Understanding the Service Operation

The system provides wireless carriers with a flexible solution for providing Gateway GPRS Support Node (GGSN) functionality for GPRS or UMTS networks.

The system functioning as a GGSN is capable of supporting the following types of subscriber data sessions:

- **Transparent IP:** The subscriber is provided basic access to a packet data network (PDN) without the GGSN authenticating the subscriber. Either a static or dynamic IP address can be assigned to the MS in this scenario.
- **Non-transparent IP:** The GGSN provides subscriber authentication services for the data session. Either a static or dynamic IP address can be assigned to the MS in this scenario.
- **Network-initiated:** An IP Packet Data Unit (PDP) is received by the GGSN from the PDN for a specific subscriber. If configured to support network-initiated sessions, the GGSN, will initiate the process of paging the MS and establishing a PDP context.
- **PPP Direct Access:** The GGSN terminates the subscribers PPP session and provides subscriber authentication services for the data session. Either a static or dynamic IP address can be assigned to the MS in this scenario.
- **Virtual Dialup Access:** The GGSN functions as an LAC, encapsulates subscriber packets using L2TP, and tunnels them directly to an LNS for processing.
- **Corporate IP VPN Connectivity:** Similar to the Virtual Dialup Access model, however, the GGSN is configured to tunnel subscriber packets to a corporate server using a protocol such as IP-in-IP.

Prior to connecting to the command line interface (CLI) and beginning the system's configuration, there are important things to understand about how the system supports these applications. This chapter provides terminology and background information that must be considered before attempting to configure the system.

Terminology

This section defines some of the terms used in the chapters that follow.

Contexts

A context is a logical grouping or mapping of configuration parameters that pertain to various physical ports, logical IP interfaces, and services. A context can be thought of as a virtual private network (VPN).

The system supports the configuration of multiple contexts. Each is configured and operates independently from the others. Once a context has been created, administrative users can then configure services, logical IP interfaces, subscribers, etc.for that context. Administrative users would then bind the logical interfaces to physical ports.

Contexts can also be assigned domain aliases, wherein if a subscriber's domain name matches one of the configured alias names for that context, then that context is used.

Contexts on the system can be categorized as follows:

- **Source context:** Also referred to as the "ingress" context, this context provides the subscriber's point-of-entry in the system. It is also the context in which services are configured. For example, in a GPRS/UMTS network, the radio network containing the Service GPRS Support Nodes (SGSNs) would communicate with the system via Gn interfaces configured within the source context as part of the GGSN service.
- **Destination context:** Also referred to as the "egress" context, this context is where a subscriber is provided services (such as access to the Internet) as defined by access point name (APN) configuration templates. For example, the system's destination context would be configured with the interfaces facilitating subscriber data traffic to/from the Internet, a VPN, or other PDN.
- **Authentication context:** This context provides authentication functionality for subscriber PDP contexts and/or administrative user sessions and contains the policies and logical interfaces for communicating with Remote Authentication Dial In User Service (RADIUS) authentication servers.

For subscriber authentication, this functionality must be configured in the same system context as the APN template(s). Optionally, to simplify the configuration process, both subscriber RADIUS authentication functionality and APN templates can be configured in the destination context.

Important To ensure scalability, authentication functionality for subscriber sessions should not be configured in the local context.

For administrative users, authentication functionality can either be configured in the local context or be authenticated in the same context as subscribers.

- **Accounting context:** This context provides accounting functionality for subscriber PDP contexts and/or administrative user sessions.

The system context in which accounting functionality is configured depends on the protocol used. Accounting for subscriber PDP contexts can be performed using either the GPRS Tunneling Protocol Prime (GTPP) or RADIUS. Accounting for administrative user sessions is based on RADIUS.

When using GTPP, it is recommended that accounting functionality be configured in a system source context along with the GGSN service.

When using RADIUS for subscriber accounting, it must be configured in the same context as RADIUS authentication. To simplify the configuration process, RADIUS-based authentication and accounting can be configured in a destination context as long as the APN templates are configured there as well.

RADIUS-based accounting for administrative user sessions can either be configured in the local context or in the same context used for subscriber accounting.

Important To ensure scalability, accounting functionality for subscriber sessions should not be configured in the local context.

- **Local context:** This is the default context on the system used to provide out-of-band management functionality. The local context is described in the Command Line Reference.

Logical Interfaces

Prior to allowing the flow of user data, the port must be associated with a virtual circuit or tunnel called a logical interface. A logical interface within the system is defined as the logical assignment of a virtual router instance that provides higher-layer protocol transport, such as Layer 3 IP addressing. Interfaces are configured as part of the VPN context and are independent from the physical port that will be used to bridge the virtual interfaces to the network.

Logical interfaces are assigned to IP addresses and are bound to a specific port during the configuration process. Logical interfaces are also associated with services through bindings. Services are bound to an IP address that is configured for a particular logical interface. When associated, the interface takes on the characteristics of the functions enabled by the service. For example, if an interface is bound to a GGSN service, it will function as a Gn interface between the GGSN service and the SGSN. Services are defined later in this section.

There are several types of logical interfaces that must be configured to support the service as described below:

- **Gn:** This is the interface used by the GGSN to communicate with SGSNs on the same GPRS/UMTS Public Land Mobile Network (PLMN). This interface serves as both the signalling and data path for establishing and maintaining subscriber PDP contexts.

  The GGSN communicates with SGSNs on the PLMN using the GPRS Tunnelling Protocol (GTP). The signalling or control aspect of this protocol is referred to as the GTP Control Plane (GTPC) while the encapsulated user data traffic is referred to as the GTP User Plane (GTPU).

  One or more Gn interfaces can be configured per system context. Gn interfaces are bound to ports on either the Ethernet 10/100 or Ethernet 1000 Line Cards or on the four-port Quad Gig-E Line Card (QGLC).

- **Ga:** This is the interface used by the GGSN to communicate with the charging gateway (CG). The charging gateway is responsible for sending GGSN charging detail records (G-CDRs) received from the GGSN for each PDP context to the billing system.

  The GGSN communicates with the CGs on the PLMN using GTP Prime (GTPP).

  One or more Ga interfaces can be configured per system context. Ga interfaces are bound to ports on either the Ethernet 10/100 or Ethernet 1000 Line Cards or on the QGLC.

- **Gc:** This is the interface used by the GGSN to communicate with the Home Location Register (HLR) via a GTP-to-MAP (Mobile Application Part) protocol convertor. This interface is used for network initiated PDP contexts.

  For network initiated PDP contexts, the GGSN will communicate with the protocol convertor using GTP. The convertor, in turn, will communicate with the HLR using MAP over Signalling System 7 (SS7).

One Gc interface can be configured per system context. Gc interfaces are bound to ports on either the Ethernet 10/100 or Ethernet 1000 Line Cards or on the QGLC.

- **Gi:** This is the interface used by the GGSN to communicate with packet data networks (PDNs) external to the PLMN. Examples of PDNs are the Internet or corporate intranets.

  Additionally, inbound packets received on this interface could initiate a network requested PDP context if the intended MS is not currently connected.

  One or more Gi interfaces can be configured per system context. Gi interfaces are bound to ports on either the Ethernet 10/100 or Ethernet 1000 Line Cards or on the QGLC.

- **Gp:** This is the interface used by the GGSN to communicate with GPRS support nodes (GSNs, e.g. GGSNs and/or SGSNs) on different PLMNs. Within the system, a single interface can serve as both a Gn and a Gp interface.

  One or more Gn/Gp interfaces can be configured per system context. Gp interfaces are bound to ports on either the Ethernet 10/100 or Ethernet 1000 Line Cards or on the QGLC.

- **AAA:** This is the interface used by the GGSN to communicate with either an authentication or accounting server on the network using the Remote Authentication Dial In User Service (RADIUS) protocol.

  This is an optional interface that can be by the GGSN for subscriber PDP context authentication or accounting. AAA interfaces are bound to ports on either the Ethernet 10/100 or Ethernet 1000 Line Cards or on the QGLC.

- **S6b**: This is an optional Diameter protocol-based interface over which the GGSN communicates with 3G AAA/HSS in LTE/SAE network for subscriber authorization.

  Important This interface is supported through license-enabled feature. For more information on this support, refer *Common Gateway Access Support* in guide.

- **DHCP:** This is the interface used by the GGSN to communicate with a Dynamic Host Control Protocol (DHCP) Server. The system can be configured to dynamically provide IP addresses for PDP contexts from the DHCP server.

  DHCP interfaces are bound to ports on either the Ethernet 10/100 or Ethernet 1000 Line Cards or on the QGLC.

Bindings

A binding is an association between "elements" within the system. There are two types of bindings: static and dynamic.

Static binding is accomplished through the configuration of the system. Static bindings are used to associate:

- A specific logical interface (configured within a particular context) to a physical port. Once the interface is bound to the physical port, traffic can flow through the context just as if it were any physically defined circuit. Static bindings support any encapsulation method over any interface and port type.
- A service to an IP address assigned to a logical interface within the same context. This allows the interface to take on the characteristics (i.e., support the protocols) required by the service. For example, a GGSN service bound to a logical interface will cause the logical interface to take on the characteristics of a Gn interface within a GPRS/UMTS network.

Dynamic binding associates a subscriber to a specific egress context based on the configuration of their profile or system parameters. This provides a higher degree of deployment flexibility as it allows a wireless carrier to support multiple services and facilitates seamless connections to multiple networks.

Services

Services are configured within a context and enable certain functionality. The following services can be configured on the system:

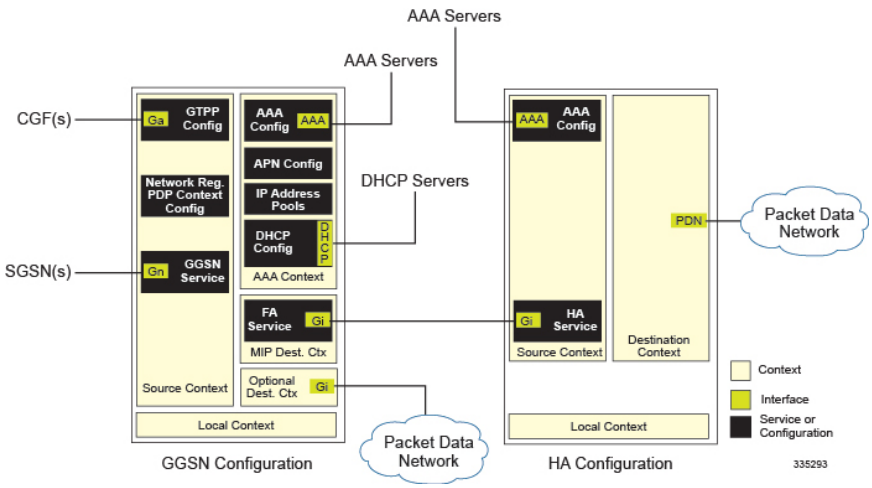
- **GGSN services:** GGSN services are configured to support both mobile-initiated and network-requested PDP contexts. The GGSN service must be bound to a logical interface within the same context. Once bound, the interface takes on the characteristics of a Gn interface. Multiple services can be bound to the same logical interface. Therefore, a single physical port can facilitate multiple Gn interfaces.
- **FA services**: FA services are configured to support Mobile IP and define FA functionality on the system.

  The system supports multiple Mobile IP configurations. A single system can perform the function of a FA only, an HA only, or a combined PDSN/FA/HA. Depending on your configuration, the FA service can create and maintain the Pi interface between the PDSN/FA and the HA or it can communicate with an HA service configured within the same context.

  The FA service should be configured in a different context from the PDSN service. However, if the FA service will be communicating with an HA that is a separate network element, it must be configured within the same context as and be bound to the Pi interfaces that allow it to communicate with the HA.
- **LAC services:** LAC services are configured on the system to provide Layer 2 Tunneling Protocol (L2TP) access concentrator (LAC) functionality. LAC services can be configured and used within networks to provide secure tunneling to an L2TP network server (LNS) on a remote PDN.
- **DHCP services:** DHCP services are configured on a system to provide dynamic assignment of IP address to PDP contexts through the use of the Dynamic Host Configuration Protocol (DHCP).

Following figure illustrates the relationship between services, interfaces, and contexts within the system for GPRS/UMTS networks.

Figure 1: Service, Interface, and Context Relationship Within the System for GPRS/UMTS Networks



The source context used to service a subscriber session is the same as the context in which the GGSN service is configured. Each GGSN service is bound to an IP address in a source context. The SGSNs select which IP address to use, typically by using DNS. Once a subscriber has established a PDP context with a GGSN, the SGSNs continue to use that same PDP context and GGSN as the subscriber moves about the network.

Destination contexts are selected based on APN configuration. When the system receives a **Create PDP Context Request** message from the SGSN, it examines the APN that was provided. If the APN is not found on the system, the system rejects the request.

After the APN has been found, the system may choose a different APN based on the system's virtual APN configuration. In any event, a final APN is selected by the system

The system determines the destination context to use based on a parameter contained within the final APN configuration. If a valid destination context name is configured for this parameter, it is used. If the name is not valid, or if it is not configured, the system uses the context in which the APN is configured.

Once the system locates the context in which the APN is configured, it uses that context for subscriber authentication and RADIUS-based accounting (if enabled). Any parameters returned by the RADIUS server during the subscriber authentication/authorization override APN configuration parameters.

If GTPP-based accounting is enabled, the system uses the source context for accounting. That context may be overridden by configuring a different accounting context to use in the GGSN service configuration.

How the System Selects Contexts

This section provides details about the process that is used to determine which context to use for context-level administrative user and/or subscriber sessions. Understanding this process allows you to better plan your configuration in terms of how many contexts and interfaces need to be configured.

Context Selection for Subscriber Sessions

The context selection process for a subscriber session is more involved than that for the administrative users.

The source context used to service a subscriber session is the same as the context in which the GGSN service is configured. Each GGSN service is bound to an IP address in a source context. The SGSNs select which IP address to use, typically by using DNS. Once a subscriber has established a PDP context with a GGSN, the SGSNs continue to use that same PDP context and GGSN as the subscriber moves about the network.

Destination contexts are selected based on APN configuration. When the system receives a **Create PDP Context Request** message from the SGSN, it examines the APN that was provided. If the APN is not found on the system, the system rejects the request.

After the APN has been found, the system may choose a different APN based on the system's virtual APN configuration. In any event, a final APN is selected by the system

The system determines the destination context to use based on a parameter contained within the final APN configuration. If a valid destination context name is configured for this parameter, it is used. If the name is not valid, or if it is not configured, the system uses the context in which the APN is configured.

Once the system locates the context in which the APN is configured, it uses that context for subscriber authentication and RADIUS-based accounting (if enabled). Any parameters returned by the RADIUS server during the subscriber authentication/authorization override APN configuration parameters.

If GTPP-based accounting is enabled, the system uses the source context for accounting. That context may be overridden by configuring a different accounting context to use in the GGSN service configuration.