GGSN Service Configuration Procedures

This chapter is meant to be used in conjunction with the previous chapter that describes the information needed to configure the system to support GGSN functionality for use in GPRS/UMTS networks.

It is recommended that you identify the options from the previous chapters that are required for your specific deployment. You can then use the procedures in this chapter to configure those options.

Important At least one Packet Accelerator Card (PAC) or Packet Services Card (PSC) must be made active prior to service configuration. Information and instructions for configuring PACs/PSCs to be active can be found in the Configuring System Settings chapter of the System Administration Guide.

Caution While configuring any base-service or enhanced feature, it is highly recommended to take care of conflicting or blocked IP addresses and port numbers for binding or assigning. In association with some service steering or access control features, like *Access Control List* configuration, use of inappropriate port number may result in communication loss. Refer respective feature configuration document carefully before assigning any port number or IP address for communication with internal or external network.

GGSN Service Configuration

GGSN services are configured within contexts and allow the system to function as a GGSN in the either a GPRS or UMTS wireless data network.

Important This section provides the minimum instruction set for configuring a GGSN service that allows the system to process PDP contexts. Commands that configure additional GGSN service properties are provided in the *GGSN 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*.

To configure the system to work as GGSN service:

Step 1 Create the GGSN service, local User Datagram Protocol (UDP) port for the Gn interfaces' IP socket, and bind it to an IP address by applying the example configuration in the *GGSN Service Creation and Binding* section.

Step 2 Associate the accounting context for the GGSN service and configure charging characteristic profile parameters for GGSN service by applying the example configuration in the *Accounting Context and Charging Characteristics Configuration* section.

Step 3 Configure the SGSN and PLMN related policy and session setup timeout for the GGSN service by applying the example configuration in the *SGSN and PLMN Policy Configuration* section.

Step 4 Optional. Configure the GGSN service to support network-requested PDP contexts by applying the example configuration in the *Network-requested PDP Context Support Configuration* section.

Step 5 Verify your GGSN configuration by following the steps in the *GGSN Configuration Verification* section.

Step 6 Save your configuration as described in the *Verifying and Saving Your Configuration* chapter.

GGSN Service Creation and Binding

Use the following example to create the GGSN service and bind it to an IP address:

```
configure
        context <vpn_ctxt_name> -noconfirm
          ggsn-service <ggsn_svc_name>


            end
```

Notes:

- A maximum of 256 services (regardless of type) can be configured per system.
- Bind address should not conflict with any other GTP-based service.

Accounting Context and Charging Characteristics Configuration

Use the following example to configure a GTPP accounting context and charging characteristics parameters for GGSN service.

```
configure
   context <vpn_ctxt_name>
      ggsn-service <ggsn_svc_name>
      accounting context <aaa_ctxt_name>

      cc profile <cc_prof_index>
      end
```

Notes:

- Charging characteristics behavior and profile index can be configured for multiple CC profile indexes. For more options and keywords like **buckets**, **interval**, , **sgsns**, **tariff**, **volume** etc., refer cc profile section in Command Line Interface Reference.
- This command works in conjunction with the **cc-sgsn** command located in the APN configuration mode that dictates which CCs should be used for subscriber PDP contexts. Refer to the *APN Configuration* section in this chapter.

SGSN and PLMN Policy Configuration

Use the following example to configure the SGSN and PLMN related policy and session setup timeout for the GGSN service:

```
configure
        context <vpn_ctxt_name>
           ggsn-service <ggsn_svc_name>
              plmn id mcc <mcc_number> [ mnc <mnc_number> ] [primary]
              sgsn address <ip_address> / <subnet_mask>
              plmn unlisted-sgsn [foreign | home | reject]
              setup-timeout <dur_sec>
              end
```

Notes:

- SGSN or PLMN related policy can be defined for multiple SGSNs or PLMN.
- For optional configuration parameters of SGSN address, refer Command Line Interface Reference.

Important The GGSN only communicates with the SGSNs configured using this command unless a PLMN policy is enabled to allow communication with unconfigured SGSNs. PLMN policies are configured using the **plmn unlisted-sgsn** command.

Network-requested PDP Context Support Configuration

Use the following example to configure the GGSN to support the network-requested PDP context:

```
configure
        context <vpn_ctxt_name>
          network-requested-pdp-context activate <ip_address> dst-context
<dst_ctxt_name> imsi <imsi> apn <apn_name>
          network-requested-pdp-context gsn-map <ip_address>
          end
```

Notes:

- It is recommended that this functionality be configured in the system source context(s) along with the GGSN service(s).
- Up to 1000 IP address can be configured for network request PDP context support.
- Only one GSN-MAP node can be configured per system context.

GGSN Configuration Verification

Step 1 Verify that your GGSN services were created and configured properly by entering the following command in Exec Mode:

show ggsn-service name <*ggsn_svc_name*>}

The output of this command given below is a concise listing of GGSN service parameter settings as shown in the sample output displayed. In this example, a GGSN service called *ggsn1* was configured and you can observe some parameters configured as default.

```
Service name:                                        ggsn1
Context:                                                 ggsn1
Associated PGW svc:                              None
Associated GTPU svc:                            None
Accounting Context Name:  ggsn1
dns-client Context Name:
Authorize:                                          Disabled
Fqdn-name:                                          Disabled
Bind:                                          Done
Local IP Address:                192.168.70.1                 Local IP Port: 2123
Self PLMN Id.:                      MCC:    450, MNC:      06
Retransmission Timeout:    20 (secs)
Max Retransmissions:          4
Restart Counter:                  16
Echo Interval:                      60 (secs)




Guard Interval:                    100 (secs)
Setup Timeout:                      60 (secs)
PLMN Policy:                          Reject unlisted SGSN
Reject Code Policy:
        Authentication Server Timeout:  User Authentication Failed
        Accounting Server Timeout:          No Resources Available
Ran Procedure Ready:          Disabled
NSAPI in Create PDP response:  Disabled
Duplicate Subscriber Addr Request: Reject
trace-collection-entity:  Disabled
Path Failure Detection on gtp msgs:  Echo
GTP Private Extensions:
                  None
Max IP sessions:                  4000000
```

```
Max PPP sessions:                2500000
Max sessions:                      4000000
Service Status:                  Started
Newcall Policy:                  None
MBMS Policy:                        None
MBMS Charging ID Optimization:  Disabled

3GPP Qos to DSCP Mapping (for G-PDUs):
        qci 1:              ef
        qci 2:              ef
        qci 3:              af11
        qci 4:              af11
        qci 5:              ef
        qci 6:              ef
        qci 7:              af21
        qci 8:              af21
        qci 9:              be
3GPP Qos to DSCP Mapping based on Alloc. Prio:
        qci 5 (Alloc. P 1):    ef
        qci 5 (Alloc. P 2):    ef
        qci 5 (Alloc. P 3):    ef
        qci 6 (Alloc. P 1):    ef
        qci 6 (Alloc. P 2):    ef
        qci 6 (Alloc. P 3):    ef
        qci 7 (Alloc. P 1):    af21
        qci 7 (Alloc. P 2):    af21
        qci 7 (Alloc. P 3):    af21
        qci 8 (Alloc. P 1):    af21
        qci 8 (Alloc. P 2):    af21
        qci 8 (Alloc. P 3):    af21
        GTPC messages:                be
        Background:                           be
Charging Characteristics(CC) Behaviors:
      No records (Bit No.):    0
Charging Characteristics(CC) Profiles:
        Profile 0:
         Buckets: 4                                                  SGSN changes: 4
        Profile 1:
         Buckets: 4                                                  SGSN changes: 4
SGSN Configuration List:
        sgsn address 2.2.2.2/32 mcc 111 mnc 999 description aaa-ggsn
```

Step 2 Verify configuration for errors by entering the following command in Exec Mode:

`show configuration errors section ggsn-service verbose`

GTPP Accounting Support Configuration

This section provides instructions for configuring GTPP-based accounting for subscriber PDP contexts. GTPP-based accounting for a subscriber can be configured by CGF server configuration in a GTPP group. Additionally individual CGF server can be configured with this example.

For information on configuring Diameter and RADIUS AAA functionality, if you are using StarOS 12.3 or an earlier release, refer to the *AAA and GTPP Interface Administration and Reference*. If you are using StarOS 14.0 or a later release, refer to the *AAA Interface Administration and Reference*.

When the GTPP protocol is used, accounting messages are sent to the charging gateways (CGs) over the Ga interface. The Ga interface and GTPP functionality are typically configured within the system's source context.

CDRs are generated according to the interim triggers configured using the charging characteristics configured for the GGSN, and a CDR is generated when the session ends.

GTPP version 2 is used by default. However, if version 2 is not supported by the CGF, the system reverts to using GTPP version 1. All subsequent CDRs are always fully-qualified partial CDRs. For CDR encoding different dictionaries are supported.

For more information on GTPP dictionaries, if you are using StarOS 12.3 or an earlier release, refer to the *AAA and GTPP Interface Administration and Reference*. If you are using StarOS 14.0 or a later release, refer to the *GTPP Interface Administration and Reference*.

Whether or not the GGSN accepts charging characteristics from the SGSN can be configured on a per-APN basis based on whether the subscriber is visiting, roaming or, home.

By default, the GGSN always accepts the charging characteristics from the SGSN. However it accepts charging characteristics from RADIUS too, they must always be provided by the SGSN for GTPPv1 requests for primary and secondary PDP contexts.

If the system is configured to reject the charging characteristics from the SGSN, the GGSN can be configured with its own that can be applied based on the subscriber type (visiting, roaming, or home) at the APN level (refer to the *APN Configuration* section of this chapter for more information). GGSN charging characteristics consist of a profile index and behavior settings (refer to the *GGSN Service Configuration* section of this chapter for more information). The profile indexes specify the criteria for closing accounting records based specific criteria (refer to the *GGSN Service Configuration* section of this chapter for more information).

Important This section provides the minimum instruction set for configuring a GTPP accounting support in a GGSN service. Commands that configure additional GTPP accounting properties are provided in the *Command Line Interface Reference* guide.

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

To configure the GTPP accounting support for a GGSN service:

Step 1 Create the GTPP group in accounting context by applying the example configuration in the *GTPP Group Creation* section.

Step 2 Configure the charging agent and GTPP server (CGF) related parameters for the GTPP accounting support by applying the example configuration in the *GTPP Group Configuration* section.

Step 3 Verify your GTPP group and accounting configuration by following the steps in the *GTPP Group Configuration Verification* section.

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

GTPP Group Creation

Use the following example to create the GTPP group to support GTPP accounting:

```
configure
        context <vpn_ctxt_name>
```

```
gtpp group <gtpp_group_name> -noconfirm
end
```

Notes:

- In addition to one default GTPP group "default" a maximum of 8 GTPP groups can be configured with this command in a context.
- In case no GTPP group is configured in this context, system creates a default GTPP group named "default" and all the CGF servers and their parameters configured in this context are applicable to this "default" GTPP group.

GTPP Group Configuration

Use the following example to configure the GTPP server parameters, GTPP dictionary, and optionally CGF to support GTPP accounting:

```
configure
        context <vpn_ctxt_name>
           gtpp group <gtpp_group_name>
              gtpp charging-agent address <ip_address> [port <port>]
              gtpp server <ip_address> [max <msgs >] [priority <priority>]
              gtpp dictionary <dictionaries>
              gtpp max-cdrs <number_cdrs> [wait-time <dur_sec>]
              gtpp transport-layer {tcp | udp}

              end
```

Notes:

- In addition to one default GTPP group "default" a maximum of 8 GTPP groups can be configured with this command in a context.
- In case no GTPP group is configured in this context, system creates a default GTPP group named "default" and all the CGF servers and their parameters configured in this context are applicable to this "default" GTPP group.
- Command for CGF **gtpp charging-agent** is optional and configuring gtpp charging-agent on port 3386 may interfere with ggsn-service configured with the same ip address. Multiple interfaces can be configured within a single context if needed.
- For more information on GTPP dictionary encoding, if you are using StarOS 12.3 or an earlier release, refer to the *AAA and GTPP Interface Administration and Reference*. If you are using StarOS 14.0 or a later release, refer to the *GTPP Interface Administration and Reference*.
- For better performance, it is recommended to configure maximum number of CDRs as 255 with **gtpp max-cdrs** command.
- Operator can select transport layer protocol as TCP or UDP for Ga interface with **gtpp transport-layer** command.
- Multiple GTPP server can be configured using multiple instances of this command subject to following limits:
  - Total 4 GTPP server in one GTPP group
  - Total 32 GTPP server in one context or in the overall configuration

- Total 33 GTPP groups (1 default and 32 user defined GTPP groups) can be configured in one context. Number of CGFs in 1 GTPP group is limited to 4 and a total of 32 CGF servers across all GTPP groups in one context are configurable.
- Total 32 GTPP groups can also be configured under an APN

GTPP Group Configuration Verification

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

`show gtpp accounting servers`

This command produces an output similar to that displayed below:

```
context: source
Preference IP                              Port      Priority     State                  Group
---------- --------------- ----- -------- ---------------- ----------
Primary      192.168.32.135        3386        1                   Active                default
Primary      192.168.89.9            3386        100                Active                 default
```

Step 2 Verify configuration for errors by entering the following command in Exec Mode:

`show configuration errors section ggsn-service verbose`

APN Configuration

This section provides instructions for configuring the APN templates that are used to determine how PDP contexts should be processed. APNs are configured in system authentication contexts.

Important This section provides the minimum instruction set for configuring APNs in a GGSN service. Commands that configure additional APN properties are provided in *APN 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 GGSN service as described in the *GGSN Service Configuration* section of this guide.

To configure the APN properties for a GGSN service:

Step 1 Create the APN in system context and specify the support of PDP contexts and selection mode by applying the example configuration in the APN Creation and Configuration section.

Step 2 Configure the authentication and accounting parameters in APN by applying the example configuration in the Authentication, Accounting, and GTPP Group Configuration in APN section.

Step 3 Configure the IP allocation method in APN by applying the example configuration in the IP Address Allocation Method Configuration in APN section.

Step 4 Optional. Configure the charging characteristics related parameters for the APN by applying the example configuration in the Charging Characteristics Parameter Configuration in APN section.

Step 5 Optional. Configure virtual APNs by applying the example configuration in the Virtual APN Configuration section.

Step 6 Optional. Configure other optional parameters for the APN by applying the example configuration in the Other Optional Parameter Configuration in APN section.

Step 7 Verify your APN configuration by following the steps in the APN Configuration Verification section.

Step 8 Save your configuration as described in the *Verifying and Saving Your Configuration* chapter.

APN Creation and Configuration

Use the following example to create and configure the APNs:

```
configure
        context <vpn_ctxt_name>
           apn <apn_name> -noconfirm
              pdp-type {ipv4 [ipv6] | ipv6 [ipv4] | ppp}
              selection-mode {sent-by-ms | chosen-by-sgsn | subscribed}
              ip context-name <dst_ctxt_name>
              end
```

Notes:

- Up to 2,048 APNs can be configured on a system.
- APN templates should be created/configured within system authentication contexts or destination context.
- Selection mode parameter's setting must be identical to the selection mode setting on the SGSN(s) that the GGSN communicates with. The GGSN rejects attempts to establish PDP contexts from any SGSN having a different setting.
- For IPv6 calls to work, the destination context must have an IPv6 interface configured in it.
- If the APN supports Mobile IP for subscriber PDP contexts, then ip context-name command is used to indicate the context in which the FA service is configured.
  - If no context name is specified, the system uses the context in which the APN is configured.
  - If Mobile IP is supported and no name is specified, the system uses the context in which the GGSN service facilitating the PDP context is located.

Authentication, Accounting, and GTPP Group Configuration in APN

This section describes the procedure to configure the authentication and accounting parameters for an APN. It also specify the procedure to attach a GTPP group with an APN.

Step 1 Configure the authentication and accounting parameters by applying the example configuration in the *Authentication and Accounting Configuration in APN* section.

Step 2 Attach a GTPP group with APN by applying the example configuration in the *GTPP Group Association to APN* section.

Authentication and Accounting Configuration in APN

Use the following example to configure the accounting mode and authentication parameter for APN:

```
configure
        context <dst_ctxt_name>
           apn <apn_name>
              accounting-mode {none | gtpp | radius [no-interims]
[no-early-pdus]}
              default authentication
              end
```

Notes:

- APNs are configured in system authentication contexts or destination context.
- The authentication process varies depending on whether the PDP context is of type IP or PPP. The **authentication** command provides **imsi-auth**, **msisdn-auth**, **eap initial-acess-request**, **allow-noauth**, **chap**, **mschap**, and **pap** options. For more information on type of authentication, refer authentication section in APN Configuration Mode Commands chapter of Command Line Interface Reference.

GTPP Group Association to APN

After configuring GTPP group at context-level, an APN within the same context can be configured to use the user defined GTPP group.

Refer section *GTPP Accounting Support Configuration* for GTPP group configuration.

```
configure
        context <vpn_ctxt_name>
           apn <apn_name>
              gtpp group <gtpp_group_name> [accounting-context <aaa_ctxt_name>]
              end
```

Notes:

- GTPP group must be configured before associating with APN or "default" GTPP group can be used.

IP Address Allocation Method Configuration in APN

Use the following example to configure the IP address allocation method for APN:

Important Additional charging characteristics parameters are configurable as part of the GGSN service. Refer to the *GGSN Service Configuration* section of this chapter for more information.

```
configure
        context <dst_ctxt_name>
           apn <apn_name>
              ip address alloc-method { dhcp-proxy [allow-deferred]
[prefer-dhcp-options] | dhcp-relay | local [allow-deferred] | no-dynamic
 [allow-deferred] } [allow-user-specified]
              end
```

Notes:

- The process used by the system to determine how the address should be allocated. For detail information on IP address allocation, refer Usage section of **ip address alloc-method** command in *APN Configuration Mode Commands* chapter of Command Line Interface Reference.
- If DHCP-Proxy and DHCP-Relay method is selected for IP address allocation, a DHCP service must be configured on the system as described in *DHCP Service Configuration* section and specified the name of DHCP Service by entering the **dhcp service-name** command as described in APN Configuration Mode Commands chapter of Command Line Interface Reference.
- If local pool is selected for IP address allocation, a local pool must be configured on the system as described in *IP Address Pool Configuration on the System* section and specified the name of a private IP address pool by entering the **ip address pool** command as described in APN Configuration Mode Commands chapter of Command Line Interface Reference.

Charging Characteristics Parameter Configuration in APN

Use the following example to configure the charging characteristics parameter for APN:

Important Additional charging characteristics parameters are configurable as part of the GGSN service. Refer to the *GGSN Service Configuration* section of this chapter for more information.

```
configure
       context <dst_ctxt_name>
          apn <apn_name>
           cc-sgsn {home-subscriber-use-GGSN | roaming-subscriber-use-GGSN
 | visiting-subscriber-use-GGSN}+
             cc-home behavior <bit> profile <index>
             cc-roaming behavior <bit> profile <index>
             cc-visiting behavior <bit> profile <index>
          end
```

Notes:

- If multiple behavior bits are configured for a single profile index, the variable bits is achieved by "Or"ing the bit strings and converting the result to hexadecimal.

Example

If behavior bits 5 (0000 0001 0000) and 11 (0100 0000 0000) are both being assigned to profile index 5 for a home subscriber, the appropriate command is **cc-home behavior** *410* **profile** *5*.

Virtual APN Configuration

Virtual APNs are references (or links) to alternative APNs to be used for PDP context processing based on properties of the context. Use the following example to configure the virtual APNs.

```
configure
        context <dst_ctxt_name>
           apn <apn_name>
virtual-apn preference priority apn apn_name [ access-gw-address { ip_address
| ip_address/mask } | bearer-access-service service_name | cc-profile
cc_profile_index [ pre-rel-9.1-cc-behavior cc_behavior_value ][ rat-type { eutran
 | gan | geran | hspa | utran | wlan } ] | cc-behavior cc_behavior_value [
rat-type { eutran | gan | geran | hspa | utran | wlan } ] | domain
domain_name | mcc mcc_number mnc mnc_number [ cc-profile cc_profile_index [
pre-rel-9.1-cc-behavior cc_behavior_value ] | cc-behavior cc_behavior_value | [
 msin-range from msin_range_from to msin_range_to ] | [ rat-type { eutran | gan
 | geran | hspa | utran | wlan } ] | msisdn-range from msisdn_start_range to
 msisdn_to_range [ rat-type { eutran | gan | geran | hspa | utran | wlan }
} | pdp-type { ipv4 | ipv6 | ipv4v6 } | roaming-mode { roaming } ] }|
rat-type { eutran | gan | geran | hspa | utran | wlan } | roaming-mode {
 home | roaming | visiting } ] }
            end
```

Notes:

- Up to 1023 references can be configured per APN. Additional information about "virtual" APNs and their operation can be found in the *Command Line Interface Reference*.

Other Optional Parameter Configuration in APN

Use the following example to configure various optional parameter for APN:

```
configure
        context <dst_ctxt_name>
           apn <apn_name>
              dns {primary | secondary} {<dns_ip_address>}
              mobile-ip required
              mobile-ip home-agent <ha_ip_address>
              ip source-violation {ignore | check [drop-limit <limit>]}
[exclude-from-accounting]
              restriction-value <value>
              timeout {absolute | idle | qos-renegotiate} <timeout_dur>
              timeout long-duration <ldt_dur> [inactivity-time <inact_dur>]
              long-duration-action detection
              long-duration-action disconnection [suppress-notification]
[dormant-only] +
              end
```

Notes:

- Mobile is supported for IP PDP contexts only. Mobile IP configuration attributes returned as part of a successful authentication during the GTP authentication phase (for non-transparent IP PDP contexts) supersede the APN configuration. Any attributes returned during the FA authentication phase are ignored.
- If mobile-ip required option is enabled, the system deletes any PDP context using the APN that can not establish a Mobile IP session.

APN Configuration Verification

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

show apn all

This command produces an output similar to that displayed below is an excerpt from a sample output. In this example, an APN called *apn1* was configured.

```
access point name (APN):      apn1
authentication context:          test
pdp type:    ipv4
ehrpd access:    N/A
Selection Mode:    subscribed
ip source violation:    Checked                          drop limit:    10
accounting mode: gtpp                                        No early PDUs: Disabled
no-interims:    Disabled
Bearer Control Mode:    none
max-primary-pdp-contexts:    1000000                 total-pdp-contexts:    1000000
current primary-pdp-contexts:    0                     total-pdp-contexts:    0
primary contexts:    not available                     total contexts: not available
max secondary contexts per-subscriber:    10    IMS Authorization:    disabled
Credit Control:      disabled
mbms bearer absolute timeout:    0                    mbms bearer idle timeout:    0
mbms ue absolute timeout:    0
permission:
local ip:    0.0.0.0                                            nexthop gateway addr:
primary dns:    0.0.0.0                                       secondary dns:    0.0.0.0
primary nbns:    0.0.0.0                                    secondary nbns:    0.0.0.0
ppp keep alive period :    0                               ppp mtu :    1500
absolute timeout :    0                                       idle timeout :    0
idle-timeout-activity ignore-downlink:        Disabled
long duration timeout:    0                                 long dur inactivity time:    Disabled
long duration action:      Detection
wimax header compression/suppression:      none
ip header compression:    vj
ip hide service address:    Disabled
ip output access-group:                                   ip input access-group:
ipv6 output access-group:                                ipv6 input access-group:
policy-group in:                                                 policy-group out:
permit ip multicast:    False
ppp authentication:
eap authentication initial-access-request:    authenticate-authorize
allow noauthentication:    Enabled                imsi authentication: Disabled
msisdn authentication:    Disabled
ip destination context:    ip-ctx
Rule Base:    default
FW-and-NAT Policy:    default
Bandwidth-Policy:    default
Link-Monitoring:    OFF
Content-Filtering Policy-Id:    Not configured
mediation accounting:    Disabled
mediation-device context:    Not set                mediation no early PDUs:    Disabled
mediation no-interims:    Disabled                    mediation delay-GTP-response: Disabled
outbound username:    N/A
ip address pools:    N/A
ip address secondary pools:    N/A
access-link ip-frag:    df-ignore
ignore DF-bit data-tunnel:    On
ip allocation type:    local pool                      allow user specified ip addr: true
prefer dhcp options:    false
allow deferred:    true
```

```
3GPP Qos to DSCP Mapping:
        qci 1:              ef
        qci 2:              ef
        qci 3:              af11
        qci 4:              af11
        qci 5:              ef
        qci 6:              ef
        qci 7:              af21
        qci 8:              af21
        qci 9:              be
3GPP Qos to DSCP Mapping based on Alloc. Prio:
        qci 5 (Alloc. P 1):    ef
        qci 5 (Alloc. P 2):    ef
        qci 5 (Alloc. P 3):    ef
        qci 6 (Alloc. P 1):    ef
        qci 6 (Alloc. P 2):    ef
        qci 6 (Alloc. P 3):    ef
        qci 7 (Alloc. P 1):    af21
        qci 7 (Alloc. P 2):    af21
        qci 7 (Alloc. P 3):    af21
        qci 8 (Alloc. P 1):    af21
        qci 8 (Alloc. P 2):    af21
        qci 8 (Alloc. P 3):  af21
GTPP Group:    gtpp-gp               GTPP Accounting Context:    acc
Mobile IPv6 Tunnel MTU:    1500
Mobile IPv6 Tunnel MTU Exceed Action:    notify-sender
Mobile IPv6 Home Agent:    none
Mobile IPv6 Home Link Prefix:    ::/0
Mobile IPv6 Home Address:    none
```

Step 2 Verify configuration for errors in APN configuration by entering the following command in Exec Mode:

`show configuration errors section ggsn-service verbose`

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 one of two methods 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.

- **DHCP-relay**: The system acts as a relay for client (MS) and forwards the DHCP Discovery Request received from 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.

Regardless of the DHCP method, 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 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 GGSN service as described in *GGSN Service Configuration* section of this chapter.

To configure the DHCP service:

Step 1 Create the DHCP service in system context and bind it by applying the example configuration in the *DHCP Service Creation* section.

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* section.

Step 3 Verify your DHCP Service configuration by following the steps in the *DHCP Service Configuration Verification* section.

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

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

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.

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

To configure the DHCPv6 service:

Step 1 Create the DHCPv6 service in system context and bind it by applying the example configuration in the *DHCPv6 Service Creation* section.

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* section.

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* section.

Step 4 Configure the DHCPv6 profile by applying the example configuration in the *DHCPv6 Profile Configuration* section.

Step 5 Associate the DHCPv6 profile configuration with the APN by applying the example configuration in the *Associate DHCPv6 Configuration* section.

Step 6 Verify your DHCPv6 Service configuration by following the steps in the *DHCPv6 Service Configuration Verification* section.

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.

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:

- DHCPv 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 allows to create a server profile and then enter 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 should the configuration options 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 integer between 0 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.
- **dhcp-client-profile** command allows to create a client profile and then enter the DHCP Client Profile configuration mode.

- **dhcpv6-client-unicast** command Enables client to send messages on unicast address towards the server.
- **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 DHCPv6.
- **enable dhcp-message-spray** command enables dhcp-client to spray a dhcp messages 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>
                dhcpv6 context-name <dest_ctxt>
                 exit
```

Notes:

- **dhcpv6 ip-address-pool-name** command is optional. In case pool name is not specified, it searches across all the configured static pools.

DHCPv6 Service Configuration Verification

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 DHCPv6service 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*

DNS Configuration for IPv4v6 PDP Context

The system can be configured to provide DNS support for IPv4v6 PDP context.

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

To configure the DNS supprot for IPv4v6 PDP contexte:

Step 1 Configure the list of domain name servers with IPv4/IPv6 address in context configuration mode by applying the example configuration in the *Creating IPv4 and IPv6 DNS List* section.

Step 2 Configure the IPv4 primary and secondray domain name server in APN configuration mode by applying the example configuration in the *Configuring IPv4 DNS* section.

Step 3 Configure the IPv6 primary and secondray domain name server in APN configuration mode by applying the example configuration in the *Configuring IPv6 DNS* section.

Step 4 Verify your DNS configuration by following the steps in the *APN Configuration Verification*.

Step 5 Save your configuration as described in the *Verifying and Saving Your Configuration*.

Creating IPv4/IPv6 DNS List

Use the following example to create the domain name server list in context configuation mode:

```
configure
        context <src_ctxt_name>
           ip name-server <ip_address secondary_ip_address>
           end
```

Notes:

- <*ip_address*> is primary IP address of the domain name server having IPv4/IPv6 address.
- <*secondary_ip_address*> is the secondary IP address of the domain name server having IPv4/IPv6 address.

- Multiple DNS can be configured by entering **ip name-server** command multiple times.

Configuring IPv4 DNS

Use the following example to configure the IPv4 DNS support in IPv4v6 PDP context:

```
configure
        context <src_ctxt_name>
           apn <apn_name>
              dns primary <ipv4_address>
              dns secondary <ipv4_address>
              end
```

Notes:

- <*ipv4_address*> is the IP address of the domain name server configured as DNS list in context configuration mode.

Configuring IPv6 DNS

Use the following example to configure the IPv6 DNS support in IPv4v6 PDP context:

```
configure
        context <src_ctxt_name>
           apn <apn_name>
              ipv6 dns primary <ipv6_address>
              ipv6 dns secondary <ipv6_address>
              end
```

Notes:

- <*ipv6_address*> is the IP address of the domain name server configured as DNS list in context configuration mode.

IP Address Pool Configuration on the System

Before an MS is able to access data services, they must have an IP address. As described previously, the GGSN supports static or dynamic addressing (through locally configured address pools on the system, DHCP client-mode, or DHCP relay-mode). Regardless of the allocation method, a corresponding address pool must be configured.

IP addresses can be dynamically assigned from a single pool/a group of IP pools/a group of IP pool groups. The addresses/IP pools/ IP pool groups are placed into a queue in each pool or pool group. An address is assigned from the head of the queue and, when released, returned to the end. This method is known as least recently used (LRU).

On initiation of a session, a request of IP address from IP pool is sent and system assigns an IP address out of "available" IP address(es) in the pool. This assigned IP address is set to "allocated" state and cannot be used for any other session during this state. As soon as the session is cleared the state of "allocated" IP address is changed to "released" and is ready for allocation to any other subscriber session. If a "hold" timer is set for assigned/released IP address(es), it will go into the "hold" state and remain there till the timer expires. As

soon as "hold timer" expires its state is changed from "hold" to "released" state and it will be available for reallocation. The "available" IPs include "free" and "released" IP addresses.

Free IPs are used first depending on which subscriber is connecting. Normally same IP is given to a subscriber. So if a subscriber is connecting again, instead of using a free IP, GGSN allocates the IP which was given to him previously. This IP will be from the released state. For GGSN, Username and IMSI are used as key for generating subscriber ID used by VPN while allocating IP from the IP pool. Therefore if the subscriber ID matches to any of the previous ones for IPs in released state, that IP is re-allocated to that subscriber, otherwise a new IP is allocated.

When a group of pools have the same priority, an algorithm is used to determine a probability for each pool based on the number of available addresses, then a pool is chosen based on the probability. This method, over time, allocates addresses evenly from the group of pools.

Important Setting different priorities on each individual pool can cause addresses in some pools to be used more frequently.

Important This section provides the minimum instruction set for configuring local IP address pools on the system. For more information on commands that configure additional parameters and options, refer ip pool command section in *Context Configuration Mode Commands* chapter of *Command Line Interface Reference*.

Caution From 14.0 onward for configuration of multiple IP pool in an APN, GGSN expects Framed-IP-Address and Framed-Pool from RADIUS.

Caution In pre-release 14.0, the maximum number of IP pools in an APN is 16 for static and dynamic type of pool. From 14.0 onward this limit has been changed for static address allocation to 1 and out of the maximum 16 pools which can be configured under a particular APN, the first IP pool should be a static pool, which is the only working static pool from an APN.

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

To configure the IP pool:

Step 1 Create the IP pool for IPv4 addresses in system context by applying the example configuration in the *IPv4 Pool Creation* section.

Step 2 Optional. Configure the IP pool for IPv6 addresses in system context by applying the example configuration in the *IPv6 Pool Creation* section.

Step 3 Verify your IP pool configuration by following the steps in the *IP Pool Configuration Verification* section.

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

IPv4 Pool Creation

Use the following example to create the IPv4 address pool:

```
configure
        context <dest_ctxt_name>
           ip pool <pool_name> <ip_address/mask> [{private| public}[priority]]
| static]
           end
```

Notes:

- To ensure proper operation, IP pools should be configured within a destination context.
- Each address in the pool requires approximately 24 bytes of memory. Therefore, in order to conserve available memory, the number of pools may need to be limited depending on the number of addresses to be configured and the number of PACs/PSCs installed.
- Setting different priorities on individual pools can cause addresses in some pools to be used more frequently.
- For more information on commands/keywords that configure additional parameters and options, refer ipv6 pool command section in Context Configuration Mode Commands chapter of Command Line Interface Reference.

IPv6 Pool Creation

Use the following example to create the IPv6 address pool:

```
configure
        context <dest_ctxt_name>
           ipv6 pool <pool_name> 6to4 local-endpoint
<ip_address>[private][public][shared][static]
           end
```

Notes:

- To ensure proper operation, IP pools should be configured within a destination context.
- Each address in the pool requires approximately 24 bytes of memory. Therefore, in order to conserve available memory, the number of pools may need to be limited depending on the number of addresses to be configured and the number of PACs/PSCs installed.
- Setting different priorities on individual pools can cause addresses in some pools to be used more frequently.
- For more information on commands/keywords that configure additional parameters and options, refer ipv6 pool command section in Context Configuration Mode Commands chapter of Command Line Interface Reference.

IP Pool Configuration Verification

Step 1 Verify that your IPv4 address pool configured properly by entering the following command in Exec Mode:

show ip pool

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

```
context : isp1:
+-----Type:         (P) - Public         (R) - Private
|                           (S) - Static         (E) - Resource
|
|+----State:       (G) - Good             (D) - Pending Delete              (R)-Resizing
||
||++--Priority: 0..10 (Highest (0) .. Lowest (10))
||||
||||+-Busyout: (B) - Busyout configured
|||||
|||||
vvvvv  Pool Name    Start Address        Mask/End Address        Used          Avail
-----  ---------- --------------- ------------------    -------- --------
PG00    ipsec            12.12.12.0              255.255.255.0               0               254
RG00    pool3            30.30.0.0                255.255.0.0                   0
65534
SG00    pool2            20.20.0.0                255.255.0.0                   10
65524
PG00    pool1            10.10.0.0                255.255.0.0                   0
65534
SG00    vpnpool        192.168.1.250        192.168.1.254               0               5
Total Pool Count: 5
```

Step 2 Verify that your IPv6 address pools configured properly by entering the following command in Exec Mode:

show ipv6 pools

The output from this command should look similar to the sample shown above except IPv6 addresses.

Gn-Gp Handoff Support Configuration

This section describes all about the configurations that are required to enable the handoff between the 3GPP 2G/3G SGSN and P-GW over Gn-Gp interfaces.

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*, GGSN service as described in *GGSN Service Configuration* section in this chapter.

To configure the Gn-Gp handoff on GGSN node:

Step 1 Create and configure the GTP-U service by applying the example configuration in the *GTP-U Service Configuration* section.

Step 2 Modify GGSN service to facilitate the handoff between SGSN/GGSN and P-GW by applying the example configuration in the *Modifying GGSN Configuration for Gn-Gp Handoff* section.

Step 3 Modify APN configuration to the "subscribed" selection mode by applying the example configuration in *APN Configuration for Gn-Gp Handoff* section.

Step 4 Verify your handoff configuration by following the steps in the *Gn-Gp Configuration Verification* section.

Step 5 Save your configuration as described in the *Verifying and Saving Your Configuration* chapter.

GTP-U Service Configuration

Use the following example to configure the GTP-U service:

```
configure
    context <ctxt_name> -noconfirm
        gtpu-service <gtpu_svc_name>
            bind ipv4-address <ip_address>
            echo-interval <time_interval>
            end
```

Notes:

- <*ctxt_name*> is name of the context which contains GTPU service on system.
- <*time_interval*> is the time interval in seconds at which GPRS Tunneling Protocol (GTP) v1-U Echo packets are sent.
- <*ip_address*> is the IP address of IPv4 or IPv6 type to which the GTP-U service will be binded.

Modifying GGSN Configuration for Gn-Gp Handoff

Use the following example to create/modify the GGSN config for this feature.

```
configure
    context <ctxt_name>
        ggsn-service <ggsn_svc_name>

            associate gtpu-service <gtpu_svc_name>
            associate pgw-service <pgw_svc_name>
            bind address <ip_address>
            end
```

Notes:

- <*ggsn_svc_name*> is name of the existing GGSN service.
- <*gtpu_svc_name*> is name of the existing GTP-U service created in *GTP-U Service Configuration* example.
- <*pgw_svc_name*> is the existing P-GW service name.
- <*ip_address*> is the same IP address to which GTP-U service is binded in *GTP-U Service Configuration* example.
- <*ctxt_name*> is the name of the context which contains the GGSN service.

APN Configuration for Gn-Gp Handoff

Use the following example to modify the APN configuration for the smooth handover support between SGSN/GGSN and P-GW:

```
configure
   context <ctxt_name>
      apn <apn_name>
         selection-mode subscribed
         ip context-name <ctxt_name>
         pdp-type <ipv4 | ipv6>
         end
```

Notes:

- Make sure that the APN Selection mode parameters setting is set to "subscribed", which is also the default mode.

Gn-Gp Configuration Verification

Verify that all the configurations made in a specific context under Context Configuration mode are in place and the P-GW service and GTP-U services have been associated to the GGSN service by entering the following command in Exec mode:

show ggsn-service name *ggsn*

The output from this command should look similar to the sample shown below. In this example context name *A* was created in Exec mode, GGSN service *ggsn* was created in GGSN Service Configuration mode, PGW service named *pgw* was an already configured service and GTP-U service named *gtpu* was configured in the GTPU Service Configuration mode:

```
Service name:                      ggsn
context:                                A
Associated PGW svc:          pgw
Associated GTPU svc:        gtpu
                           .
                           .
Bind:                                   Done
Local IP Address:              120.56.45.12            Local IP Port:          2123
                           ...
                           ...
Echo Interval:                    60 (secs)
                           .
                           .
                           .
```

FA Services Configuration

FA services are configured within contexts and allow the system to function as an FA in the 3G wireless data network.

Important This section provides the minimum instruction set for configuring an FA service that allows the system to process data sessions. Commands that configure additional FA service properties are provided in the Command Line Interface Reference. Additionally, when configuring Mobile IP take into account the MIP timing considerations discussed in *Mobile-IP and Proxy-MIP Timer Considerations*.

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

To configure the FA service:

Step 1 Create the FA service in the system context created to facilitate FA service by applying the example configuration in the *FA Service Creation* section.

Step 2 Bind the configured FA service to a local IP address interface with UDP port and specify the maximum number of subscribers that can access this service for the Pi interfaces' IP socket by applying the example configuration in the *IP Interface and UDP Port Binding for Pi Interface* section.

Step 3 Configure the security parameter index (SPI) between FA service and HA by applying the example configuration in the *Security Parameter Index (SPI) Configuration* section.

Step 4 Specify the FA agent advertisement related parameters like lifetime, number of advertisements, and registration lifetime by applying the example configuration in the *FA Agent Advertisement Parameter Configuration* section.

Step 5 Configure the number of registration per subscriber, authentication procedure, and registration timeout parameters for this FA service by applying the example configuration in the *Subscriber Registration, Authentication and Timeout Parameter Configuration* section.

Step 6 Optional. Configure the FA service for controlling the negotiation and sending of the I-bit in revocation messages by applying the example configuration in the *Revocation Message Configuration* section.

Step 7 Verify your FA service configuration by following the steps in the *FA Service Configuration Verification* section.

Step 8 Save your configuration as described in the *Verifying and Saving Your Configuration* chapter.

FA Service Creation

Use the following example to create the FA service:

Important A maximum of 256 services (regardless of type) can be configured per system.

```
configure
        context <fa_ctxt_name> -noconfirm
          fa-service <fa_svc_name> -noconfirm]
             end
```

Notes:

- *<fa_ctxt_name>* is name of the context to use for FA service configuraiton. Generally FA should be configured within a destination context.

- *<fa_svc_name>* is name of the FA service where other parameters have to configure for FA functionality.

IP Interface and UDP Port Binding for Pi Interface

Use the following example to bind the FA service to an local IP interface and specify the maximum number of subscribers that can access this service. Binding an interface to the FA service causes the interface to take on the characteristics of a Pi interface.

```
configure
        context <fa_ctxt_name>
           fa-service <fa_svc_name>
              bind address <fa_ip_address> max-subscribers <max_subs>
              ip local-port <udp_port_num>
              end
```

Notes:

- *<fa_svc_name>* is name of the FA service which is created to configure FA functionality.
- *<fa_ip_address>* is the local IP address in IPv4/IPv6 notation for providing Pi interface characteristics.
- *<max_subs>* is the maximum number of subscribers that can access this service on this interface. This can be configured to any integer value from 0 to 500,000. The default is 500,000.

Important The maximum number of subscribers supported is dependant on the session capacity license installed and the number of active PACs/PSCs installed in the system. For more information on session capacity license, refer to the Software Management Operations chapter of the System Administration Guide.

- *<udp_port_num>* is the UDP port number from 1 through 65535 to be used for Pi interface. Default port number is 434.
- For more information on commands/keywords that configure additional parameters and options, refer *FA Service Configuration Mode Commands* chapter of *Command Line Interface Reference*.

Security Parameter Index (SPI) Configuration

Use the following example to configure the security parameter index (SPI) between FA service and HA:

Important A maximum of 2048 FA-HA SPIs can be configured for a single FA service.

```
configure
        context <fa_ctxt_name>
           fa-service <fa_svc_name>
              fa-ha-spi remote-address <ha_ip_address> spi-number <spi_num>
{encrypted secret <enc_secret_key> | secret <secret_key>}     [description
<desc_string>]
              end
```

Notes:

- <*fa_svc_name*> is name of the FA service which is created to configure FA functionality.
- <*ha_ip_address*> is the IP address in IPv4/IPv6 notation of HA to which this FA service will interact.
- <*spi_num*> specifies the SPI number which indicates a security context between the FA and the HA in accordance with RFC 2002 and can be configured to any integer value from 256 through 4294967295.
- <*enc_secret_key*> specifies the encrypted shared key between the FA and the HA services. It must be from 1 to 127 alpha and/or numeric characters and is case sensitive.

Important The encrypted keyword is intended only for use by the system while saving configuration scripts. The system displays the encrypted keyword in the configuration file as a flag that the variable following the **secret** keyword is the encrypted version of the plain text secret. Only the encrypted secret is saved as part of the configuration file.

- <*secret_key*> specifies the secret shared key between the FA and the HA services. It must be from 1 to 127 alpha and/or numeric characters and is case sensitive.
- <*desc_string*> is the description for this SPI and must be from 1 to 31 alpha and/or numeric characters.
- For more information on commands/keywords that configure additional parameters and options, refer FA Service Configuration Mode Commands chapter of Command Line Interface Reference.

FA Agent Advertisement Parameter Configuration

Use the following example to configure the agent advertisement parameters for this FA service:

```
configure
        context <fa_ctxt_name>
           fa-service <fa_svc_name>
              advertise adv-lifetime <advt_dur>
              advertise num-adv-sent <advt_num>
              advertise reg-lifetime <reg_dur>
              end
```

Notes:

- <*fa_svc_name*> is name of the FA service which is created to configure FA functionality.
- <*advt_dur*> is the amount of time that an FA agent advertisement remains valid in the absence of further advertisements. It is measured in seconds and can be configured to any integer value from 1 to 65535. The default is 9000.
- <*advt_num*> is the number of unanswered agent advertisements that the FA service allows during call setup before it rejects the session. It can be any integer value from 1 to 65535. The default is 3.
- <*reg_dur*> specify the longest registration lifetime that the FA service allows in any Registration Request message from the mobile node. It is measured in seconds and can be configured to any integer value from 1 to 65534. The default is 600.

Subscriber Registration, Authentication and Timeout Parameter Configuration

Use the following example to configure the number of subscriber registration, authentication procedure and registration timeout parameters for this FA service:

```
configure
        context <fa_ctxt_name>
           fa-service <fa_svc_name>
              multiple-reg <reg_num>
              reg-timeout <timeout_dur>
             authentication mn-aaa {always | ignore-after-handoff | init-reg
 | init-reg-except-handoff | renew-and-dereg-noauth | renew-reg-noauth}
[optimize-retries]
              end
```

Notes:

- *<fa_svc_name>* is name of the FA service which is created to configure FA functionality.
- *<reg_num>* is the number of simultaneous Mobile IP sessions that are to be supported for a single subscriber. It can be configured to any integer value from 1 to 3. The default value is 1.

Important The system supports multiple Mobile IP sessions per subscriber only if the subscriber's mobile node has a static IP address. The system only allows a single Mobile IP session for mobile nodes that receive a dynamically assigned home IP address.

Important In addition, because only a single Mobile IP or proxy-Mobile IP session is supported for IP PDP contexts, this parameter must remain at its default configuration.

- *<timeout_dur>* is the maximum amount of time that the FA service waits for a Registration Rely message from the HA. It is measured in seconds and can be configured to any integer value from 1 to 65535. The default value is 45.
- For more information on authentication mn-aaa commands/keywords that configure additional parameters and options, refer FA Service Configuration Mode Commands chapter of Command Line Interface Reference.

Revocation Message Configuration

Use the following example to configure the FA service for controlling the negotiation and sending of the I-bit in revocation messages:

```
configure
        context <fa_ctxt_name>
           fa-service <fa_svc_name>
              revocation negotiate-i-bit
              end
```

Notes:

- By default the system will not send the I-bit in the revocation message.

FA Service Configuration Verification

Step 1 Verify that your FA service is configured properly by entering the following command in Exec Mode:

show fa-service all

The output from this command should look similar to the sample shown below. In this example an FA service named fa1 was configured in the isp1 context.

```
Service name:              fa1
      Context:                   isp1
      Bind:                          Done                                Max Subscribers:
  500000
      Local IP Address: 195.20.20.3                 Local IP Port                  434
      Lifetime:                  00h10m00s                    Registration Timeout: 45 (secs)
     Advt Lifetime          02h30m00s                     Advt Interval:               5000 (msecs)

      Num Advt:                  5
      Advt Prefix Length Extn: NO
      Reverse Tunnel:        Enabled                        GRE Encapsulation:          Enabled
SPI(s):
    FAHA: Remote Addr: 195.30.30.3/32
      Hash Algorithm:        HMAC_MD5                     SPI Num:    1000
      Replay Protection: Timestamp                    Timestamp Tolerance: 60
IPSEC Crypto Map(s):
      Peer HA Addr:                    195.30.30.2
            Crypto Map:                  test
      Registration Revocation:        Enabled      Reg-Revocation I bit:      Enabled
      Reg-Revocation Max Retries:  3                  Reg-Revocation Timeout: 3 (secs)
      Reg-Rev on InternalFailure: Enabled
```

Step 2 Verify configuration for errors in FA service by entering the following command in Exec Mode:

show configuration errors section fa-service verbose

Common Gateway Access Support Configuration

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, PGW, 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 GGSN service as described in *GGSN Service Configuration* section in this chapter.

To configure the S6b and other advance features:

Step 1 Configure Diameter endpoint by applying the example configuration in the *Diameter Endpoint Configuration* section.

Step 2 Create or modify AAA group by applying the example configuration in the *AAA Group Configuration* section.

Step 3 Modify GGSN service to allow authorization with HSS by applying the example configuration in the *Authorization over S6b Configuration* section.

Step 4 *Optional*. Create and associate DNS client parameters by applying the example configuration in the *DNS Client Configuration* section.

Step 5 *Optional*. Modify GGSN service to accept duplicate calls when received with same IP address by applying the example configuration in the *Duplicate Call Accept Configuration* section.

Step 6 Verify your S6b configuration by following the steps in the *Common Gateway Access Support Configuration Verification* section.

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

Diameter End-Point Configuration

Use the following example to define the diameter accounting end-point and associate a diameter accounting dictionary for this feature:

```
configure
   context <ctxt_name>
      diameter endpoint <endpoint_name>
         origin host <diameter_host_name> address <ip_address>
         peer <peer_name> realm <peer_realm_name>
address <ip_address>
port <port_number>
         end
```

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 Diamtere endpoint.

Authorization over S6b Configuration

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

```
configure
   context <ggsn_ctxt_name>
      ggsn-service <ggsn_svc_name>
         plmn-unlisted-sgsn home
         authorize-with-hss
         fqdn host <host_name> realm <realm_name>
         end
```

Notes:

- <*ggsn_svc_name*> is name of the GGSN service which is already created on the system.

DNS Client Configuration

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

```
configure
   context <ggsn_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
      ggsn-service <ggsn_svc_name>
           default dns-client context
           end
```

Notes:

- <*ggsn_svc_name*> is name of the GGSN service which is already created on the system.

Duplicate Call Accept Configuration

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

```
configure
   context <ggsn_ctxt_name>
      ggsn-service <ggsn_svc_name>
         newcall duplicate-subscriber-requested-address accept
         end
```

Notes:

- <*ggsn_svc_name*> is name of the GGSN service which is already created on the system.

Common Gateway Access Support Configuration Verification

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

show ggsn-service all

The output from this command should look similar to the sample shown below. In this example GGSN service named *GGSN1* was configured in the *vpn1* context.

```
Service name:                    ggsn1
Context:                            cn1
Associated PGW svc:           None
Associated GTPU svc:         None
Accounting Context Name:cn1
dns-client Context Name:cn1
Authorize:                          hss
Fqdn-name:                          xyz.abcstarent.networks.com
Bind:                                  Not Done
Local IP Address:             0.0.0.0                    Local IP Port:                    2123
Self PLMN:                          Not defined
Retransmission Timeout: 5 (secs)
```

Rf Interface Configuration for Offline Charging

This section describes the step-by-step procedure for the configurations that are required to setup the Rf interface on GGSN to support offline charging.

These instructions assume that you have already configured the system level configuration as described in *System Administration Guide*, GGSN service as described in *GGSN Service Configuration* section in this chapter.

To configure the Rf interface on GGSN node:

Step 1 Create and configure the accounting policy by applying the example configuration in the *Accounting Policy Configuration* section.

Step 2 Configure a AAA group to associate the diameter accounting dictionary with the by applying the example configuration in the *AAA Group Configuration* section.

Step 3 Configuring an APN to associate the accounting policy by applying the example configuration in *APN Configuration for Rf Interface* section.

Step 4 Verify your Rf interface configuration by following the steps in the *Rf Interface Configuration Verification*

Step 5 Save your configuration as described in the *Verifying and Saving Your Configuration* chapter.

Accounting Policy Configuration

Use the following example to configure the accounting policy for this feature:

```
configure
   context <ctxt_name>
      policy accounting <policy_name>
         operator-string <ip_address>
         accounting-level [ sdf | flow ]
         cc profile [ 2 | 4 | 6 | 8 ] [ buckets | interval | sdf-interval
| sdf-volume | serving nodes | tariff | volume ]
         end
```

Diameter End-Point Configuration

Use the following example to define the diameter accounting end-point and associate a diameter accounting dictionary for this feature:

```
configure
   context <ctxt_name>
      diameter endpoint <endpoint_name>
         origin host <diameter_host_name> address <ip_address>
         peer <peer_name> realm <peer_realm_name>
address <ip_address>
port <port_number>
         end
```

AAA Group Configuration

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

```
configure
   context <ctxt_name>
      aaa group <group_name>
         diameter accounting endpoint <endpoint_name>
         diameter accounting dictionary [ aaa-custom1 | aaa-custom10 |
aaa-custom2 | aaa-custom3 | aaa-custom4 | aaa-custom5 | aaa-custom6 |
aaa-custom7 | aaa-custom8 | aaa-custom9 ]
         diameter accounting server <diameter_hostname> priority <number>
         end
```

APN Configuration for Rf Interface

Use the following example create/modify the APN configuration for this feature:

```
configure
   context <ctxt_name>
      apn <apn_name>
         associate accounting-policy <policy_name>
         end
```

Rf Interface Configuration Verification

Verify that your Rf interface configuration for offline charging support is configured properly by entering the following command in Exec Mode:

show configuration context *ctxt_name*

The output from this command should look similar to the sample shown below. In this example accounting policy named *test_policy* was configured in the *rf_context* context.

```
config
    context rf_context
        subscriber default
        exit
        apn apn
            associate accounting-policy test_policy
        exit
        aaa group default
        exit
        aaa group rf_aaa
            diameter accounting dictionary aaa-custom6
            diameter accounting endpoint rf_endpoint
            diameter accounting server rf_server priority 2
        exit
        gtpp group default
        exit
        policy accounting test_policy
            accounting-level flow
            operator-string Rf_string
            cc profile 2 buckets 5
        exit
        diameter endpoint rf_endpoint
            origin host rf_diameter address 1.2.3.4
            peer ak realm ak_realm address 2.3.4.5 port 52
        exit
        ip igmp profile default
        exit
    exit
end
```

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 ggsn msg-type { dpc | ipca
| nrupc | emergency-call | arp { 1 | 2 | 3 }+ | 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 GGSN 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 Delete PDP message type at the GGSN node to bypass throttling.

```
egress bypass-rlf ggsn msg-type dpc
```