.
Peer realm name	The Gy origin realm name described above.
Peer address and port number	The IP address and port number of the OCS.
Route-entry peer	The Gy endpoint name described above.

How This Configuration Works

The following figure and supporting text describe how this configuration with a single source and destination context is used by the system to process a subscriber call originating from the GTP LTE network.

Figure 5: Elements of the PMIP P-GW Supporting an eHRPD Network

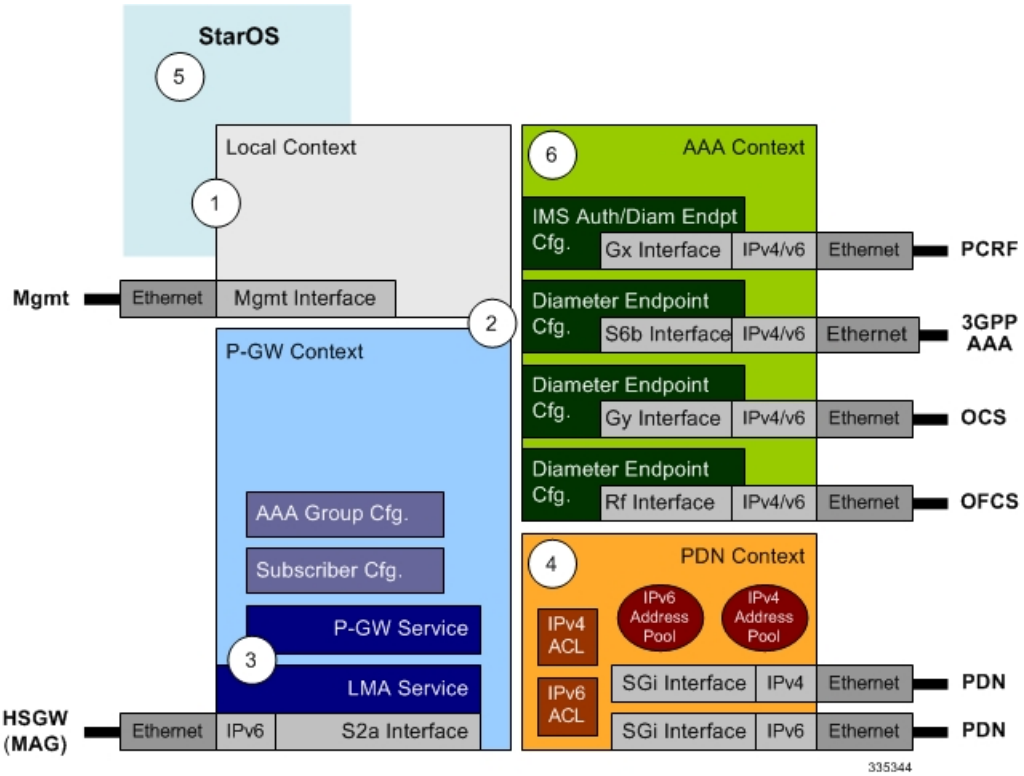


1. The S-GW establishes the S5/S8 connection by sending a Create Session Request message to the P-GW including an Access Point name (APN).
2. The P-GW service determines which context to use to provide AAA functionality for the session. This process is described in the *How the System Selects Contexts* section located in the *Understanding the System Operation and Configuration* chapter of the *System Administration Guide*.
3. The P-GW uses the configured Gx Diameter endpoint to establish the IP-CAN session.
4. The P-GW sends a CC-Request (CCR) message to the PCRF to indicate the establishment of the IP-CAN session and the PCRF acknowledges with a CC-Answer (CCA).
5. The P-GW uses the APN configuration to select the PDN context. IP addresses are assigned from the IP pool configured in the selected PDN context.
6. The P-GW responds to the S-GW with a Create Session Response message including the assigned address and additional information.
7. The S5/S8 data plane tunnel is established and the P-GW can forward and receive packets to/from the PDN.

P-MIP P-GW (eHRPD) Configuration

To configure the system to perform as a standalone P-MIP P-GW in an eHRPD network environment, review the following graphic and subsequent steps.

Figure 6: P-MIP P-GW (eHRPD) Configuration



Procedure

Step 1 Set system configuration parameters such as activating PSCs by applying the example configurations found in the *System Administration Guide*.

Step 2 Set initial configuration parameters such as creating contexts and services by applying the example configurations found in Initial Configuration.

Step 3 Configure the system to perform as a P-MIP P-GW and set basic P-GW parameters such as P-MIP interfaces and an IP route by applying the example configurations presented in P-GW Service Configuration, on page 58.

Step 4 Configure the PDN context by applying the example configuration in P-GW PDN Context Configuration, on page 59.

Step 5 Enable and configure the active charging service for Gx interface support by applying the example configuration in Active Charging Service Configuration, on page 60.

Step 6 Create a AAA context and configure parameters for AAA and policy by applying the example configuration in AAA and Policy Configuration.

Step 7 Verify and save the configuration by following the instruction in Verifying and Saving the Configuration, on page 63.

Initial Configuration

Procedure

Step 1 Set local system management parameters by applying the example configuration in Modifying the Local Context, on page 55.

Step 2 Create the context where the P-GW service will reside by applying the example configuration in Creating and Configuring a P-MIP P-GW Context, on page 56.

Step 3 Create and configure APNs in the P-GW context by applying the example configuration in Creating and Configuring APNs in the P-GW Context, on page 56.

Step 4 Create and configure AAA server groups in the P-GW context by applying the example configuration in Creating and Configuring AAA Groups in the P-GW Context, on page 57 section.

Step 5 Create an eGTP service within the newly created context by applying the example configuration in Creating and Configuring an LMA Service, on page 58.

Step 6 Create a context through which the interface to the PDN will reside by applying the example configuration in Creating a P-GW PDN Context, on page 58.

Modifying the Local Context

Use the following example to set the default subscriber and configure remote access capability in the local context:

```
configure
  context local
    interface <lcl_cntxt_intrfc_name>
      ip address <ip_address> <ip_mask>
      exit
```

```
    server ftpd
      exit
    server telnetd
      exit
    subscriber default
      exit
    administrator <name> encrypted password <password> ftp
    ip route <ip_addr/ip_mask> <next_hop_addr> <lcl_cntxt_intrfc_name>
    exit
  port ethernet <slot#/port#>
    no shutdown
    bind interface <lcl_cntxt_intrfc_name> local
    end
```

Creating and Configuring a P-MIP P-GW Context

Use the following example to create a P-GW context, create an S2a IPv6 interface (for data traffic to/from the HSGW), and bind the S2a interface to a configured Ethernet port:

```
configure
  context <pgw_context_name> -noconfirm
    interface <s2a_interface_name> tunnel
      ipv6 address <address>
      tunnel-mode ipv6ip
        source interface <name>
        destination address <ipv4 or ipv6 address>
        exit
      exit
    policy accounting <rf_policy_name> -noconfirm
      accounting-level {level_type}
      accounting-event-trigger interim-timeout action stop-start
      operator-string <string>
      cc profile <index> interval <seconds>
      exit
    subscriber default
      exit
    exit
  port ethernet <slot_number/port_number>
    no shutdown
    bind interface <s2a_interface_name> <pgw_context_name>
    end
```

Notes:

- The S2a (P-GW to HSGW) interface must be an IPv6 address.
- Set the accounting policy for the Rf (off-line charging) interface. The accounting level types are: flow, PDN, PDN-QCI, QCI, and subscriber. Refer to the *Accounting Profile Configuration Mode Commands* chapter in the *Command Line Interface Reference* for more information on this command.

Creating and Configuring APNs in the P-GW Context

Use the following configuration to create an APN:

```
configure
  context <pgw_context_name> -noconfirm
    apn <name>
      accounting-mode radius-diameter
      associate accounting-policy <rf_policy_name>
      ims-auth-service <gx_ims_service_name>
      aaa group <rf-radius_group_name>
      dns primary <ipv4_address>
      dns secondary <ipv4_address>
      ip access-group <name> in
      ip access-group <name> out
      mediation-device context-name <pgw_context_name>
      ip context-name <pdn_context_name>
      ipv6 access-group <name> in
      ipv6 access-group <name> out
      active-charging rulebase <name>
      end
```

Notes:

- The IMS Authorization Service is created and configured in the AAA context.
- Multiple APNs can be configured to support different domain names.
- The associate accounting-policy command is used to associate a pre-configured accounting policy with this APN. Accounting policies are configured in the P-GW context. An example is located in Creating and Configuring a P-MIP P-GW Context, on page 56.

Creating and Configuring AAA Groups in the P-GW Context

Use the following example to create and configure AAA groups supporting RADIUS and Rf accounting:

```
configure
  context <pgw_context_name> -noconfirm
    aaa group <rf-radius_group_name>
      radius attribute nas-identifier <id>
      radius accounting interim interval <seconds>
      radius dictionary <name>
      radius mediation-device accounting server <address> key <key>
      diameter authentication dictionary <name>
      diameter accounting dictionary <name>
      diameter authentication endpoint <s6b_cfg_name>
      diameter accounting endpoint <rf_cfg_name>
      diameter authentication server <s6b_cfg_name> priority <num>
      diameter accounting server <rf_cfg_name> priority <num>
      exit
    aaa group default
      radius attribute nas-ip-address address <ipv4_address>
      radius accounting interim interval <seconds>
      diameter authentication dictionary <name>
      diameter accounting dictionary <name>
      diameter authentication endpoint <s6b_cfg_name>
      diameter accounting endpoint <rf_cfg_name>
```

```
diameter authentication server <s6b_cfg_name> priority <num>
diameter accounting server <rf_cfg_name> priority <num>
```

Creating and Configuring an LMA Service

Use the following configuration example to create the LMA service:

```
configure
  context <pgw_context_name>
    lma-service <lma_service_name> -noconfirm
      no aaa accounting
      revocation enable
      bind address <s2a_ipv6_address>
      end
```

Notes:

- The **no aaa acounting** command is used to prevent duplicate accounting packets.
- Enabling revocation provides for MIP registration revocation in the event that MIP revocation is negotiated with a MAG and a MIP binding is terminated, the LMA can send a revocation message to the MAG.

Creating a P-GW PDN Context

Use the following example to create a P-GW PDN context and Ethernet interfaces.

```
configure
  context <pdn_context_name> -noconfirm
    interface <sgi_ipv4_interface_name>
      ip address <ipv4_address>
      exit
    interface <sgi_ipv6_interface_name>
      ipv6 address <address>
      end
```

P-GW Service Configuration

Procedure

Step 1 Configure the P-GW service by applying the example configuration in Configuring the P-GW Service, on page 58.

Step 2 Specify an IP route to the HRPD Serving Gateway by applying the example configuration in Configuring a Static IP Route, on page 59.

Configuring the P-GW Service

Use the following example to configure the P-GW service:

```
configure
  context <pgw_context_name>
    pgw-service <pgw_service_name> -noconfirm
      associate lma-service <lma_service_name>
```

```
associate qci-qos-mapping <name>
authorize external
fqdn host <domain_name> realm <realm_name>
plmn id mcc <id> mnc <id>
end
```

Notes:

- QCI-QoS mapping configurations are created in the AAA context. Refer to Configuring QCI-QoS Mapping, on page 63 for more information.
- External authorization is performed by the 3GPP AAA server through the S6b interface. Internal authorization (APN) is default.
- The **fqdn host** command configures a Fully Qualified Domain Name for the P-GW service used in messages between the P-GW and a 3GPP AAA server over the S6b interface.

Configuring a Static IP Route

Use the following example to configure static IP routes for data traffic between the P-GW and the HSGW:

```
configure
  context <pgw_context_name>
    ipv6 route <ipv6_addr/prefix> next-hop <hsgw_addr> interface
<pgw_hsgw_intrfc_name>
    end
```

Notes:

- Static IP routing is not required for configurations using dynamic routing protocols.

P-GW PDN Context Configuration

Use the following example to configure IP pools and IP Access Control Lists (ACLs), and bind ports to the interfaces in the PDN context:

```
configure
  context <pdn_context_name> -noconfirm
    ip pool <name> range <start_address end_address> public <priority>
    ipv6 pool <name> range <start_address end_address> public <priority>
    subscriber default
      exit
    ip access-list <name>
      redirect css service <name> any
      permit any
      exit
    ipv6 access-list <name>
      redirect css service <name> any
      permit any
      exit
    aaa group default
      exit
        exit
  port ethernet <slot_number/port_number>
    no shutdown
```

```
      bind interface <pdn_sgi_ipv4_interface_name> <pdn_context_name>
      exit
    port ethernet <slot_number/port_number>
      no shutdown
      bind interface <pdn_sgi_ipv6_interface_name> <pdn_context_name>
      end
```

Active Charging Service Configuration

Use the following example to enable and configure active charging:

```
configure
  require active-charging optimized-mode
  active-charging service <name>
    ruledef <name>
      <rule_definition>
        .
        .
      <rule_definition>
      exit
    ruledef <name>
      <rule_definition>
        .
        .
      <rule_definition>
      exit
    charging-action <name>
      <action>
        .
        .
      <action>
      exit
    charging-action <name>
      <action>
        .
        .
      <action>
      exit
    packet-filter <packet_filter_name>
      ip remote-address = { < ipv4/ipv6_address> | <ipv4/ipv6_address/mask> }
      ip remote-port { = < port_number> | range <start_port_number> to
<end_port_number> }
      exit
    rulebase default
    exit
    rulebase <name>
      <rule_base>
        .
        .
      <rule_base>
      end
```

Notes:

- A rulebase is a collection of rule definitions and associated charging actions.
- Active charging in optimized mode enables the service as part of the session manager instead of part of ACS managers.
- As depicted above, multiple rule definitions, charging actions, and rule bases can be configured to support a variety of charging scenarios.
- Routing and/or charging rule definitions can be created/configured. The maximum number of routing rule definitions that can be created is 256. The maximum number of charging rule definitions is 2048.
- Charging actions define the action to take when a rule definition is matched.

Important If uplink packet is coming on the dedicated bearer, only rules installed on the dedicated bearer are matched. Static rules are not matched and packets failing to match the same will be dropped.

AAA and Policy Configuration

Procedure

Step 1 Configure AAA and policy interfaces by applying the example configuration in the Creating and Configuring the AAA Context, on page 61 section.

Step 2 Create and configure QCI to QoS mapping by applying the example configuration in the Configuring QCI-QoS Mapping, on page 63 section.

Creating and Configuring the AAA Context

Use the following example to create and configure a AAA context including diameter support and policy control, and bind ports to interfaces supporting traffic between this context, a PCRF, a 3GPP AAA server, an on-line charging server, and an off-line charging server:

```
configure
  context <aaa_context_name> -noconfirm
    interface <s6b_interface_name>
      ip address <ipv4_address>
      exit
    interface <gx_interface_name>
      ipv6 address <address>
      exit
    interface <rf_interface_name>
      ip address <ipv4_address>
      exit
    interface <gy_interface_name>
      ipv6 address <address>
      exit
    subscriber default
```

```
    exit
  ims-auth-service <gx_ims_service_name>
    p-cscf discovery table <#> algorithm round-robin
    p-cscf table <#> row-precedence <#> ipv6-address <pcrf_adr>
    policy-control
      diameter origin endpoint <gx_cfg_name>
      diameter dictionary <name>
      diameter host-select table <#> algorithm round-robin
     diameter host-select row-precedence <#> table <#> host <gx_cfg_name>

      exit
    exit
  diameter endpoint <s6b_cfg_name>
    origin realm <realm_name>
    origin host <name> address <aaa_ctx_ipv4_address>
    peer <s6b_cfg_name> realm <name> address <aaa_ip_addr>
    route-entry peer <s6b_cfg_name>
    exit
  diameter endpoint <gx_cfg_name>
    origin realm <realm_name>
    origin host <name> address <aaa_context_ip_address>
    peer <gx_cfg_name> realm <name> address <pcrf_ipv6_addr>
    route-entry peer <gx_cfg_name>
    exit
  diameter endpoint <rf_cfg_name>
    origin realm <realm_name>
    origin host <name> address <aaa_ip_address>
    peer <rf_cfg_name> realm <name> address <ofcs_ip_addr>
    route-entry peer <rf_cfg_name>
    exit
  diameter endpoint <gy_cfg_name>
    use-proxy
    origin realm <realm_name>
    origin host <name> address <aaa_ip_address>
    connection retry-timeout <seconds>
    peer <gy_cfg_name> realm <name> address <ocs_ip_addr>
    route-entry peer <gy_cfg_name>
    exit
  exit
port ethernet <slot_number/port_number>
  no shutdown
  bind interface <s6b_interface_name> <aaa_context_name>
  exit
port ethernet <slot_number/port_number>
  no shutdown
  bind interface <gx_interface_name> <aaa_context_name>
  exit
port ethernet <slot_number/port_number>
  no shutdown
  bind interface <gy_interface_name> <aaa_context_name>
  exit
port ethernet <slot_number/port_number>
```

```
no shutdown
bind interface <rf_interface_name> <aaa_context_name>
end
```

Notes:

- The **p-cscf table** command under **ims-auth-service** can also specify an IPv4 address to the PCRF.
- The S6b interface IP address can also be specified as an IPv6 address using the **ipv6 address** command.
- The Gx interface IP address can also be specified as an IPv4 address using the **ip address** command.
- The Gy interface IP address can also be specified as an IPv4 address using the **ip address** command.
- The Rf interface IP address can also be specified as an IPv6 address using the **ipv6 address** command.

Configuring QCI-QoS Mapping

Use the following example to create and map QCI values to enforceable QoS parameters:

```
configure
  qci-qos-mapping <name>
    qci 1 user-datagram dscp-marking <hex>
    qci 3 user-datagram dscp-marking <hex>
    qci 9 user-datagram dscp-marking <hex>
    end
```

Notes:

- The P-GW does not support non-standard QCI values unless a valid license key is installed.

  QCI values 1 through 9 are standard values defined in 3GPP TS 23.203; the P-GW supports these standard values.

  From 3GPP Release 8 onwards, operator-specific/non-standard QCIs can be supported and carriers can define QCI 128- 254.

- The above configuration only shows one keyword example. Refer to the *QCI - QOS Mapping Configuration Mode Commands* chapter in the *Command Line Interface Reference* for more information on the **qci** command and other supported keywords.

Verifying and Saving the Configuration

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*.

Configuring Optional Features on the P-GW

The configuration examples in this section are optional and provided to cover the most common uses of the P-GW in a live network. The intent of these examples is to provide a base configuration for testing.

Configuring ACL-based Node-to-Node IP Security on the S5 Interface

The configuration example in this section creates an IKEv2/IPSec ACL-based node-to-node tunnel endpoint on the S5 interface.

Important Use of the IP Security feature requires that a valid license key be installed. Contact your local Sales or Support representative for information on how to obtain a license.

Creating and Configuring a Crypto Access Control List

The following example configures a crypto ACL (Access Control List), which defines the matching criteria used for routing subscriber data packets over an IPSec tunnel:

```
configure
  context <pgw_context_name> -noconfirm
    ip access-list <acl_name>
      permit tcp host <source_host_address> host <dest_host_address>
      end
```

Notes:

- The **permit** command in this example routes IPv4 traffic from the server with the specified source host IPv4 address to the server with the specified destination host IPv4 address.

Creating and Configuring an IPSec Transform Set

The following example configures an IPSec transform set, which is used to define the security association that determines the protocols used to protect the data on the interface:

```
configure
  context <pgw_context_name> -noconfirm
    ipsec transform-set <ipsec_transform-set_name>
      encryption aes-cbc-128
      group none
      hmac sha1-96
      mode tunnel
      end
```

Notes:

- The encryption algorithm, **aes-cbc-128**, or Advanced Encryption Standard Cipher Block Chaining, is the default algorithm for IPSec transform sets configured on the system.
- The **group none** command specifies that no crypto strength is included and that Perfect Forward Secrecy is disabled. This is the default setting for IPSec transform sets configured on the system.
- The **hmac** command configures the Encapsulating Security Payload (ESP) integrity algorithm. The **sha1-96** keyword uses a 160-bit secret key to produce a 160-bit authenticator value. This is the default setting for IPSec transform sets configured on the system.
- The **mode tunnel** command specifies that the entire packet is to be encapsulated by the IPSec header including the IP header. This is the default setting for IPSec transform sets configured on the system.

Creating and Configuring an IKEv2 Transform Set

The following example configures an IKEv2 transform set:

```
configure
  context <pgw_context_name> -noconfirm
    ikev2-ikesa transform-set <ikev2_transform-set_name>
      encryption aes-cbc-128
      group 2
      hmac sha1-96
      lifetime <sec>
      prf sha1
      end
```

Notes:

- The encryption algorithm, **aes-cbc-128**, or Advanced Encryption Standard Cipher Block Chaining, is the default algorithm for IKEv2 transform sets configured on the system.
- The **group 2** command specifies the Diffie-Hellman algorithm as Group 2, indicating medium security. The Diffie-Hellman algorithm controls the strength of the crypto exponentials. This is the default setting for IKEv2 transform sets configured on the system.
- The **hmac** command configures the Encapsulating Security Payload (ESP) integrity algorithm. The **sha1-96** keyword uses a 160-bit secret key to produce a 160-bit authenticator value. This is the default setting for IKEv2 transform sets configured on the system.
- The **lifetime** command configures the time the security key is allowed to exist, in seconds.
- The **prf** command configures the IKE Pseudo-random Function which produces a string of bits that cannot be distinguished from a random bit string without knowledge of the secret key. The **sha1** keyword uses a 160-bit secret key to produce a 160-bit authenticator value. This is the default setting for IKEv2 transform sets configured on the system.
- IKEv2 ACL mode with NATT is not supported.
- IKEv2 with VRF is not supported.

Creating and Configuring a Crypto Map

The following example configures an IKEv2 crypto map:

```
configure
  context <pgw_context_name>
    crypto map <crypto_map_name> ikev2-ipv4
      match address <acl_name>
      peer <ipv4_address>
      authentication local pre-shared-key key <text>
      authentication remote pre-shared-key key <text>
      ikev2-ikesa transform-set list  <name1> . . . name6>
      payload <name> match ipv4
        lifetime <seconds>
        ipsec transform-set list <name1> . . . <name4>
        exit
      exit
```

```
    interface <s5_intf_name>
      ip address <ipv4_address>
      crypto-map <crypto_map_name>
      exit
    exit
  port ethernet <slot_number/port_number>
    no shutdown
    bind interface <s5_intf_name> <pgw_context_name>
    end
```

Notes:

- The type of crypto map used in this example is IKEv2/IPv4 for IPv4 addressing. An IKEv2/IPv6 crypto map can also be used for IPv6 addressing.
- The **ipsec transform-set list** command specifies up to four IPSec transform sets.

Configuring APN as Emergency

The configuration example in this section configures an emergency APN for VoLTE based E911 support.

In APN Configuration Mode, specify the name of the emergency APN and set the emergency inactivity timeout as follows. You may also configure the P-CSCF FQDN server name for the APN.

```
configure
  context <pgw_context_name> -noconfirm
    apn <name>
      emergency-apn
      timeout emergency-inactivity <seconds>
      p-cscf fqdn <fqdn>
      end
```

Notes:

- By default, an APN is assumed to be non-emergency.
- The **timeout emergency-inactivity** command specifies the timeout duration, in seconds, to check inactivity on the emergency session. <*seconds*> must be an integer value from 1 through 3600.
- By default, emergency inactivity timeout is disabled (0).
- The **p-cscf fqdn** command configures the P-CSCF FQDN server name for the APN. <*fqdn*> must be a string from 1 to 256 characters in length.
- P-CSCF FQDN has more significance than CLI-configured P-CSCF IPv4 and IPv6 addresses.

Configuring Common Gateway Access Support

This section describes some advance feature configuration to support multiple access networks (CDMA, eHRPD ,and LTE) plus a GSM/UMTS for international roaming with the same IP addressing behavior and access to 3GPP AAA for subscriber authorization. Subscribers using static IP addressing will be able to get the same IP address regardless of the access technology.

This configuration combines 3G and 4G access technologies in a common gateway supporting logical services of HA, P-GW, and GGSN to allow subscribers to have the same user experience, independent of the access technology available.

Important This feature is a license-enabled support and you may need to install a feature specific session license on your system to use some commands related to this configuration.

These instructions assume that you have already configured the system level configuration as described in *System Administration Guide* and P-GW service.

To configure the S6b and other advance features:

1. Configure Diameter endpoint by applying the example configuration in Diameter Endpoint Configuration, on page 67.
2. Create or modify AAA group by applying the example configuration in AAA Group Configuration, on page 67.
3. Modify P-GW service to allow authorization with HSS by applying the example configuration in Authorization over S6b Configuration, on page 68.
4. *Optional*. Create and associate DNS client parameters by applying the example configuration in DNS Client Configuration, on page 68.
5. *Optional*. Modify P-GW service to accept duplicate calls when received with same IP address by applying the example configuration in Duplicate Call Accept Configuration, on page 68.
6. Verify your S6b configuration by following the steps in Common Gateway Access Support Configuration Verification, on page 69.
7. Save your configuration as described in the *Verifying and Saving Your Configuration* chapter.

Diameter Endpoint Configuration

Use the following example to configure the Diameter endpoint:

```
configure
  context <pgw_ctxt_name> -noconfirm
    diameter endpoint <s6b_endpoint_name>
      origin host <host_name> address <ip_address>
      peer <peer_name> realm <realm_name> address <ip_address> port <port_num>
    end
```

Notes:

- <*pgw_ctxt_name*> is name of the context which contains P-GW service on system.

AAA Group Configuration

Use the following example create/modify the AAA group for this feature.

```
configure
  context <fa_ctxt_name>
    aaa group <aaa_grp_name>
      diameter authentication dictionary aaa-custom15
        diameter authentication endpoint <s6b_endpoint_name>
        diameter authentication server <server_name> priority <priority>
        end
```

Notes:

- <*s6b_endpoint_name*> is name of the existing Diameter endpoint.

Authorization over S6b Configuration

Use the following example to enable the S6b interface on P-GW service with 3GPP AAA/HSS:

```
configure
   context <pgw_ctxt_name>
      pgw-service <pgw_svc_name>
         plmn id mcc <number> mnc <number>
         authorize-with-hss
         fqdn host <host_name> realm <realm_name>
         end
```

Notes:

- <*pgw_svc_name*> is name of the P-GW service which is already created on the system.

DNS Client Configuration

Use the following example to enable the S6b interface on P-GW service with 3GPP AAA/HSS:

```
configure
   context <pgw_ctxt_name>
      ip domain-lookup
      ip name-servers <ip_address/mask>
      dns-client <dns_name>
         bind address <ip_address>
         resolver retransmission-interval <duration>
         resolver number-of-retries <retrie>
         cache ttl positive <ttl_value>
         exit
      pgw-service <pgw_svc_name>
         default dns-client context
         end
```

Notes:

- <*pgw_svc_name*> is name of the P-GW service which is already created on the system.

Duplicate Call Accept Configuration

Use the following example to configure P-GW service to accept the duplicate session calls with request for same IP address:

```
configure
   context <pgw_ctxt_name>
      pgw-service <pgw_svc_name>
         newcall duplicate-subscriber-requested-address accept
         end
```

Notes:

- <*pgw_svc_name*> is name of the P-GW service which is already created on the system.

Common Gateway Access Support Configuration Verification

1. Verify that your common gateway access support is configured properly by entering the following command in Exec Mode:

   show pgw-service all

   The output from this command should look similar to the sample shown below. In this example P-GW service named *PGW1* was configured in the *vpn1* context.

```
Service name:                   pgw1
Context:                        cn1
Associated PGW svc:             None
Associated GTPU svc:            None
Accounting Context Name:        cn1
dns-client Context Name:        cn1
Authorize:                      hss
Fqdn-name:                      xyz.abc@starent.networks.com
Bind:                           Not Done
Local IP Address:               0.0.0.0          Local IP Port:
2123
Self PLMN:                      Not defined
Retransmission Timeout:         5 (secs)
```

Configuring Dynamic Node-to-Node IP Security on the S5 Interface

The configuration example in this section creates an IPSec/IKEv2 dynamic node-to-node tunnel endpoint on the S5 interface.

Important Use of the IP Security feature requires that a valid license key be installed. Contact your local Sales or Support representative for information on how to obtain a license.

Creating and Configuring an IPSec Transform Set

The following example configures an IPSec transform set, which is used to define the security association that determines the protocols used to protect the data on the interface:

```
configure
  context <pgw_context_name> -noconfirm
    ipsec transform-set <ipsec_transform-set_name>
      encryption aes-cbc-128
      group none
      hmac sha1-96
      mode tunnel
      end
```

Notes:

- The encryption algorithm, **aes-cbc-128**, or Advanced Encryption Standard Cipher Block Chaining, is the default algorithm for IPSec transform sets configured on the system.

- The **group none** command specifies that no crypto strength is included and that Perfect Forward Secrecy is disabled. This is the default setting for IPSec transform sets configured on the system.
- The **hmac** command configures the Encapsulating Security Payload (ESP) integrity algorithm. The **sha1-96** keyword uses a 160-bit secret key to produce a 160-bit authenticator value. This is the default setting for IPSec transform sets configured on the system.
- The **mode tunnel** command specifies that the entire packet is to be encapsulated by the IPSec header, including the IP header. This is the default setting for IPSec transform sets configured on the system.

Creating and Configuring an IKEv2 Transform Set

The following example configures an IKEv2 transform set:

```
configure
  context <pgw_context_name> -noconfirm
    ikev2-ikesa transform-set <ikev2_transform-set_name>
      encryption aes-cbc-128
      group 2
      hmac sha1-96
      lifetime <sec>
      prf sha1
      end
```

Notes:

- The encryption algorithm, **aes-cbc-128**, or Advanced Encryption Standard Cipher Block Chaining, is the default algorithm for IKEv2 transform sets configured on the system.
- The **group 2** command specifies the Diffie-Hellman algorithm as Group 2, indicating medium security. The Diffie-Hellman algorithm controls the strength of the crypto exponentials. This is the default setting for IKEv2 transform sets configured on the system.
- The **hmac** command configures the Encapsulating Security Payload (ESP) integrity algorithm. The **sha1-96** keyword uses a 160-bit secret key to produce a 160-bit authenticator value. This is the default setting for IKEv2 transform sets configured on the system.
- The **lifetime** command configures the time the security key is allowed to exist, in seconds.
- The **prf** command configures the IKE Pseudo-random Function, which produces a string of bits that cannot be distinguished from a random bit string without knowledge of the secret key. The **sha1** keyword uses a 160-bit secret key to produce a 160-bit authenticator value. This is the default setting for IKEv2 transform sets configured on the system.

Creating and Configuring a Crypto Template

The following example configures an IKEv2 crypto template:

```
configure
  context <pgw_context_name> -noconfirm
    crypto template <crypto_template_name> ikev2-dynamic
      ikev2-ikesa transform-set list <name1> . . . <name6>
      ikev2-ikesa rekey
      payload <name> match childsa match ipv4
        ipsec transform-set list <name1> . . . <name4>
```

```
      rekey
      end
```

Notes:

- The **ikev2-ikesa transform-set list** command specifies up to six IKEv2 transform sets.
- The **ipsec transform-set list** command specifies up to four IPSec transform sets.

Binding the S5 IP Address to the Crypto Template

The following example configures the binding of the S5 interface to the crypto template:

```
configure
  context <pgw_ingress_context_name> -noconfirm
    gtpu-service <gtpu_ingress_service_name>
      bind ipv4-address <s5_interface_ip_address> crypto-template
<sgw_s5_crypto_template>
      exit
    egtp-service <egtp_ingress_service_name>
      interface-type interface-pgw-ingress
      associate gtpu-service <gtpu_ingress_service_name>
      gtpc bind ipv4-address <s5_interface_ip_address>
      exit
    pgw-service <pgw_service_name> -noconfirm
      plmn id mcc <id> mnc <id> primary
      associate egtp-service <egtp_ingress_service_name>
      end
```

Notes:

- The **bind** command in the GTP-U and eGTP service configuration can also be specified as an IPv6 address using the **ipv6-address** command.

Configuring Guard Timer on Create Session Request Processing

P-GW has an existing timer "session setup-timeout" which is hard coded to 60 seconds, which is used as a guard timer for session creation. This timer is used for all APNs and is started when a Create Session Request is received for any session creation.

Internal or external processing issues or delay at external interfaces, for example, Gx/Gy, can cause Create Session Request processing to run longer than time expected in end to end call setup. If the session processing is not complete when the timer expires, the Create Session Request processing is stopped and the P-GW performs an internal cleanup by stopping all other corresponding sessions, for example Gx/Gy. The P-GW responds with a Create Session Failure response stating that no resources are available to S-GW. In successful cases when there's no delay timer is stopped during sending out the Create Session Response.

A new CLI command has been introduced to allow a configurable value to override the previously hardcoded default session setup timeout value of 60 seconds. This will help to fine tune the call setup time at P-GW with respect to end to end call setup time.

Configuring Session Timeout

The following configuration example makes a P-GW session setup timeout configurable.

```
configure
  context  context_name
    pgw-service  service_name
      setup-timeout  timer-value
      [  default | no ] setup-timeout
      end
```

Notes:

- **setup-timeout**: Specifies the session setup timeout period, in seconds. If P-GW is able to process the Create Session Request message before the timer expires, P-GW stops the timer and sends a successful Create Session Response.

  timer_value must be an integer from 1 to 120.

  Default: 60 seconds

- **default**: Default value is 60 seconds. If no value is set, the P-GW service sets the timer to the default value.
- **no**: Sets the timer to the default value of 60 seconds.

Configuring the GTP Echo Timer

The GTP echo timer on the ASR 5500 P-GW can be configured to support two different types of path management: default and dynamic. This timer can be configured on the GTP-C and/or the GTP-U channels.

Default GTP Echo Timer Configuration

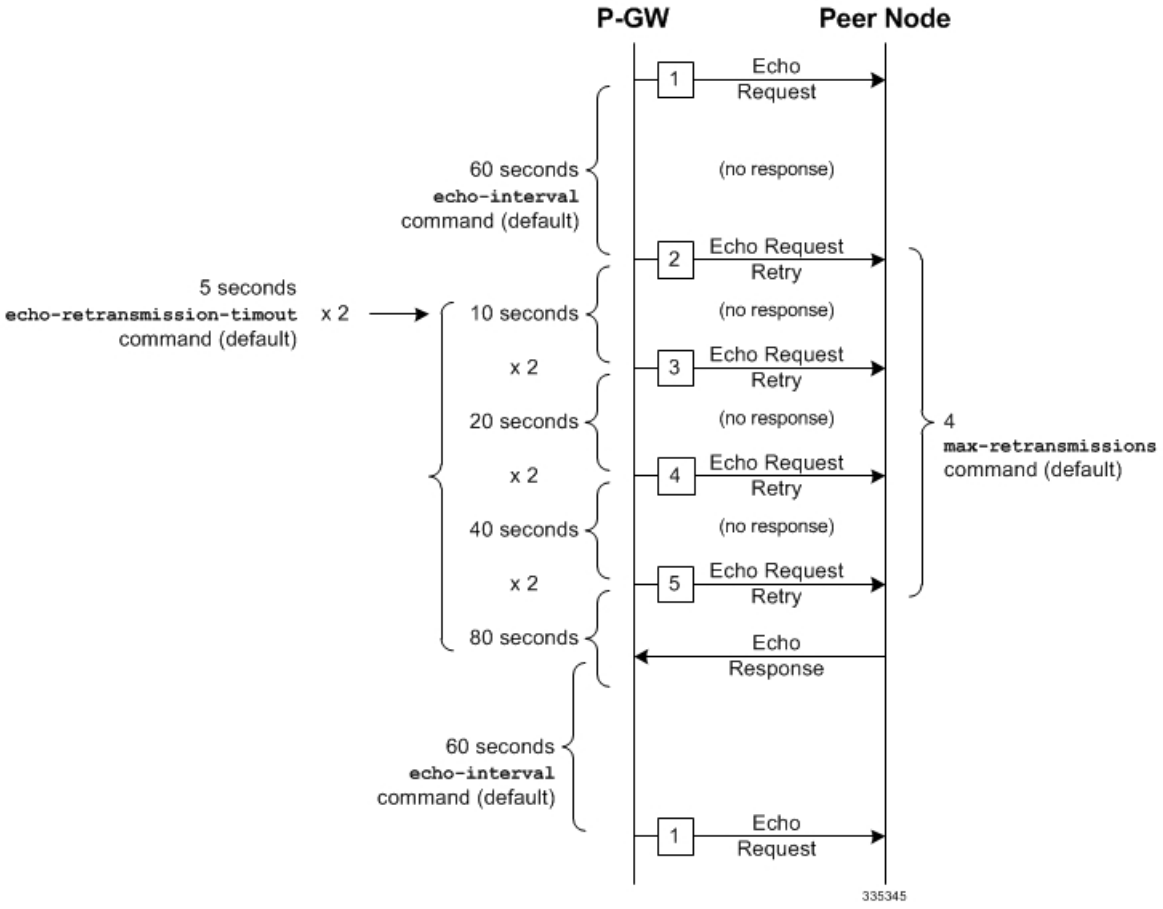
The following examples describe the configuration of the default eGTP-C and GTP-U interface echo timers:

eGTP-C

```
configure
     configure
          context <context_name>
               egtp-service <egtp_service_name>
                    gtpc echo-interval <seconds>
                    gtpc echo-retransmission-timeout <seconds>
                    gtpc max-retransmissions <num>
                    end
```

Notes:

- The following diagram describes a failure and recovery scenario using default settings of the three **gtpc** commands in the example above:



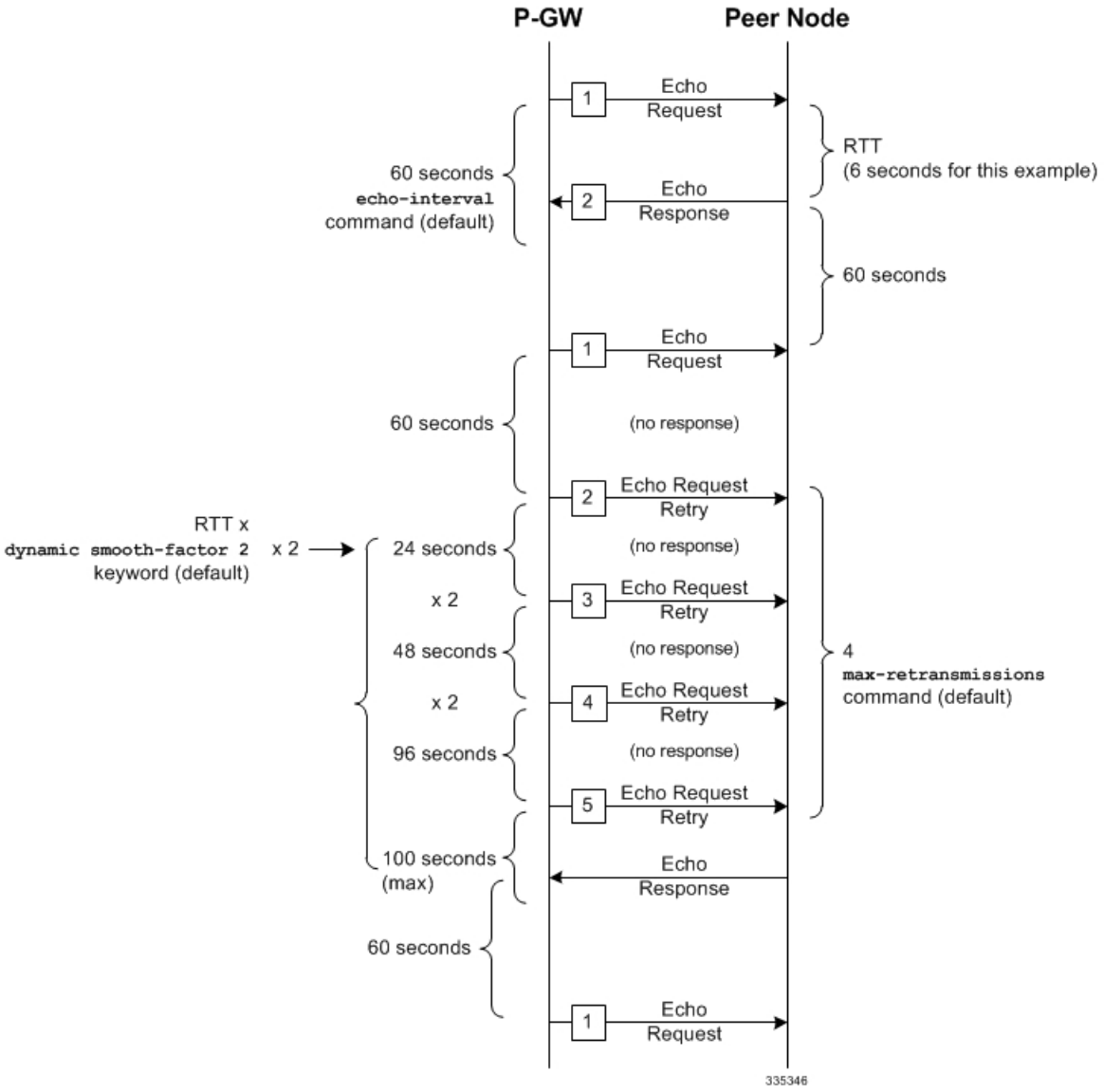
- The multiplier (x2) is system-coded and cannot be configured.

GTP-U

```
configure
  configure
    context <context_name>
      gtpu-service <gtpu_service_name>
        echo-interval <seconds>
        echo-retransmission-timeout <seconds>
        max-retransmissions <num>
        end
```

Notes:

- The following diagram describes a failure and recovery scenario using default settings of the three GTP-U commands in the example above:



- The multiplier (x2) is system-coded and cannot be configured.

Dynamic GTP Echo Timer Configuration

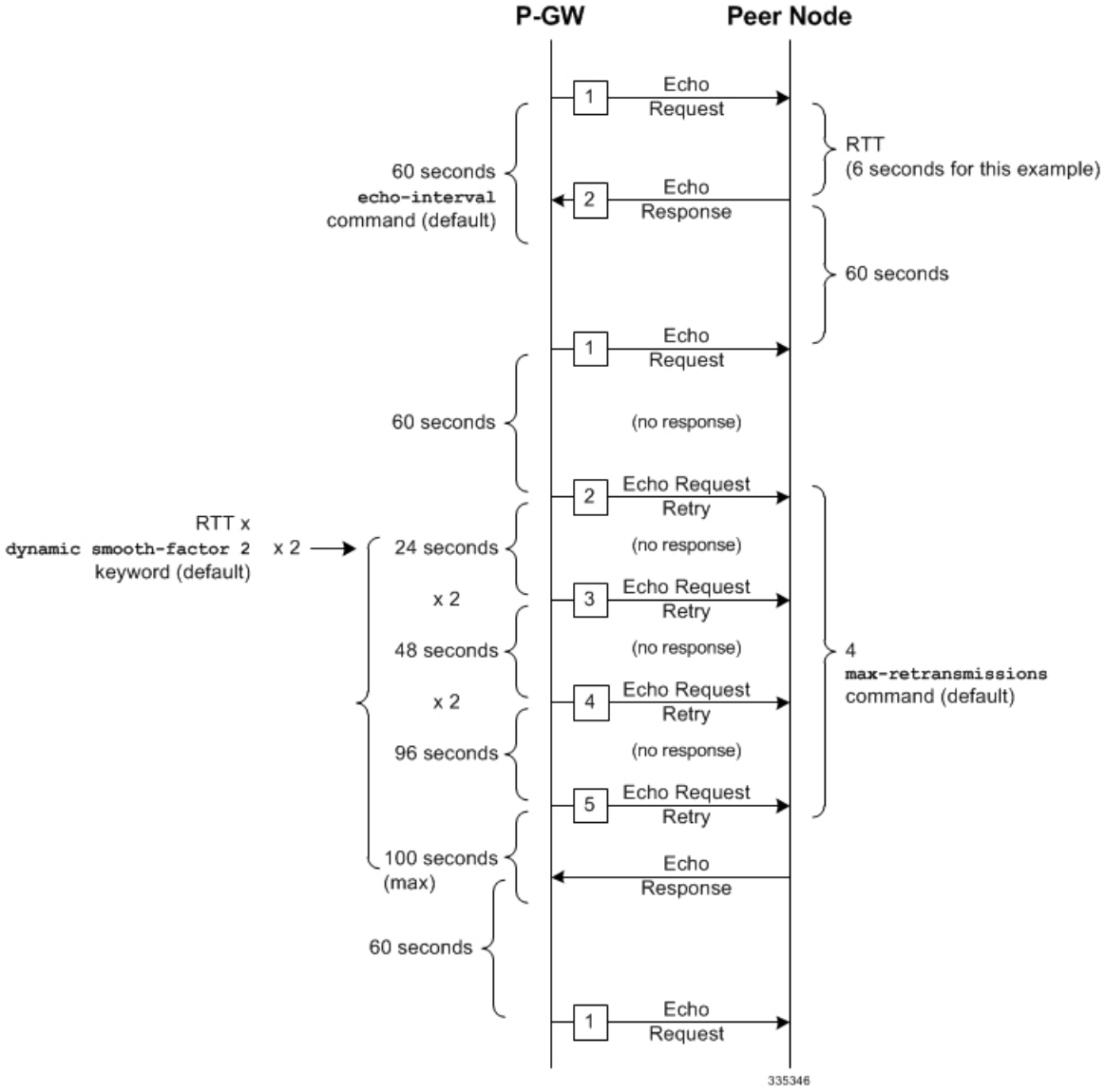
The following examples describe the configuration of the dynamic eGTP-C and GTP-U interface echo timers:

eGTP-C

```
configure
  configure
    context <context_name>
      egtp-service <egtp_service_name>
        gtpc echo-interval <seconds> dynamic smooth-factor <multiplier>
        gtpc echo-retransmission-timeout <seconds>
        gtpc max-retransmissions <num>
        end
```

Notes:

- The following diagram describes a failure and recovery scenario using default settings of the three **gtpc** commands in the example above and an example round trip timer (RTT) of six



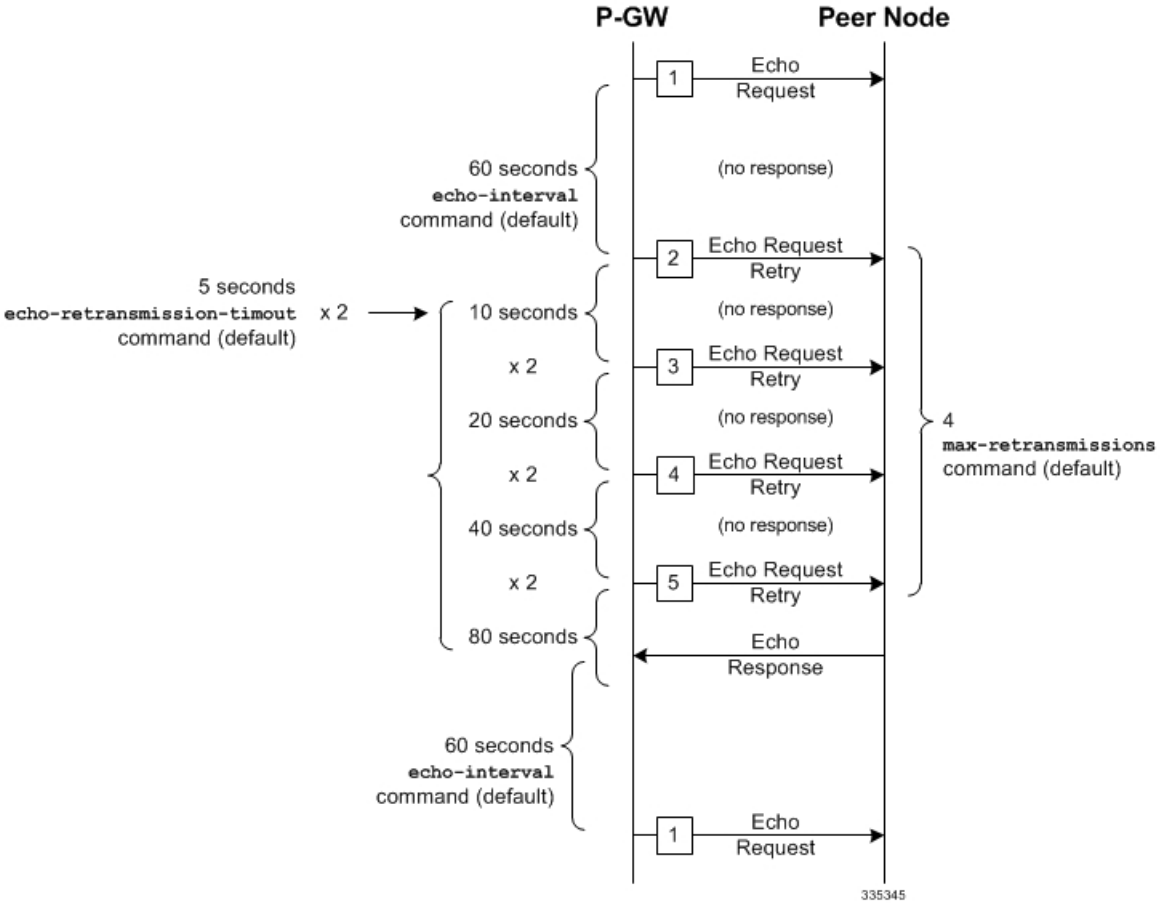
- The multiplier (x2) and the 100 second maximum are system-coded and cannot be configured.

GTP-U

```
configure
  configure
    context <context_name>
      gtpu-service <gtpu_service_name>
        echo-interval <seconds> dynamic smooth-factor <multiplier>
        echo-retransmission-timeout <seconds>
        max-retransmissions <num>
        end
```

Notes:

- The following diagram describes a failure and recovery scenario using default settings of the three **gtpc** commands in the example above and an example round trip timer (RTT) of six seconds:



- The multiplier (x2) and the 100 second maximum are system-coded and cannot be configured.

Configuring GTPP Offline Accounting on the P-GW

By default the P-GW service supports GTPP accounting. To provide GTPP offline charging, configure the P-GW with the example parameters below:

```
configure
      gtpp single-source
      context <ingress_context_name>
            subscriber default
                  accounting mode gtpp
                  exit
            gtpp group default
                  gtpp charging-agent address <gz_ipv4_address>
                  gtpp echo-interval <seconds>
                  gtpp attribute diagnostics
                  gtpp attribute local-record-sequence-number
                  gtpp attribute node-id-suffix <string>
                  gtpp dictionary <name>
                  gtpp server <ipv4_address> priority <num>
                  gtpp server <ipv4_address> priority <num> node-alive enable
```

```
            exit
      policy accounting <gz_policy_name>
            accounting-level {type}
            operator-string <string>
            cc profile <index> buckets <num>
            cc profile <index> interval <seconds>
            cc profile <index> volume total <octets>
            exit
      exit
context <ingress_context_name>
      apn apn
            associate accounting-policy <gz_policy_name>
            exit
      interface <gz_interface_name>
            ip address <address>
            exit
      exit
port ethernet <slot_number/port_number>
      no shutdown
      bind interface <gz_interface_name> <ingress_context_name>
      end
```

Notes:

- **gtpp single-source** is enabled to allow the system to generate requests to the accounting server using a single UDP port (by way of a AAA proxy function) rather than each AAA manager generating requests on unique UDP ports.
- **gtpp** is the default option for the **accounting mode** command.
- An accounting mode configured for the call-control profile will override this setting.
- **accounting-level** types are: flow, PDN, PDN-QCI, QCI, and subscriber. Refer to the *Accounting Profile Configuration Mode Commands* chapter in the *Command Line Interface Reference* for more information on this command.

Configuring GTP Throttling Feature

The GTP Throttling feature allows the operator to control the rate of incoming/outgoing messages on P-GW/GGSN.

Configuring the Outgoing Control Message Throttling

The following configuration helps to enable outgoing control message throttling.

```
configure
  context context_name
  [no] gtpc overload-protection egress rlf-template rlf_template_name
throttling-overload-policy throttling_overload_policy_name
  end
```

Configuring the Incoming Control Message Throttling

The following configuration helps to enable incoming control message throttling.

```
configure
  context context_name
  [no] gtpc overload-protection ingress msg-rate msg_rate [delay-tolerance
```

```
msg_queue_delay ] [ queue-size queue_size ]
 end
```

Configuring Local QoS Policy

The configuration examples in this section create a local QoS policy. A local QoS policy service can be used to control different aspects of a session, such as QoS, data usage, subscription profiles, or server usage, by means of locally defined policies.

Important Use of the Local QoS Policy feature requires that a valid license key be installed. Contact your local Sales or Support representative for information on how to obtain a license.

Creating and Configuring a Local QoS Policy

The following configuration example enables a local QoS policy on the P-GW:

```
configure
  local-policy-service <name> -noconfirm
    ruledef <ruledef_name> -noconfirm
      condition priority <priority> <variable> match <string_value>
      condition priority <priority> <variable> match <int_value>
      condition priority <priority> <variable> nomatch <regex>
      exit
    actiondef <actiondef_name> -noconfirm
      action priority <priority> <action_name> <arguments>
      action priority <priority> <action_name> <arguments>
      exit
    actiondef <actiondef_name> -noconfirm
      action priority <priority> <action_name> <arguments>
      action priority <priority> <action_name> <arguments>
      exit
    eventbase <eventbase_name> -noconfirm
      rule priority <priority> event <list_of_events> ruledef <ruledef_name>
actiondef <actiondef_name>
      end
```

Notes:

- A maximum of 16 local QoS policy services are supported.
- A maximum 256 ruledefs are suggested in a local QoS policy service for performance reasons.
- The **condition** command can be entered multiple times to configure multiple conditions for a ruledef. The conditions are examined in priority order until a match is found and the corresponding condition is applied.
- A maximum of 256 actiondefs are suggested in a local QoS policy service for performance reasons.
- The **action** command can be entered multiple times to configure multiple actions for an actiondef. The actions are examined in priority order until a match is found and the corresponding action is applied.
- Currently, only one eventbase is supported and must be named "default".

- The **rule** command can be entered multiple times to configure multiple rules for an eventbase.
- A maximum of 256 rules are suggested in an eventbase for performance reasons.
- Rules are executed in priority order, and if the rule is matched the action specified in the actiondef is executed. If an event qualifier is associated with a rule, the rule is matched only for that specific event. If a qualifier of **continue** is present at the end of the rule, the subsequent rules are also matched; otherwise, rule evaluation is terminated on first match.

Binding a Local QoS Policy

Option 1: The following configuration example binds the previously configured local QoS policy:

```
configure
  context <pgw_context_name> -noconfirm
    apn <name>
      ims-auth-service <local-policy-service name>
      end
```

Notes:

- A maximum of 30 authorization services can be configured globally in the system. There is also a system limit for the maximum number of total configured services.
- Useful in case of emergency calls; PCRF is not involved.

Option 2: The following configuration example may also be used to bind the previously configured local QoS policy or a failure handling template:

```
configure
  context <pgw_context_name> -noconfirm
    ims-auth-service <auth_svc_name>
      policy-control
        associate failure-handling-template <template_name>
        associate local-policy-service <service_name>
        end
```

Notes:

- Only one failure handling template can be associated with the IMS authorization service. The failure handling template should be configured prior to issuing this command.
- The failure handling template defines the action to be taken when the Diameter application encounters a failure supposing a result-code failure, tx-expiry or response-timeout. The application will take the action given by the template. For more information on failure handling template, refer to the *Diameter Failure Handling Template Configuration Mode Commands* chapter in the *Command Line Interface Reference*.
- You must select "local-fallback" in the failure handling template to support fallback to local policy.
- To support fallback to local policy in case of failure at PCRF, the local policy service should be associated with an IMS authorization service. In case of any failures, the local policy template associated with the ims-auth service will be chosen for fallback.

Verifying Local QoS Policy

The following configuration example verifies if local QoS service is enforced:

```
logging filter active facility local-policy level debug
logging active
show local-policy statistics all
```

Notes:

- Please take extreme caution not to use logging feature in console port and in production nodes.

Configuring X.509 Certificate-based Peer Authentication

The configuration example in this section enables X.509 certificate-based peer authentication, which can be used as the authentication method for IP Security on the P-GW.

Important Use of the IP Security feature requires that a valid license key be installed. Contact your local Sales or Support representative for information on how to obtain a license.

The following configuration example enables X.509 certificate-based peer authentication on the P-GW.

In Global Configuration Mode, specify the name of the X.509 certificate and CA certificate, as follows:

```
configure
  certificate name <cert_name> pem url <cert_pem_url> private-key pem url
<private_key_url>
  ca-certificate name <ca_cert_name> pem url <ca_cert_url>
  end
```

Notes:

- The **certificate name** and **ca-certificate list ca-cert-name** commands specify the X.509 certificate and CA certificate to be used.
- The PEM-formatted data for the certificate and CA certificate can be specified, or the information can be read from a file via a specified URL as shown in this example.

When creating the crypto template for IPSec in Context Configuration Mode, bind the X.509 certificate and CA certificate to the crypto template and enable X.509 certificate-based peer authentication for the local and remote nodes, as follows:

```
configure
  context <pgw_context_name> -noconfirm
    crypto template <crypto_template_name> ikev2-dynamic
      certificate name <cert_name>
      ca-certificate list ca-cert-name <ca_cert_name>
      authentication local certificate
      authentication remote certificate
      end
```

Notes:

- A maximum of 16 certificates and 16 CA certificates are supported per system. One certificate is supported per service, and a maximum of four CA certificates can be bound to one crypto template.
- The **certificate name** and **ca-certificate list ca-cert-name** commands bind the certificate and CA certificate to the crypto template.
- The **authentication local certificate** and **authentication remote certificate** commands enable X.509 certificate-based peer authentication for the local and remote nodes.

Configuring RFL Bypass Feature

The Bypass Rate Limit Function is an enhancement to the existing GTP Throttling feature. The RLF feature allows the operator to control the bypassing of some messages being throttled.

A new command option **throttling-override-policy** has been added to the existing CLI command **gtpc overload-protection egress rlf-template rlf-temp** which allows you to selectively by-pass throttling for a configured message type or for all messages in emergency call or priority call or call for the configured APN. A new CLI command mode **throttling-override-policy** has been also been introduced for Generic syntax for throttling override policy.

Configuring the Throttling Override Policy Mode

The following configuration helps to create a GTP-C Throttling Override Policy and to enter GTP-C Throttling Override Policy mode.

```
configure
  throttling-override-policy throttling-override-policy_name
```

Notes:

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-throttling-override-policy)#
```

Configuring the RLF Bypass Feature

The following configuration configures message types which can bypass the rate limiting function.

```
configure
  throttling-override-policy  throttling-override-policy_name
    [  default | no ] egress bypass-rlf pgw { msg-type { cbr | dbr | ubr
 | emergency-call | earp-pl-list {1 | 2 | 3 | 4 | 5 … | 15 }+ | apn-names
  <apn-name1>  <apn-name2>  <apn-name3>   }
    end
```

Notes:

- If an empty throttling-override-policy is created, then the default values for all the configurables are zeros/disabled.
- If no throttling-override-policy is associated, then **show service configuration** for P-GW will show it as "n/a".
- Maximum number of throttling-override-policy that can be added are 1024. This limit is the same as max RLF templates.

Example

The following command configures Create Bearer Request message type at the P-GW node to bypass throttling.

```
egress bypass-rlf pgw msg-type cbr
```

Auto Correction of VoLTE Sessions

Feature Information

Summary Data

Status	Modified Functionality
Introduced-In Release	21.2
Modified-In Release(s)	Not Applicable
Applicable Product(s)	P-GW
Applicable Platform(s)	ASR 5500
Default Setting	Disabled
Related CDETS ID(s)	CSCvc72275
Related Changes in This Release	Not Applicable
Related Documentation	*P-GW Administration Guide* *Command Line Interface Reference*

Revision History

Important Revision history details are not provided for features introduced before Release 21.2.

Revision Details	Release	Release Date
New in this release.	21.2	April 27, 2017

Feature Description

When dynamic rules for IP Multimedia Subsystem (IMS) sessions are lost after a switchover, VoLTE calls are impacted. To recover the calls, the IMS sessions have to be cleared manually to re-establish the PDN with the correct dynamic rules. The Auto Correction of VoLTE Sessions feature enables a dynamic rule check such that when the P-GW receives an RAR (Re-Auth-Request) message, it automatically identifies and rectifies

the issue without manual intervention. This features only applies to the APN that is configured on that uses the "RAR" message as a trigger for the check.

How It Works

After the APN receives any RAR message from the Policy Control and Charging Rules Function (PCRF), a Re-Auth- Answer (RAA) message is immediately sent. When the feature is enabled, an additional check is done at the P-GW to verify if there are any dynamic rules associated with the default bearer. Assuming the Session Initiation Protocol (SIP) rule on the default bearer is recovered, other dedicated bearers are also recovered. If dynamic rules are not associated with the default bearer, the call is terminated. Then, a Delete Bearer Request is sent for the default bearer with the cause code - Reactivation Required. To ensure the reason code is sent, the APN must be configured with "pdn-behavior ims". Subsequently, a Credit-Control-Request-Type (CCR-T) is sent to PCRF and other diameter interfaces (s6b, Gy, and Rf). Thereby, the automatic recovery procedure involves termination of a subscriber connection when an anomaly is detected. The subscriber has to then reconnect to the network. The mobile originated or terminated call is rejected for the subscriber where the dynamic rules are lost after a switchover.

Configuring the Auto Correction of VoLTE Sessions Feature

The following section provides the configuration commands to enable or disable the feature.

Enabling or Disabling the Dynamic Rule Check

The new CLI command, **pdn validate-post-switchover**, is added to enable the dynamic rule check for the auto correction of the VoLTE session. To enable this feature, configure the command at the base APN. This feature should be configured only for the VoLTE/IMS APNs for which auto recovery is required.

This feature is disabled by default.

To enable or disable the feature, enter the following commands:

```
configure
   context <context_name>
       apn <apn_name>
          [no] pdn validate-post-switchover
          end
```

Notes:

- **no:** Disables the configured Auto correction of VoLTE sessions on the base APN.
- **pdn validate-post-switchover:** Validates the dynamic rules for automatic recovery after a switchover.

Monitoring and Troubleshooting

This section provides information regarding show commands and/or their outputs in support of the Auto Correction of VoLTE Sessions feature.

Show Commands

This section lists all the show commands available to monitor this feature.

show configuration apn

The above CLI command is introduced to check if the feature is enabled at the APN level. If "pdn validate-post-switchover" is present then the feature is enabled.

show active-charging service statistics

This command has been modified to display the following output:

```
show active-charging service statistics
ACS Data Statistics:
  Packets Dropped due to System-Limit L4-Flows:                          0
  Packets Dropped - Invalid Len in IP Hdr(Dwlink):                       0
  Packets Dropped - Invalid Ver in IP Hdr(Dwlink):                       0
  Packets Not Processed due to Flow-limit:                               0
  Packets Not Processed due to CLP not found:                            0
  Packets Dropped CLP in Preservation Mode:                              0
  Total Pkts:                                                            0
  Total Collisions in data session hash:                                 0

ACS Reject Reason:
  RuleBase Mismatch  :                                                   0
  Bandwidth-Policy Mismatch  :                                           0
  CBB-Policy Mismatch  :                                                 0
  CF Policy Mismatch  :                                                  0
  No RuleBase configured in APN/Subs:                                    0
  No active rule in Rulebase/Subs:                                       0
  No Bandwidth-Policy configured in APN/Subs:                            0
  No Resources:                                                          0
  Max Sessions:                                                          0
  Reject Probability Exceeded:                                           0
  Rule Recovery Failed:                                                  0
  CDR Flow Control Initiated:                                            0

Protocol Reject stats:
  WTP Non-initial PDU:                                                   0
  WSP-CO Non-initial Connect PDU                                         0

Dynamic Rule Statistics:
  Total Subscribers:                0   Current Subscribers:             0
  Charging Msg Received:            0   Rule Defn Received:              0
  Installs Received:                0   Removes Received:                0
  Installs Succeeded:               0   Removes Succeeded:               0
  ADC Rules Received:               0   Total ADC Rules:                 0
  ADC Install Succeeded:            0   ADC Install Failed:              0
  ADC Custom Mute Received:         0   ADC Custom Unmute Received:      0
  ADC Start Sent:                   0   ADC Stop Sent:                   0
  L7 Rules Received:                0
  L7 Install Succeeded:             0   L7 Install Failed:               0
  Installs Failed:                  0   Removes Failed:                  0
  Install Failure Reason:
    No Resources:                   0   No Rulebase Match:               0
    No RuleName Match:              0   Rulebase Count Exceeded:         0
    Local Copy Failed:              0   Invalid Protocol:                0
    Invalid Source Mask:            0   Invalid Dest Mask:               0
    No Grp-of-Rdef Match:           0
    ADC Invalid Rule:               0   ADC Invalid Readdress:           0
    L7 Rule Invalid:                0
    L7 Protocol Invalid:            0   L7 Field Invalid:                0
    L7 Operator Invalid:            0   L7 Value Invalid:                0
    L7 Case-Sens Invalid:           0
  Remove Failure Reason:
    No RuleName Match:              0   No Grp-of-Rdef Match:            0
```

```
    Local Copy Failed:              0

Bandwidth Limiting Statistics:
    ITC Drops:
      Uplink Packets:                   0   Uplink Bytes:                 0
      Downlink Packets:                 0   Downlink Bytes:               0
    Dynamic Rule Bandwidth Limiting Drops:
      Uplink Packets:                   0   Uplink Bytes:                 0
      Downlink Packets:                 0   Downlink Bytes:               0
    Per-Bearer Bandwidth Limiting Drops:
      Uplink Packets:                   0   Uplink Bytes:                 0
      Downlink Packets:                 0   Downlink Bytes:               0

Credit-Control Group Statistics:
  CC Dropped Uplink Packets:        0  CC Dropped Uplink Bytes:           0
  CC Dropped Downlink Packets:      0  CC Dropped Downlink Bytes:         0

Readdressing Failure Statistics (Packets):
  Non SYN Flow:                     0  Duplicate Key:                     0
  Dropped Pkts:                     0


First-request-only redirections:                                        0

Fallback Statistics:
  Bandwidth Policy Applied:                                             0
  Bandwidth Policy Failed:                                              0
```

Bulk Statistics

This section lists all the bulk statistics that have been added, modified, or deprecated to support this feature.

ECS Schema

This section displays the new bulk stats that have been added to indicate dynamic recovery failure :

- dyn_rule_recovery_failure:

  The total number of sessions terminated due to dynamic rule recovery failure.
- dyn_rule_recovery_num_sess_not_terminated:

  The total number of sessions that are not terminated after switchover because dynamic rules were not installed on the default bearer.