Configuring the Evolved Packet Data Gateway

This chapter provides configuration instructions for the ePDG (evolved Packet Data Gateway).

Important Information about the commands in this chapter can be found in the *eHRPD/LTE 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.

The following section is included in this chapter:

Configuring the System to Perform as an Evolved Packet Data Gateway

This section provides a high-level series of steps and the associated configuration file examples for configuring the system to perform as an ePDG in a test environment. For a configuration example without instructions, see "Sample Evolved Packet Data Gateway Configuration File".

Information provided in this section includes the following:

Required Information

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

Required Local Context Configuration Information

Table 1: Required Information for Local Context Configuration

Required Information	Description
Management Interface Configuration	
Interface name(s)	The name(s) of the management interface(s), which can be from 1 to 79 alpha and/or numeric characters. Multiple names are needed if multiple interfaces will be configured.
IP address(es) and subnet mask(s)	The IPv4 address(es) and subnet mask(s) assigned to the interface(s). Multiple addresses and subnet masks are needed if multiple interfaces will be configured.
Remote access type(s)	The type(s) of remote access that will be used to access the system, such as ftpd, sshd, and/or telnetd.
Security administrator name(s)	The name(s) of the security administrator(s) with full rights to the system.
Security administrator password(s)	Open or encrypted passwords can be used.
Gateway IP address(es)	Used when configuring static IP routes from the management interface(s) to a specific network.
Physical Ethernet port number	The physical Ethernet port to which the interface(s) will be bound. Ports are identified by the chassis slot number where the line card resides, followed by the number of the physical connectors on the card. For example, port 24/1 identifies connector number 1 on the card in slot 24. A single physical port can facilitate multiple interfaces.

Required Information for ePDG Context and Service Configuration

Table 2: Required Information for ePDG Context and Service Configuration 0

Required Information	Description
ePDG Context Configuration	
ePDG context name	The name of the ePDG context, which can be from 1 to 79 alpha and/or numeric characters.
EAP profile name(s)	The name(s) of the EAP profile(s) to be used for UE authentication via the EAP authentication method.
IPSec transform set name(s)	The name(s) of the IPSec transform set(s) to be used by the ePDG service.

Required Information	Description
IKEv2 transform set name(s)	The name(s) of the IKEv2 transform set(s) to be used by the ePDG service.
Crypto template name(s)	The name(s) of the IKEv2 crypto template(s) to be used by the ePDG service.
Configuration for the SWu, SWm, and DNS Interfaces, and the SWu and SWm Loopback Interfaces	
SWu interface name	The name of the SWu interface, which can be from 1 to 79 alpha and/or numeric characters. This is the interface that carries the IPSec tunnels between the WLAN UEs and the ePDG.
SWm interface name	The name of the SWm interface, which can be from 1 to 79 alpha and/or numeric characters. This is the interface between the ePDG and the external 3GPP AAA server.
DNS interface name	The name of the DNS interface, which can be from 1 to 79 alpha and/or numeric characters. This is the interface between the ePDG and the external DNS.
SWu loopback interface name	The name of the SWu loopback interface, which can be from 1 to 79 alpha and/or numeric characters.
SWm loopback interface name	The name of the SWm loopback interface, which can be from 1 to 79 alpha and/or numeric characters.
IP addresses and subnet masks	The IP addresses assigned to the SWu (IPv4), SWm (either IPv4 or IPv6), and DNS interfaces (either IPv4 or IPv6), and to the SWu (IPv4) and SWm (either IPv4 or IPv6) loopback interfaces.
Physical Ethernet port numbers	The physical Ethernet ports to which the SWu, DNS, and SWm interfaces will be bound. Ports are identified by the chassis slot number where the line card resides, followed by the number of the physical connectors on the card. For example, port 19/1 identifies connector number 1 on the card in slot 19. A single physical port can facilitate multiple interfaces.
AAA Group Configuration	
Diameter authentication dictionary	The name of the Diameter dictionary used for authentication.
Diameter endpoint name	The name of the Diameter endpoint, which can be from 1 to 63 alpha and/or numeric characters. This is the name of the external 3GPP AAA server using the SWm interface.
ePDG Service Configuration	

Required Information	Description
ePDG service name	The name of the ePDG service, which can be from 1 to 63 alpha and/or numeric characters.
PLMN ID (Public Land Mobile Network Identifier)	The MCC (Mobile Country Code) and MNC (Mobile Network Code) for the ePDG.
Egress context name	The name of the Egress context, which can be from 1 to 79 alpha and/or numeric characters.
MAG service name	The name of the MAG (Mobile Access Gateway) service on the ePDG, which can be from 1 to 63 alpha and/or numeric characters.
EGTP service name	The name of the EGTP service associated with ePDG, which can be from 1 to 63 alpha and/or numeric characters.
ePDG FQDN	The ePDG FQDN (Fully Qualified Domain Name), used for longest suffix matching during P-GW dynamic allocation. The ePDG FQDN can be from 1 to 256 alpha and/or numeric characters.
Diameter endpoint name	The name of the Diameter endpoint, which can be from 1 to 63 alpha and/or numeric characters. This is the name of the external 3GPP AAA server using the SWm interface.
Origin host	The name of the Diameter origin host, which can be from 1 to 255 alpha and/or numeric characters.
Origin host address	The IPv6 address of the Diameter origin host.
Peer name	The name of the Diameter endpoint, which can be from 1 to 63 alpha and/or numeric characters. This is the name of the external 3GPP AAA server using the Swm interface.
Peer realm name	The name of the peer realm, which can be from 1 to 127 alpha and/or numeric 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.
Peer address	The IPv4 or IPv6 address of the Diameter endpoint.
DNS client name	The name of the DNS client on the ePDG, which can be from 1 to 63 alpha and/or numeric characters.
DNS address	The IPv4 or IPv6 address of the local DNS client.

Required Information for Egress Context and MAG Service Configuration

The following table lists the information that is required to configure the Egress context and MAG (Mobile Access Gateway) service on the ePDG.

Note ePDG can only be configured and associated either with MAG or EGTP and not both at a time.

Table 3: Required Information for Egress Context and MAG Service Configuration 1

Required Information	Description
Egress context name	The name of the Egress context, which can be from 1 to 79 alpha and/or numeric characters.
S2b Interface Configuration	
S2b interface name	The name of the S2b interface, which can be from 1 to 79 alpha and/or numeric characters. This is the interface that carries the PMIPv6 signaling between the MAG (Mobile Access Gateway) function on the ePDG and the LMA (Local Mobility Anchor) function on the P-GW.
MIPv6 address and subnet mask	The MIPv6 address and subnet mask assigned to the S2b interface.
S2b loopback interface name	The name of the S2b loopback interface, which can be from 1 to 79 alpha and/or numeric characters.
MIPv6 address and subnet mask	The MIPv6 address and subnet mask assigned to the S2b loopback interface.
Gateway IPv6 address	The gateway IP address for configuring the IPv6 route from the S2b interface to the P-GW.
MAG Service Configuration	
MAG service name	The name of the MAG (Mobile Access Gateway) service, which can be from 1 to 63 alpha and/or numeric characters.
Physical Ethernet port numbers	The physical Ethernet ports to which the SWu, DNS, SWm, and S2b interfaces will be bound. Ports are identified by the chassis slot number where the line card resides, followed by the number of the physical connectors on the card. For example, port 24/1 identifies connector number 1 on the card in slot 24. A single physical port can facilitate multiple interfaces.

Required Information for Egress Context and EGTP Service Configuration

The following table lists the information that is required to configure the Egress context and EGTP (Evolved GPRS Tunneling Protocol) service on the ePDG.

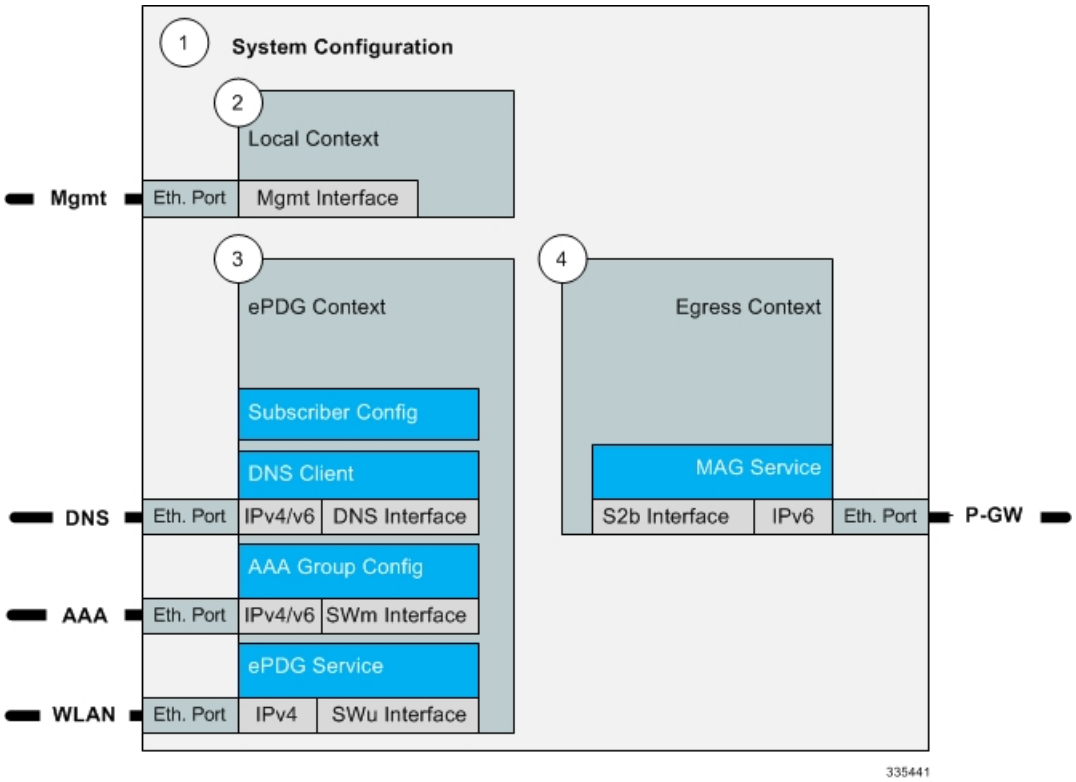
Note ePDG can only be configured and associated either with MAG or EGTP and not both at a time.

Table 4: Required Information for Egress Context and EGTP Service Configuration 2

Required Information	Description
Egress context name	The name of the Egress context, which can be from 1 to 79 alpha and/or numeric characters.
S2b Interface Configuration	
S2b interface name	The name of the S2b interface, which can be from 1 to 79 alpha and/or numeric characters. This is the interface that carries the GTPv2 Signaling and data messages between ePDG and PGW.
S2b loopback interface name	The name of the S2b loopback interface, which can be from 1 to 79 alpha and/or numeric characters.
Gateway IPv6 address	The gateway IP address for configuring from the S2b interface to the P-GW.
eGTP Service Configuration	
GTPU service name	Use GTPU service name to allow configuration of GTPU Service. Use the bind configuration to bind the s2b loopback address. This will be used for data plane of GTPv2.
egtp-service name	Use EGTP service name to allow configuration of eGTP service. Use the bind configuration to bind the s2b loopback address for gtpc and also use the association cli to associate the gtpu-service name.

Evolved Packet Data Gateway Configuration

The figure below shows the contexts in which ePDG configuration occurs. The steps that follow the figure explain the high-level ePDG configuration steps.



Step 1 Set system configuration parameters such as activating PSC2s, enabling Diameter Proxy mode, and enabling session recovery by following the configuration examples in the *System Administration Guide*.

Step 2 Set initial configuration parameters in the local context by following the configuration example in the section Initial Configuration, on page 7

Step 3 Configure the ePDG context, the EAP profile, the IPSec and IKEv2 transform sets, the crypto template, the SWu, SWm, and DNS interfaces, the SWu and SWm loopback interfaces, and the AAA group for Diameter authentication by following the configuration example in the section ePDG Context and Service Configuration, on page 8

Step 4 Configure the Egress context and MAG service or Egress context and EGTP by following the configuration example in the section Egress Context and MAG Service Configuration, on page 12 or Required Information for Egress Context and EGTP Service Configuration, on page 6

Step 5 Enable ePDG bulk statistics by following the configuration example in the section Bulk Statistics Configuration, on page 14

Step 6 Enable system logging activity by following the configuration example in the section Logging Configuration, on page 15

Step 7 Save the configuration file.

Initial Configuration

Set local system management parameters by following the configuration example in the section Modifying the Local Context, on page 8.

Modifying the Local Context

Use the following configuration example to create a management interface, configure remote access capability, and set the default subscriber in the local context:

```
configure
     context local
          interface <mgmt_interface_name>
               ip address <ip_address> <subnet_mask>
               exit
          server ftpd
          ssh key <data> length <octets>
          ssh key <data> length <octets>
          ssh key <data> length <octets>
          server sshd
               subsystem sftpd
               exit
          server telnetd
               exit
          subscriber default
               exit
          administrator <name> encrypted password <password> ftp
          aaa group default
             exit
          gttp group default
               exit
          ip route 0.0.0.0 0.0.0.0 <gateway_ip_addr> <mgmt_interface_name>
          exit
     port ethernet <slot_number/port_number>
          no shutdown
          bind interface <mgmt_interface_name> local
          exit
     end
```

The **server** command configures remote server access protocols for the current context. The system automatically creates a default subscriber, a default AAA group, and a default GTTP group whenever a context is created. The **ip route** command in this example creates a default route for the management interface.

ePDG Context and Service Configuration

Step 1 Create the context in which the ePDG service will reside by following the configuration example in the section Creating the ePDG Context, on page 8

Step 2 Create the ePDG service by following the configuration example in the section Creating the ePDG Service, on page 10

Creating the ePDG Context

Use the following configuration example to create the ePDG context, the EAP profile, the IPSec and IKEv2 transform sets, the crypto template, the SWu, SWm, and DNS interfaces, the SWm and IPSec loopback interfaces, and the AAA group for Diameter authentication:

```
configure
     context <epdg_context_name>
          eap-profile <eap_profile_name>
               mode authenticator-pass-through
               exit
          ipsec transform-set <ipsec_tset_name>
               hmac aes-xcbc-96
               exit
          ikev2-ikesa transform-set <ikev2_ikesa_tset_name>
               hmac aes-xcbc-96
               prf aes-scbc-128
               exit
          crypto template <crypto_template_name> ikev2-dynamic
               authentication remote eap-profile <eap_profile_name>
                    exit
               ikev2-ikesa retransmission-timeout <milliseconds>
               ikev2-ikesa transform-set list <ikev2_ikesa_tset_name>
               ikev2-ikesa rekey
               payload <payload_name> match childsa match any
               ipsec transform-set list <ipsec_tset_name>
                    lifetime <seconds>
                    rekey keepalive
                    exit
               ikev2-ikesa keepalive-user-activity
               ikev2-ikesa policy error-notification
 ikev2-ikesa policy use-rfc5996-notification
               exit
          ip routing maximum-paths <max_num>
          interface <swu_interface_name>
               ip address <ip_address> <subnet_mask>
               exit
          interface <swm_interface_name>
               ip address <ip_address> <subnet_mask>
               exit
          interface <epdg_dns_interface_name>
               ip address <ip_address> <subnet_mask>
               exit
          interface <swu_loopback_interface_name> loopback
               ip address <ip_address> <subnet_mask>
               exit
          interface <swm_ipsec_loopback_interface_name> loopback
               ip address <ip_address> <subnet_mask>
               exit
          subscriber default
               aaa group <group_name>
               ip context-name <epdg_context_name>
               exit
          aaa group default
               exit
          aaa group <group_name>
               diameter authentication dictionary <aaa_custom_dictionary>
```

```
            diameter authentication endpoint <endpoint_name>
            diameter authentication max-retries <max_retries>
            diameter authentication max-transmissions <max_transmissions>
           diameter authentication request-timeout <request_timeout_duration>

            diameter authentication failure-handling eap-request
request-timeout action terminate
            diameter authentication failure-handling eap-request
result-code <start_result_code_1> to <end_result_code_1> action retry-and-terminate

            diameter authentication failure-handling eap-request
result-code <start_result_code_2> to <end_result_code_2> action terminate
            diameter authentication server <host_name> priority <priority>
            exit
        gttp group default
        exit
    end
```

In this example, the EAP method is used for UE authentication. The **eap-profile** command creates the EAP profile to be used in the crypto template for the ePDG service. The **mode authenticator-pass-through** command specifies that the ePDG functions as an authenticator passthrough device, enabling an external EAP server to perform UE authentication.

The **crypto template** command and associated commands are used to define the cryptographic policy for the ePDG. You must create one crypto template per ePDG service. The **ikev2-dynamic** keyword in the **crypto template** command specifies that IKEv2 protocol is used. The **authentication remote** command specifies the EAP profile to use for authenticating the remote peer.

The **rekey keepalive** command enables Child SA (Security Association) rekeying so that a session will be rekeyed even when there has been no data exchanged since the last rekeying operation. The **ikev2-ikesa keepalive-user-activity** command resets the user inactivity timer when keepalive messages are received from the peer. The **ikev2-ikesa policy error-notification** command enables the ePDG to generate Error Notify messages for Invalid IKEv2 Exchange Message ID and Invalid IKEv2 Exchange Syntax for the IKE_SA_INIT exchange.

The **ip routing maximum-paths** command enables ECMP (Equal Cost Multiple Path) routing support and specifies the maximum number of ECMP paths that can be submitted by a routing protocol in the current context. The **interface** command creates each of the logical interfaces, and the associated **ip address** command specifies the IP address and subnet mask of each interface.

The **aaa group** command configures the AAA server group in the ePDG context and the **diameter authentication** commands specify the associated Diameter authentication settings.

The **ikev2-ikesa policy use-rfc5996-notification** command enables processing for new notification payloads added in RFC 5996, and is disabled by default.

Creating the ePDG Service

Use the following configuration example to do the following:

- Create the ePDG service.
- Specify the context in which the MAG/EGTP service will reside.
- Specify the ePDG FQDN (Fully Qualified Domain Name) used for longest suffix matching during P-GW dynamic allocation.
- Bind the crypto template to the ePDG service.

- Specify the Diameter origin endpoint and associated settings.
- Specify the name of the DNS client for DNS queries and bind the IP address.

Important When GTPv2 is used instead of mobile-access-gateway configuration, ePDG shall use associate egtp-service *egtp_service_name*.

```
configure
     context <epdg_context_name>
          epdg-service <epdg_service_name>
               plmn id mcc <code> mnc <code>
```

Note If egtp service is used, we should have **associate egtp-service** *<egtp service name>* instead of **mobile-access-gateway**

```
               mobile-access-gateway context <egress_context_name> mag-service
<mag_service_name>
               setup-timeout <seconds>
               fqdn <domain_name>
               bind address <ip_address> crypto-template <crypto_template_name>
               pgw-selection agent-info error-terminate
               dns-pgw selection topology weight
               exit
          ip route <ip_address/subnet mask> <ip_address/subnet mask> <gateway_ip_address>
 <mgmt_interface_name>
          ip domain-lookup
          ip name-servers <ip_address>
          diameter endpoint <endpoint_name>
               use-proxy
               origin host <host_name> address <ip_address> port <port_number>
               response-timeout <seconds>
               connection timeout <seconds>
               cea-timeout <seconds>
               dpa-timeout <seconds>
               connection retry-timeout <seconds>
               peer <peer_name> realm <realm_name> address <ip_address>
               route-entry peer <peer_id> weight <priority>
               exit
          dns-client <dns_client_name>
               bind address <ip_address>
               exit
          end
```

The ePDG context defaults to a MAG service configured in the same context unless the **mobile-access-gateway** command is used to specify the context where the MAG service will reside as shown above. The **fqdn** command configures the ePDG FQDN (Fully Qualified Domain Name) for longest suffix match during P-GW dynamic allocation. The IP address that you to the ePDG service above is used as the connection point for establishing the IKEv2 sessions between the WLAN UEs and the ePDG. The **pgw-selection agent-info error-terminate** command specifies the action to be taken during P-GW selection when the MIP6-agent-info parameter is

expected but not received from the AAA server/HSS, which is to terminate P-GW selection and reject the call. The **dns-pgw selection topology weight** command enables P-GW load balancing based on both topology, in which the nearest P-GW to the subscriber is selected first, and weight, in which the P-GW is select based on a weighted average.

The **ip route** command in this example creates a route for the SWu interface between the WLAN UEs and the ePDG and specifies the destination IP addresses that will use this route. The **ip domain-lookup** command enables domain name lookup via DNS for the current context. The **ip name-servers** command specifies the IP address of the DNS that the ePDG context will use for logical host name resolution. The **diameter endpoint** command specifies the Diameter origin endpoint.

The **origin host** command specifies the origin host for the Diameter endpoint. The **peer** command specifies a peer address for the Diameter endpoint. The **route-entry** command creates an entry in the route table for the Diameter peer.

The **dns-client** command specifies the DNS client used during P-GW FQDN discovery.

Egress Context and MAG Service Configuration

Create the Egress context and the MAG (Mobile Access Gateway) service by following the configuration example in the section Configuring the Egress Context and MAG Service, on page 12

Configuring the Egress Context and MAG Service

Use the following configuration example to configure the Egress context, the MAG (Mobile Access Gateway) service, the S2b interface and S2b loopback interface to the P-GW, and bind all of the logical interfaces to the physical Ethernet ports.

```
configure
     context <egress_context_name>
          interface <s2b_interface_name>
               ipv6 address <ipv6_address>
               exit
          interface <s2b_loopback_interface_name>
               ipv6 address <ipv6_address>
               exit
          subscriber default
               exit
          aaa group default
               exit
          gtpp group default
               exit
          mag-service <mag_service_name>
               reg-lifetime <seconds>
               bind address <ipv6_address>
               exit
          ipv6 route <ipv6_address/prefix_length> next-hop <ipv6_address> interface
 <s2b_interface_name>
          exit
     port ethernet <slot_number/port_number>
          no shutdown
          vlan <tag>
          bind interface <swu_interface_name> <epdg_context_name>
```

```
    exit
port ethernet <slot_number/port_number>
    no shutdown
    vlan <tag>
    bind interface <epdg_dns_interface_name> <epdg_context_name>
    exit
port ethernet <slot_number/port_number>
    no shutdown
    vlan <tag>
    bind interface <swm_interface_name> <epdg_context_name>
    exit
port ethernet <slot_number/port_number>
    no shutdown
    vlan <tag>
    bind interface <s2b_interface_name> <egress_context_name>
    exit
end
```

The **mag-service** command creates the MAG (Mobile Access Gateway) service that communicates with the LMA (Local Mobility Anchor) service on the P-GW to provide network-based mobility management. The **ipv6 route** command configures a static IPv6 route to the next-hop router. In this configuration, it configures a static route from the ePDG to the P-GW over the S2b interface. The **bind interface** command binds each logical interface to a physical Ethernet port.

Egress Context and EGTP Service Configuration

Create the Egress context and the EGTP (Evolved GPRS Tunnel Protocal) service by following the configuration example in the section Configuring the Egress Context and EGTP Service, on page 13

Configuring the Egress Context and EGTP Service

Use the following configuration example to configure thegress context, the EGTP (Evolved GPRS Tunnel Protocal) service, the S2b interface and S2b loopback interface to the P-GW, and bind all of the logical interfaces to the physical Ethernet ports.

Important If you modify the **interface-type** command, the parent service (service within which the eGTP/GTP-U service is configured) will automatically restart. Service restart results in dropping of active calls associated with the parent service.

```
configure
    context <egress_context_name>
        interface <s2b_interface_name>
            ipv4/ipv6 address <ipv6_address>
            exit
        interface <s2b_loopback_interface_name>
            ipv4/ipv6 address <ipv6_address>
            exit
        subscriber default
            exit
        aaa group default
```

```
            exit
        gtpp group default
            exit
        gtpu-service <gtpu-service-name>
            reg-lifetime <seconds>
            bind ipv4/ipv6-address <s2bloopbackipv4/ipv6_address>
            exit
        egtp-service egtp-epdg-egress
            interface-type interface-epdg-egress
            associate gtpu-service gtpu-epdg-egress
            exit
       ipv4/ipv6 route <ipv4/ipv6_address/prefix_length> next-hop <ip4/ipv6_address>
interface <s2b_interface_name>
        exit
    port ethernet <slot_number/port_number>
        no shutdown
        vlan <tag>
        bind interface <swu_interface_name> <epdg_context_name>
        exit
    port ethernet <slot_number/port_number>
        no shutdown
        vlan <tag>
        bind interface <epdg_dns_interface_name> <epdg_context_name>
        exit
    port ethernet <slot_number/port_number>
        no shutdown
        vlan <tag>
        bind interface <swm_interface_name> <epdg_context_name>
        exit
    port ethernet <slot_number/port_number>
        no shutdown
        vlan <tag>
        bind interface <s2b_interface_name> <egress_context_name>
        exit
    end
```

The **egtp-service** command creates the eGTP (evolved GPRS Tunneling Protocol) service that communicates with the LMA (Local Mobility Anchor) service on the P-GW to provide network-based mobility management. The **ipv6 route** command configures a static IPv6 route to the next-hop router. In this configuration, it configures a static route from the ePDG to the P-GW over the S2b interface. The **bind interface** command binds each logical interface to a physical Ethernet port.

Bulk Statistics Configuration

Use the following configuration example to enable ePDG bulk statistics:

```
configure
    bulkstats collection
    bulkstats mode
        sample-interval <time_interval>
        transfer-interval <xmit_time_interval>
        file <number>
```

```
            receiver <ip_address> primary mechanism ftp login <username>
password <pwd>
            receiver <ip_address> secondary mechanism ftp login <username>
password <pwd>
            epdg schema <file_name> format " txbytes : txbytes txpkts :
txpkts rxbytes : rxbytes rxpkts : rxpkts sess-txbytes : sess-txbytes
sess-rxbytes : sess-rxbytes sess-txpackets : sess-txpackets sess-rxpackets
 : sess-rxpackets eap-rxttlsrvrpassthru : eap-rxttlsrvrpassthru
eap-rxsuccsrvrpassthru : eap-rxsuccsrvrpassthru num-gtp-bearermodified :
 num-gtp-bearermodified num-gtp-db-active : num-gtp-db-active
num-gtp-db-released : num-gtp-db-released curses-gtp-ipv4 : curses-gtp-ipv4
 curses-gtp-ipv6 : curses-gtp-ipv6 curses-gtp-ipv4v6 : curses-gtp-ipv4v6
 "
            end
```

The **bulkstats collection** command in this example enables bulk statistics, and the system begins collecting pre-defined bulk statistical information.

The **bulkstats mode** command enters Bulk Statistics Configuration Mode, where you define the statistics to collect.

The **sample-interval** command specifies the time interval, in minutes, to collect the defined statistics. The *<time-interval>* can be in the range of 1 to 1440 minutes. The default value is 15 minutes.

The **transfer-interval** command specifies the time interval, in minutes, to transfer the collected statistics to the receiver (the collection server). The *<xmit_time_interval>* can be in the range of 1 to 999999 minutes. The default value is 480 minutes.

The **file** command specifies a file in which to collect the bulk statistics. A bulk statistics file is used to group bulk statistics schema, delivery options, and receiver configuration. The *<number>* can be in the range of 1 to 4.

The **receiver** command in this example specifies a primary and secondary collection server, the transfer mechanism (in this example, ftp), and a login name and password.

The **epdg schema** command specifies that the epdg schema is used to gather statistics. The *<file_name>* is an arbitrary name (in the range of 1 to 31 characters) to use as a label for the collected statistics defined by the **format** option. The **format** option defines within quotation marks the list of variables in the epdg schema to collect. The format string can be in the range of 1 to 3599.

For descriptions of the epdg schema variables, see "ePDG Schema Statistics" in the *Statistics and Counters Reference.* For more information on configuring bulk statistics, see the *System Administration Guide.*

Logging Configuration

Use the following configuration example to enable logging on the ePDG:

```
configure
     logging filter active facility sessmgr level <critical/error>
     logging filter active facility ipsec level <critical/error>
     logging filter active facility ikev2 level <critical/error>
     logging filter active facility epdg level <critical/error>
     logging filter active facility aaamgr level<critical/error>
     logging filter active facility diameter level<critical/error>
     logging filter active facility egtpc level<critical/error>
```

```
logging filter active facility egtpmgr level<critical/error>
logging filter active facility gtpumgr level<critical/error>
logging filter active facility diameter-auth level<critical/error>
logging active
end
```

Non UICC device support for certificate and multi authentication configuration

List of authentication methods are defined and associated in Crypto Template. The basic sample configuration required for OCSP and Certificate based authentication is as follows. For backward compatibility, the configuration for auth method inside Crypto Template will be working.

The following are the configuration considerations:

1. At max three sets of authentication methods in list can be associated.
2. Each set has only one local and one remote authentication method configuration.
3. The existing configuration inside the Crypto Template takes precedence over the new auth-method-set defined in case same auth method is configured at both places.

configure

CA Certificate for device certificate authentication:

ca-certificate name *<ca-name>* **pem url file:** *<ca certificate path>*

ePDG Certificate:

```
certificate name <epdg-name> pem url file: <epdg certificate path> private-key
pem url file:<epdg private key path>
       eap-profile <profile name>
          mode authenticator-pass-through
       exit
       ikev2-ikesa auth-method-set <list-name-1>
         authentication remote certificate
         authentication local certificate
       exit
         ikev2-ikesa auth-method-set <list-name-2>
           authentication eap-profile eap1
       exit
            crypto template boston ikev2-subscriber
       ikev2-ikesa auth-method-set list <list-name-2> <list-name-2>
         certificate <epdg-name>
         ca-certificate list ca-cert-name <ca-name>
       exit
```

Saving the Configuration

Save the ePDG configuration file 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, see the *System Administration Guide* and the *eHRPD/LTE Command Line Interface Reference.*

Verifying the Configuration

For additional information on how to verify and save configuration files, see the *System Administration Guide* and the *eHRPD/LTE Command Line Interface Reference.*