GGSN Support in GPRS/UMTS Wireless Data Services

The Cisco systems provides wireless carriers with a flexible solution that functions as a Gateway GPRS Support Node (GGSN) in General Packet Radio Service (GPRS) or Universal Mobile Telecommunications System (UMTS) wireless data networks.

This overview provides general information about the GGSN including:

Product Description

The GGSN works in conjunction with Serving GPRS Support Nodes (SGSNs) within the network to perform the following functions:

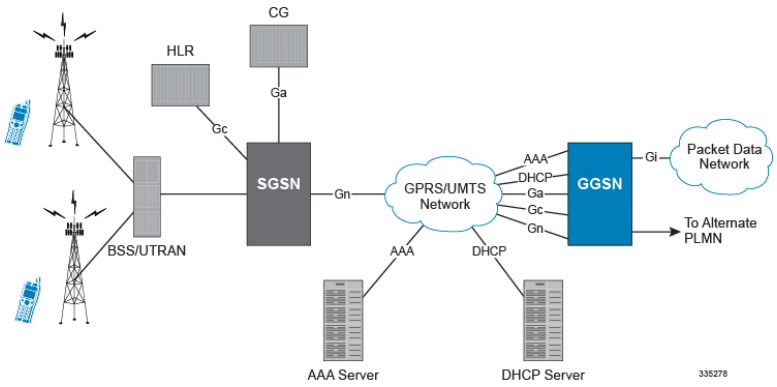
- Establish and maintain subscriber Internet Protocol (IP) or Point-to-Point Protocol (PPP) type Packet Data Protocol (PDP) contexts originated by either the mobile or the network
- Provide charging detail records (CDRs) to the charging gateway (CG, also known as the Charging Gateway Function (CGF))
- Route data traffic between the subscriber's Mobile Station (MS) and a Packet Data Networks (PDNs) such as the Internet or an intranet

PDNs are associated with Access Point Names (APNs) configured on the system. Each APN consists of a set of parameters that dictate how subscriber authentication and IP address assignment is to be handled for that APN.

In addition to providing the basic GGSN functionality as described above, the system can be configured to support Mobile IP and/or Proxy Mobile IP data applications to provide mobility for subscriber IP PDP contexts. When supporting these services, the system can be configured to either function as a GGSN and Foreign

Agent (FA), a stand-alone Home Agent (HA), or a GGSN, FA, and HA simultaneously within the carrier's network.

Figure 1: Basic GPRS/UMTS Network Topology



In accordance with RFC 2002, the FA is responsible for mobile node registration with, and the tunneling of data traffic to/from the subscriber's home network. The HA is also responsible for tunneling traffic, but also maintains subscriber location information in Mobility Binding Records (MBRs).

Product Specification

This section describes the hardware and software requirements for GGSN service.

This section provides the following information:

Licenses

The GGSN is a licensed Cisco product and therefore separate session and feature licenses may be required. Contact your Cisco account representative for detailed information on specific licensing requirements. For information on installing and verifying licenses, refer to the *Managing License Keys* section of the *Software Management Operations* chapter in the *System Administration Guide*.

Qualified Platforms

GGSN is a StarOS application that runs on Cisco ASR 5500 and virtualized platforms. For additional platform information, refer to the appropriate System Administration Guide and/or contact your Cisco account representative.

Operating System Requirements

The Cisco GGSN is available for ST16 and chassis.

Network Deployment and Interfaces

This section describes the supported interfaces and deployment scenario of GGSN in GPRS/UMTS network.

The following information is provided in this section:

GGSN in the GPRS/UMTS Data Network

The figures shown below display simplified network views of the Cisco GGSN in a GPRS/UMTS network and the system supporting Mobile IP and Proxy Mobile IP function; and both GGSN/Foreign Agent (FA) and GGSN/FA/Home Agent (HA) combinations respectively.

Figure 2: Basic GPRS/UMTS Network Topology 1

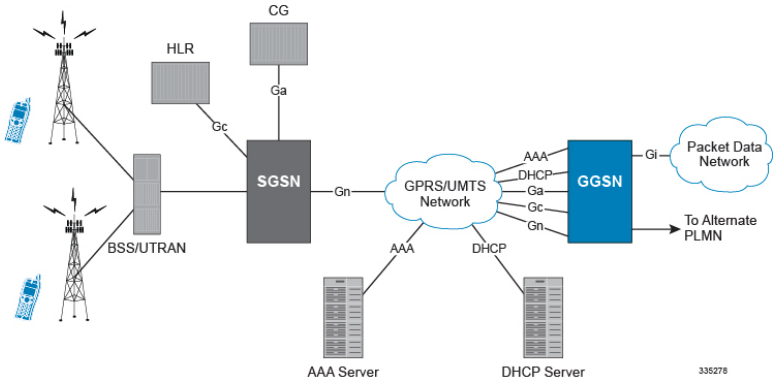


Figure 3: Combined GGSN/FA Deployment for Mobile IP and/or Proxy Mobile IP Support

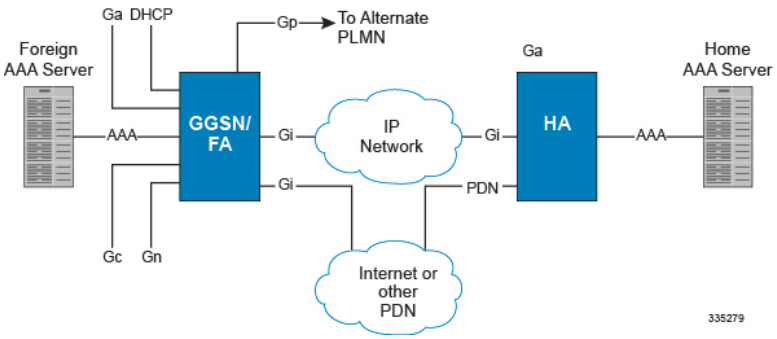
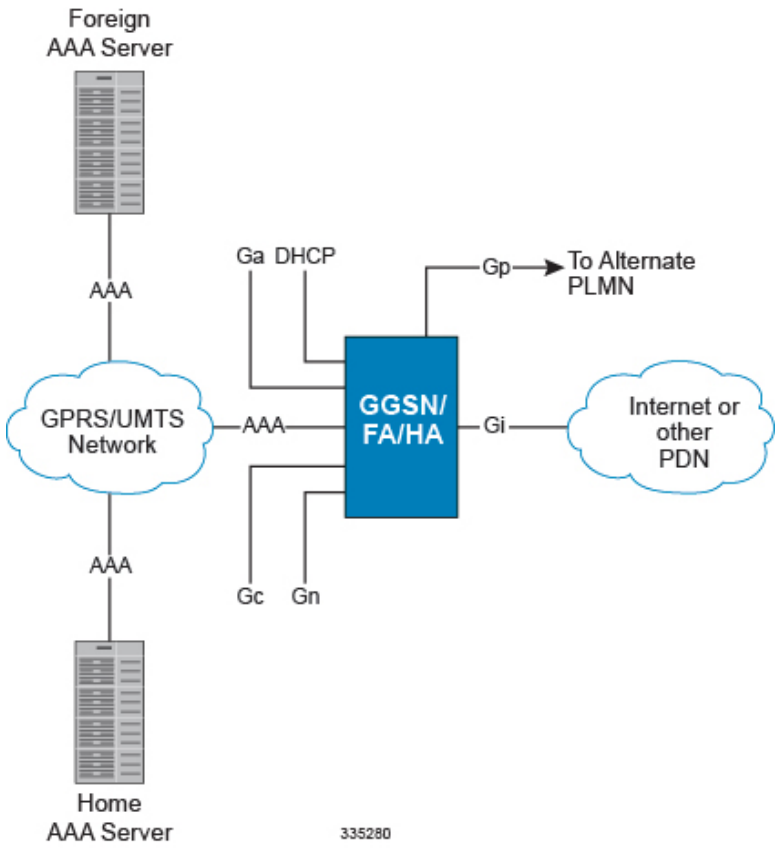


Figure 4: Combined GGSN/FA/HA Deployment for Mobile IP and/or Proxy Mobile IP Support



Supported Interfaces

In support of both mobile and network originated subscriber PDP contexts, the system GGSN provides the following network interfaces:

- **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 signaling and the data path for establishing and maintaining subscriber PDP contexts.

  The GGSN communicates with SGSNs on the PLMN using GPRS Tunnelling Protocol (GTP). The signaling 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).

Important One or more Gn interfaces can be configured per system context.

- **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 Data Records (G-CDRs) received from the GGSN for each PDP context to the billing system. System supports TCP and UDP as transport layer for this interface.

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

Important One or more Ga interfaces can be configured per system context.

- **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 Signaling System 7 (SS7).

  One Gc interface can be configured per system context.

- **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.

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

  For systems configured as a GGSN/FA, this interface is used to communicate with HAs for Mobile IP and Proxy Mobile IP support.

  One or more Gi interfaces can be configured per system context. For Mobile IP and Proxy Mobile IP, at least one Gi interface must be configured for each configured FA service. Note that when the system is simultaneously supporting GGSN, FA, and HA services, traffic that would otherwise be routed over the Gi interface is routed inside the chassis.

- **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.

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

  This is an optional interface that can be used by the GGSN for subscriber PDP context authentication and accounting.

- **DHCP**: This is the interface used by the GGSN to communicate with a Dynamic Host Control Protocol (DHCP) Server. The system can be configured as DHCP-Proxy or DHCP Client to provide IP addresses to MS on PDP contexts activation the DHCP server dynamically.

- **Gx**: This is an optional Diameter protocol-based interface over which the GGSN communicates with a Charging Rule Function (CRF) for the provisioning of charging rules that are based on the dynamic analysis of flows used for an IP Multimedia Subsystem (IMS) session. The system provides enhanced support for use of Service Based Local Policy (SBLP) to provision and control the resources used by the IMS subscriber. It also provides Flow based Charging (FBC) mechanism to charge the subscriber dynamically based on content usage.

Important The Gx interface is a license-enabled support. For more information on this support, refer *Gx Interface Support* in this guide.

- **Gy**: This is an optional Diameter protocol-based interface over which the GGSN communicates with a Charging Trigger Function (CTF) server that provides online charging data. Gy interface support provides an online charging interface that works with the ECS deep packet inspection feature. With Gy, customer traffic can be gated and billed in an "online" or "prepaid" style. Both time- and volume-based charging models are supported. In all of these models, differentiated rates can be applied to different services based on shallow or deep packet inspection.

Important This interface is supported through Enhanced Charging Service. For more information on this support, refer *Enhanced Charging Service Administration Guide*.

- **GRE**: This new protocol interface in GGSN platform adds one additional protocol to support mobile users to connect to their enterprise networks: Generic Routing Encapsulation (GRE). GRE Tunneling is a common technique to enable multi-protocol local networks over a single-protocol backbone, to connect non-contiguous networks and allow virtual private networks across WANs. This mechanism encapsulates data packets from one protocol inside a different protocol and transports the data packets unchanged across a foreign network. It is important to note that GRE tunneling does not provide security to the encapsulated protocol, as there is no encryption involved (like IPSEC offers, for example).

Important The GRE protocol interface is a license-enabled support. For more information on this support, refer *GRE Protocol Interface Support* in this guide.

- **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.

  The S6b interface has the ability to pull SGSN-MCC-MNC from either GTP or AAA-I and send to OCS. When a customer roams into a GSM environment, OCS needs location information for online charging and metering. 3GPP-SGSN-MCC-MNC AVP, and Location Information AVP are defined in Gy and can be used to identify customer location. With this feature, the GGSN collects the value of SGSN-MCC-MNC from the S6b AAA message, so that it can be available to OCS through Gy interface while passing CCR and CCA messages.

  The S6b interface has been enhanced to pass on the UE assigned IPv6 address (IPv6 prefix and IPv6 interface ID) to the AAA server. S6b interface also has support for Framed-IPv6-Pool, Framed IP Pool, and served party IP address AVPs based IP allocation. With this support, based on the Pool name and APN name received from AAA server, the selection of a particular IP pool from the configuration is made for assigning the IP address.

  The S6b interface on the P-GW or GGSN can be manually disabled to stop all message traffic to the 3GPP AAA during overload conditions. When the interface is disabled, the system uses locally configured APN-specific parameters including: Framed-Pool, Framed-IPv6-Pool, Idle-Timeout, Charging-Gateway-Function-Host, Server-Name (P-CSCF FQDN). This manual method is used when the HSS/3GPP AAA is in overload condition to allow the application to recover and mitigate the impact to subscribers

  The IPv6 address reporting through Authorization-Authentication-Request (AAR) towards the S6b interface is no longer a default feature. It is now configurable through the command line interface.

Another enhancement on S6b interface support is the new S6b Retry-and-Continue functionality that creates an automatic trigger in the GGSN and P-GW to use the locally configured APN profile upon receipt of any uniquely defined Diameter error code on the S6b interface for an Authorization-Authentication-Request (AA-R) only. This procedure would be utilized in cases where a protocol, transient, or permanent error code is returned from the both the primary and secondary AAA to the GGSN or P-GW. This behavior is only applicable to the aaa-custom15 Diameter dictionary.

Important The S6b interface can still be disabled via the CLI per the existing MOPs in the event of a long-term AAA outage

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

- **Rf**: This interface enables offline accounting functions on the GGSN in accordance with the 3GPP Release 8 specifications. The charging data information is recorded at the GGSN for each mobile subscriber UE pertaining to the radio network usage. Due to the transfer of charging information to GGSN, the services being rendered are not affected in real time.

Important GGSN Software also supports additional interfaces. For more information on additional interfaces, refer *Features and Functionality - Optional Enhanced Feature Software* section.

Features and Functionality - Base Software

This section describes the features and functions supported by default in base software on GGSN service and do not require any additional licenses.

Important To configure the basic service and functionality on the system for GGSN service, refer configuration examples provide in *GGSN Administration Guide*.

16,000 SGSN Support

With growing roaming agreements, many more GPRS/UMTS networks support certain APNs and therefore the number of SGSNs that could connect to the GGSN increases. This feature increases the number of connected SGSNs thereby allowing a single GGSN service to support a much larger roaming network.

The GGSN service supports a maximum of 16,000 SGSN IP addresses. The chassis limit for bulk statistics collection is also limit to 16,000. No change in configuration is needed to support this feature.

AAA Server Groups

Value-added feature to enable VPN service provisioning for enterprise or MVNO customers. Enables each corporate customer to maintain its own AAA servers with its own unique configurable parameters and custom dictionaries.

This feature provides support for up to 800 AAA (RADIUS and Diameter) server groups and 800 NAS IP addresses that can be provisioned within a single context or across the entire chassis. A total of 128 servers can be assigned to an individual server group. Up to 1,600 accounting, authentication and/or mediation servers are supported per chassis and may be distributed across a maximum of 1,000 APNs. This feature also enables the AAA servers to be distributed across multiple APN within the same context.

For more information, refer to the *AAA Interface Administration and Reference*.

Access Control List Support

Access Control Lists provide a mechanism for controlling (i.e permitting, denying, redirecting, etc.) packets in and out of the system.

IP access lists, or Access Control Lists (ACLs) as they are commonly referred to, are used to control the flow of packets into and out of the system. They are configured on a per-context basis and consist of "rules" (ACL rules) or filters that control the action taken on packets that match the filter criteria

Once configured, an ACL can be applied to any of the following:

- An individual interface
- All traffic facilitated by a context (known as a policy ACL)
- An individual subscriber
- All subscriber sessions facilitated by a specific context

There are two primary components of an ACL:

- Rule: A single ACL consists of one or more ACL rules. The rule is a filter configured to take a specific action on packets matching specific criteria. Up to 128 rules can be configured per ACL.

  Each rule specifies the action to take when a packet matches the specifies criteria. This section discusses the rule actions and criteria supported by the system.

- Rule Order: A single ACL can consist of multiple rules. Each packet is compared against each of the ACL rules, in the order in which they were entered, until a match is found. Once a match is identified, all subsequent rules are ignored.

Important For more information on Access Control List configuration, refer *IP Access Control List* in *System Administration Guide*.

ANSI T1.276 Compliance

ANSI T1.276 specifies security measures for Network Elements (NE). In particular it specifies guidelines for password strength, storage, and maintenance security measures.

ANSI T1.276 specifies several measures for password security.

These measures include:

- Password strength guidelines
- Password storage guidelines for network elements
- Password maintenance, e.g. periodic forced password changes

These measures are applicable to the ST16 and chassis and the Web Element Manager since both require password authentication. A subset of these guidelines where applicable to each platform will be implemented. A known subset of guidelines, such as certificate authentication, are not applicable to either product. Furthermore, the platforms support a variety of authentication methods such as RADIUS and SSH which are dependent on external elements. ANSI T1.276 compliance in such cases will be the domain of the external element. ANSI T1.276 guidelines will only be implemented for locally configured operators.

APN Support

The GGSN's Access Point Name (APN) support offers several benefits:

- Extensive parameter configuration flexibility for the APN.
- Creation of subscriber tiers for individual subscribers or sets of subscribers within the APN.
- Virtual APNs to allow differentiated services within a single APN.

Virtual APN Selection feature enables an operator to select Virtual APN based on 4 cc-profile bits and 12 cc-behavior bits or on the basis on complete 16 cc-behavior bits of Charging Characteristics for GGSN, P-GW, and SAEGW nodes, thus utilizing all 16 bits. This functionality is CLI controlled.

Up to 2,048 APNs can be configured in the GGSN. An APN may be configured for any PDP-type and PDP-type for roamers, that is, PPP, IPv4, IPv6 or both IPv4 and IPv6. Many dozens of parameters may be configured independently for each APN.

Here are a few highlights of what may be configured:

- **Accounting**: RADIUS, GTPP or none. Server group to use. Charging characteristics. Interface with mediation servers.
- **Authentication**: Protocol, such as, CHAP or PAP or none. Default username/password. Server group to use. Limit for number of PDP contexts.
- **Enhanced Charging**: Name of rulebase to use, which holds the enhanced charging configuration (e.g., eG-CDR variations, charging rules, prepaid/postpaid options, etc.).
- **IP**: Method for IP address allocation (e.g., local allocation by GGSN, Mobile IP, DHCP, DHCP relay, etc.). IP address ranges, with or without overlapping ranges across APNs.
- **Tunneling**: PPP may be tunneled with L2TP. IPv4 may be tunneled with GRE, IP-in-IP or L2TP. Load-balancing across multiple tunnels. IPv6 is tunneled in IPv4. Additional tunneling techniques, such as, IPsec and VLAN tagging may be selected by the APN, but are configured in the GGSN independently from the APN.
- **QoS**: IPv4 header ToS handling. Traffic rate limits for different 3GPP traffic classes. Mapping of R98 QoS attributes to work around particular handset defections. Dynamic QoS renegotiation (described elsewhere).

After an APN is determined by the GGSN, the subscriber may be authenticated/authorized with an AAA server. The GGSN allows the AAA server to return VSAs (Vendor Specific Attributes) that override any/all of the APN configuration. This allows different subscriber tier profiles to be configured in the AAA server, and passed to the GGSN during subscriber authentication/authorization.

The GGSN's Virtual APN feature allows the carrier to use a single APN to configure differentiated services. The APN that is supplied by the SGSN is evaluated by the GGSN in conjunction with multiple configurable parameters. Then the GGSN selects an APN configuration based on the supplied APN and those configurable parameters. The configurable parameters are: the access gateway IP address, bearer access service name, charging characteristics (CC)-profile index, subscribers within an MSISN range, subscriber's mcc/mnc, whether the subscriber is home/visiting/roaming, subscriber's domain name and the radio access (RAT) type including gen, geran, hspa, eutran, utran, and wlan.

Important For more information on APN configuration, refer *APN Configuration* in *GGSN Service Configuration*.

APN AMBR Support

The APN-AMBR (Aggregated Maximum Bit Rate) limits the aggregare bit rate that can be expected to be provided across all non-GBR PDP contexts/bearers and across all PDN connections of the same APN. APN-AMBR value is transferred over the Gn and Gx interface.

APN-AMBR is enforced at GGSN to rate limit the traffic across all non-GBR bearers. If APN-AMBR is not supported by SGSN in the network, GGSN derives APN-AMBR AVP to be sent to PCRF in CCR-I from MBR of the initial PDP context received from SGSN. When MBR of any PDP context gets changed by SGSN, GGSN locally authorizes requested MBR unless it is higher than APN-AMBR. In such case, GGSN can either lower the requested MBR or reject it based on local configuration.

Traffic Policing

The Cisco GGSN offers a variety of traffic conditioning and bandwidth management capabilities. These tools enable usage controls to be applied on a per-subscriber, per-EPS bearer or per-PDN/APN basis. It is also possible to apply bandwidth controls on a per-APN AMBR capacity. These applications provide the ability to inspect and maintain state for user sessions or Service Data Flows (SDFs) within them using shallow L3/L4 analysis or high touch deep packet inspection at L7. Metering of out-of-profile flows or sessions can result in packet discards or reducing the DSCP marking to Best Effort priority.

Backup and Recovery of Key KPI Statistics

Before the Backup and Recovery of Key KPI Statistics feature was implemented, statistics were not backed up and could not be recovered after a SessMgr task restart. Due to this limitation, monitoring the KPI was a problem as the GGSN, P-GW, SAEGW, and S-GW would lose statistical information whenever task restarts occurred.

KPI calculation involves taking a delta between counter values from two time intervals and then determines the percentage of successful processing of a particular procedure in that time interval. When a SessMgr crashes and then recovers, the GGSN, P-GW, SAEGW, and S-GW lose the counter values - they are reset to zero. So, the KPI calculation in the next interval will result in negative values for that interval. This results in a dip in the graphs plotted using the KPI values, making it difficult for operations team to get a consistent view of the network performance to determine if there is a genuine issue or not.

This feature makes it possible to perform reliable KPI calculations even if a SessMgr restart occurs.

Important For more information on Backup and Recovery of Key KPI Statistics, refer to the *Backup and Recovery of Key KPI Statistics* chapter in this guide.

Bulk Statistics Support

The system's support for bulk statistics allows operators to choose to view not only statistics that are of importance to them, but also to configure the format in which it is presented. This simplifies the post-processing of statistical data since it can be formatted to be parsed by external, back-end processors.

When used in conjunction with the Web Element Manager, the data can be parsed, archived, and graphed.

The system can be configured to collect bulk statistics (performance data) and send them to a collection server (called a receiver). Bulk statistics are statistics that are collected in a group. The individual statistics are grouped by schema.

The following schemas are supported for GGSN service:

- **System**: Provides system-level statistics
- **Card**: Provides card-level statistics
- **Port**: Provides port-level statistics
- **FA**: Provides FA service statistics
- **HA**: Provides HA service statistics
- **IP Pool**: Provides IP pool statistics
- **PPP**: Provides Point-to-Point Protocol statistics
- **GTPC**: Provides GPRS Tunneling Protocol - Control message statistics
- **GTPP**: Provides GPRS Tunneling Protocol - Prime message statistics
- **APN**: Provides Access Point Name statistics
- **RADIUS**: Provides per-RADIUS server statistics
- **ECS**: Provides Enhanced Charging Service Statistics

The system supports the configuration of up to 4 sets (primary/secondary) of receivers. Each set can be configured with to collect specific sets of statistics from the various schemas. Statistics can be pulled manually from the system or sent at configured intervals. The bulk statistics are stored on the receiver(s) in files.

The format of the bulk statistic data files can be configured by the user. Users can specify the format of the file name, file headers, and/or footers to include information such as the date, system host name, system uptime, the IP address of the system generating the statistics (available for only for headers and footers), and/or the time that the file was generated.

When the Web Element Manager is used as the receiver, it is capable of further processing the statistics data through XML parsing, archiving, and graphing.

The Bulk Statistics Server component of the Web Element Manager parses collected statistics and stores the information in the PostgreSQL database. If XML file generation and transfer is required, this element generates the XML output and can send it to a Northbound NMS or an alternate bulk statistics server for further processing.

Additionally, if archiving of the collected statistics is desired, the Bulk Statistics server writes the files to an alternative directory on the server. A specific directory can be configured by the administrative user or the default directory can be used. Regardless, the directory can be on a local file system or on an NFS-mounted file system on the Web Element Manager server.

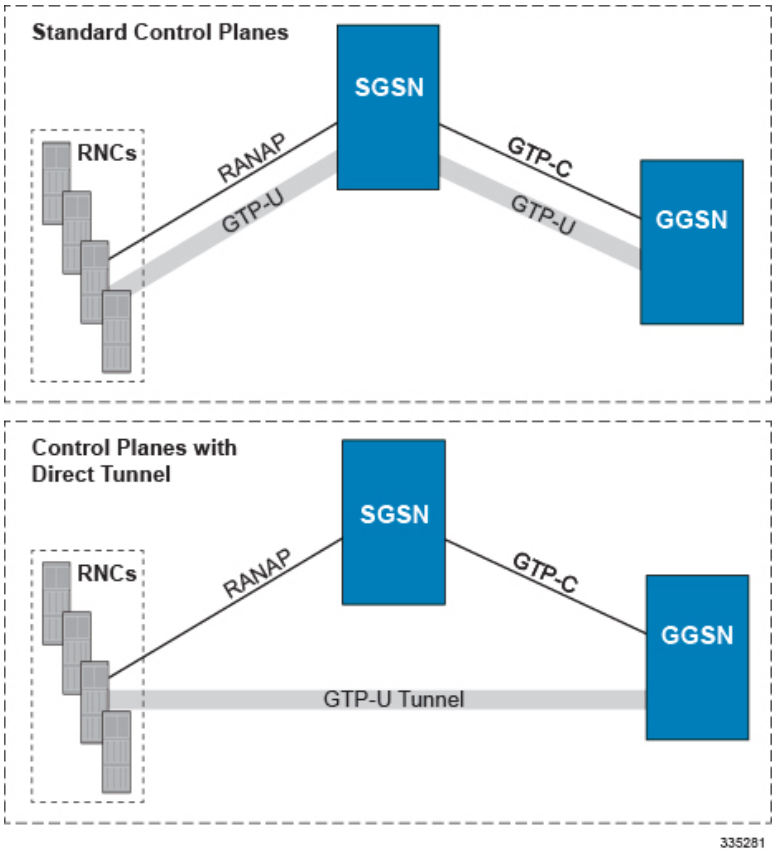
Direct Tunnel Support

Direct tunnel improves the user experience (e.g. expedited web page delivery, reduced round trip delay for conversational services, etc.) by eliminating SGSN tunnel 'switching' latency from the user plane. An additional advantage of Direct Tunnel from an operational and capital expenditure perspective is that direct tunnel optimizes the usage of user plane resources by removing the requirement for user plane processing on the SGSN.

The Direct Tunnel architecture allows the establishment of a direct user plane tunnel between the RAN and the GGSN, bypassing the SGSN. The SGSN continues to handle the control plane signalling and typical makes the decision to establish Direct Tunnel at PDP Context Activation. A Direct Tunnel is achieved at PDP context activation by the SGSN establishing a user plane (GTP-U) tunnel directly between RNC and GGSN (using an Update PDP Context Request towards the GGSN).

The following figure illustrates the working of Direct Tunnel between RNC and GGSN.

Figure 5: Direct Tunnel Support in GGSN



A major consequence of deploying Direct Tunnel is that it produces a significant increase in control plane load on both the SGSN and GGSN components of the packet core. It is therefore of paramount importance to a wireless operator to ensure that the deployed GGSNs are capable of handling the additional control plane loads introduced of part of Direct Tunnel deployment. The Cisco GGSN and SGSN offers massive control plane transaction capabilities, ensuring system control plane capacity will not be a capacity limiting factor once Direct Tunnel is deployed.

DHCP Support

Dynamic IP address assignment to subscriber IP PDP contexts using the Dynamic Host Control Protocol as defined by the following standards:

- RFC 2131, Dynamic Host Configuration Protocol
- RFC 2132, DHCP Options and BOOTP Vendor Extensions

As described in the PDP Context Support section of this document, the method by which IP addresses are assigned to a PDP context is configured on an APN-by-APN basis. Each APN template dictates whether it will support static or dynamic addresses.

Dynamically assigned IP addresses for subscriber PDP contexts can be assigned through the use of DHCP.

The system can be configured to support DHCP using either of the following mechanisms:

- **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.
- **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.

Important For more information on DHCP service configuration, refer *DHCP Configuration* section in *GGSN Service Configuration* chapter.

DHCPv6 Support

The Dynamic Host Configuration Protocol (DHCP) for IPv6 enables the DHCP servers to pass the configuration parameters such as IPv6 network addresses to IPv6 nodes. It offers the capability of allocating the reusable network addresses and additional configuration functionality automatically.

The DHCPv6 support does not just feature the address allocation, but also fulfills the requirements of Network Layer IP parameters. Apart from these canonical usage modes, DHCPv6's Prefix-Delegation (DHCP-PD) has also been standardized by 3GPP (Rel 10) for "network-behind-ue" scenarios.

GGSN manages IPv6 prefix life-cycle just like it manages IPv4 addresses, thus it is responsible for allocation, renew, and release of these prefixes during the lifetime of a session. IPv6 Prefix is mainly for the UE's session attached to GGSN, where as delegated prefix is for network/devices behind UE. For IPv6 prefixes. GGSN may be obtained from either local-pool, AAA (RADIUS/DIAMETER) or external DHCPv6 servers based on respective configuration. For Delegated IPv6 Prefix allocation, GGSN obtained it from external DHCPv6 servers based on configuration.

Unicast Address Support Feature: The IPv6 prefix delegation for the requested UE is either allocated locally or from an external DHCPv6 server by P-GW, GGSN, SAEGW based on configuration at these nodes. These DHCP messages are sent to the external DHCPv6 server using multicast address as destination address. In networks where there are large number of P-GW servers, but less number of DHCP servers, the DHCPv6 messages with multicast address have to travel through the entire network, increasing load on the network. The Unicast address support feature enables the operator to send all DHCPv6 messages on unicast address towards external server using configured address of DHCPv6 server in a DHCP service. This feature is CLI controlled and the operator needs to configure a CLI to support for client unicast operation to the DHCP Server.

The following requirements for DHCPv6 support is available:

- RFC 3315, Dynamic Host Configuration Protocol for IPv6 (Basic DHCPv6)
- RFC 3633, prefix delegation mechanism

Important For more information on DHCPv6 service configuration, refer *DHCPv6 Configuration* section in *GGSN Service Configuration* chapter.

DHCPv6 Prefix Delegation

GGSN supports DHCPv6 Prefix Delegation.

DHCPv6 prefix delegation is required to support deployment models where multiple IPv6 prefixes can be delegated to the UE and which can be further subnetted by the UE and assigned to the links in its internal network. UE will act as a IPv6 router here and will be responsible for just prefix delegation or for prefix delegation along with address assignment and other configuration information. DHCPv6 prefix delegation will allow prefixes to be delegated to the UE independent of bearer establishment and thus without requiring any changes to the mobility signaling protocols.

Important For more information on DHCPv6 prefix delegation configuration, refer *GGSN Service Configuration* chapter.

DSCP Marking

Provides support for more granular configuration of DSCP marking.

For different Traffic class, the GGSN supports per-GGSN service and per-APN configurable DSCP marking for Uplink and Downlink direction based on Allocation/Retention Priority in addition to the current priorities.

The GGSN supports configurable DSCP marking of the outer header of a GTP-U tunnel packet based on a QCI/THP table for the Gn/Gp interfaces. This feature allows configuring DSCP marking table on a per APN basis.

In order to be backward compatible with old configuration, if a DSCP marking table is associated with GGSN service and not with the APN, then the one in GGSN service will be used. If table is associated in both GGSN service and APN, then the one on APN will take precedence.

Table 1: Default DSCP Value Matrix

Allocation Priority	1	2	3
Traffic Handling Priority			
1	ef	ef	ef
2	af21	af21	af21
3	af21	af21	af21

RAT-Type based DSCP Marking

With 21.6 and later releases, operators can perform DSCP marking on gateways such as GGSN, P-GW, and SAE-GW, based on RAT-Type. It allows the operator to configure different QoS services and to optimize traffic based on the RAT-Type: EUTRAN, GERAN, and UTRAN.

RAT-Type based DSCP marking includes the following:

- Support for all QCI and ARP values.
- Support for Standard and non-Standard QCIs.
- If a particular RAT-Type is not configured, the DSCP marking functionality is applied to all RAT-Type.

- Applicable for Virtual APNs.
- During Inter-RAT hand-offs, DSCP marking is based on the RAT-Type of the current hand-off.
- DSCP marking per RAT-Type is only applicable for user data traffic and not for control traffic (GTP-C packets).

Important Backward compatibility is maintained for existing DSCP marking and IP-ToS functionalities.

IMS Emergency Session Support

Emergency bearer services are provided to support IMS emergency sessions. Emergency bearer services are functionalities provided by the serving network when the network is configured to support emergency services. These services are provided to normal attached UEs and depending on local regulation, to UEs that are in limited service state. Receiving emergency services in limited service state does not require a subscription. Depending on local regulation and an operator's policy, the SGSN may allow or reject an emergency attach request for UEs in limited service state.

Following four different behaviors of emergency bearer support are included:

- Valid UEs Only: No limited service state UEs are supported in the network. Only normal UEs that have a valid subscription, are authenticated and authorized for PS service in the attached location are allowed. It is not expected that a normal UE would perform an emergency attach. Normal UEs should be attached to the network and then perform a PDN Connection Request when an IMS emergency session is detected by the UE.
- Authenticated UEs Only: These UEs must have a valid IMSI. These UEs are authenticated and may be in limited service state due to being in a location that they are restricted from service. A UE that cannot be authenticated will be rejected.
- IMSI Required, Authentication Optional: These UEs must have an IMSI. If authentication fails, the UE is granted access and the unauthenticated IMSI retained in the network for recording purposes. The IMEI is used in the network as the UE identifier. IMEI only UEs will be rejected (e.g., UICCless UEs).
- All UEs: Along with authenticated UEs, this includes UEs with an IMSI that cannot be authenticated and UEs with only an IMEI. If an unauthenticated IMSI is provided by the UE, the unauthenticated IMSI is retained in the network for recording purposes. The IMEI is used in the network to identify the UE.

Framed-Route Attribute Support

The Framed-Route attribute provides routing information to be configured for the user on the network access server (NAS). The Framed-Route information is returned to the RADIUS server in the Access-Accept message.

Mobile Router enables a router to create a PDN Session which the GGSN authorizes using RADIUS server. The RADIUS server authenticates this router and includes a Framed-Route attribute in the access-accept response packet. Framed-Route attribute also specifies the subnet routing information to be installed in the GGSN for the "mobile router." If the GGSN receives a packet with a destination address matching the Framed-Route, the packet is forwarded to the mobile router through the associated PDN Session. For more information, see *Routing Behind the Mobile Station on an APN* chapter.

Generic Corporate APN

Any operator may not be aware of the IP address that a corporation may assign to subscribers through AAA or DHCP and the traffic is sent from the GGSN to the corporation over a tunnel, this feature allows the operator to terminate such users.

Normally the GGSN validates the IP address assigned by RADIUS, however this feature removes the need for this, but does assume that the subscriber traffic is forwarded out of the GGSN through a tunnel.

When the IP address is statically assigned, i.e., either MS provided, RADIUS provided or DHCP provided, the IP address validation is not performed if the address policy is set to disable address validation.

ACL and Policy Group Info processing would still be performed.

Additionally, there is support for Virtual APN selection based on RADIUS VSA returned during Authentication.

The existing Virtual APN selection mechanism is being enhanced to select the Virtual APN based on RADIUS VSA returned during authentication.

The selected V-APN may further require AAA authentication (and accounting) with its own servers.

GnGp Handoff Support

In LTE deployments, the smooth handover support is required between 3G/2G and LTE networks, and Evolved Packet Core (EPC) is designed to be a common packet core for different access technologies. Since support for seamless handover across different access technologies is basic requirement for EPC, PGW needs to support handovers as user equipment (UE) moves across different access technologies.

Cisco's PGW supports inter-technology mobility handover between 4G and 3G/2G access. Interworking is supported between the 4G and 2G/3G SGSNs which provide only Gn and Gp interfaces but no S3, S4 or S5/S8 interfaces. Therefore these Gn/Gp SGSNs provide no functionality introduced specifically for the evolved packet system (EPS) or for interoperation with the E-UTRAN. These handovers are supported only with a GTP-based S5/S8 and PGW supports handovers between GTPv2 based S5/S8 and GTPv1 based Gn/Gp tunneled connections. In this scenario, the PGW works as an IP anchor for the EPC.

Important Handover is supported for IPv4, IPv6, and IPv4v6 PDN connections

GnGp Handoff in Non-Roaming Scenario

Depending on the existing deployments, PLMN may operate Gn/Gp 2G and/or 3G SGSNs as well as MME and SGW for E-UTRAN access. In such cases, the PGW works as an anchor point for both GERAN/UTRAN and E-UTRAN access. Depending on APN, MME/SGSN select a PGW for each call.

In the home network (non-roaming) when UE firstly attaches to the E-UTRAN, it sets up a PDN connection with some EPS bearers and when the UE moves to Gn/Gp SGSN served GERAN/UTRAN access, handover is initiated from MME to the Gn/Gp SGSN. Gn/Gp SGSN then notifies PGW (with GGSN functionality) about the handoff of EPS bearers. During this handover, each EPS bearer in the PDN connection is converted into a PDP context.

The other way, when the UE first attaches on to Gn/Gp SGSN served GERAN/UTRAN, it sets up PDP contexts, and when the UE moves to E-UTRAN access, handover is initiated from Gn/Gp SGSN to the MME. MME then notifies the PGW (through SGW) about the handoff of PDP contexts to the E-UTRAN access. During this handover, all PDP contexts sharing the same APN and IP address are converted to EPS bearers

of same PDN connection. Here one of the PDP context is selected as a Default bearer and rest of the PDP contexts are designated as Dedicated bearers.

GnGp Handoff in Roaming Scenario

In the roaming scenario, the vPLMN (Virtual PLMN) operates Gn/Gp 2G and/or 3G SGSNs as well as MME and SGW for E-UTRAN access and hPLMN (Home PLMN) operates a PGW. Other remaining things work as in non-roaming scenario.

Important For more information on configuration of Gn-Gp Handoff, refer the *Gn-Gp Support Configuration* section of *GGSN Service Configuration Procedures* chapter.

GTPP Support

Support for the GPRS Tunnelling Protocol Prime (GTPP) in accordance with the following standards:

- **3GPP TS 32.015 v3.12.0 (2003-12)**: 3rd Generation Partnership project; Technical Specification Group Services and System Aspects; Telecommunication Management; Charging and billing; GSM call and event data for the Packet Switched (PS) domain (Release 1999) for support of Charging on GGSN
- **3GPP TS 32.215 v5.9.0 (2005-06)**: 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Telecommunication management; Charging management; Charging data description for the Packet Switched (PS) domain (Release 4)
- **3GPP TS 29.060 v7.9.0 (2008-09)**: Technical Specification; 3rd Generation Partnership Project; Technical Specification Group Core Network; General Packet Radio Service (GPRS); GPRS Tunnelling Protocol (GTP) across the Gn and Gp interface (Release 6)

The system supports the use of GTPP for PDP context accounting. 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. As specified by the standards, a CDR is not generated when a session starts. 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. For interim accounting, STOP/START pairs are sent based on configured triggers.

GTPP version 2 is always used. 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. All CDR fields are R4.

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. They must always be provided by the SGSN for GTPv1 requests for primary PDP contexts. If they are not provided for secondary PDP contexts, the GGSN re-uses those from the primary.

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. GGSN charging characteristics consist of a profile index and behavior settings. The profile indexes specify the criteria for closing accounting records based specific criteria.

Important For more information on GTPP group configuration, refer *GTPP Accounting Configuration* in *GGSN Service Configuration* chapter.

Host Route Advertisement

When subscribers are assigned IP addresses from RADIUS or HLR, yet are allowed to connect to multiple GGSNs through the use of DNS round robin or failover, the IP addresses of the subscribers can be advertised on a per user (host) basis to the Gi network using dynamic routing, thereby providing IP reachability to these users.

IP address pools are configured on the GGSN for many reasons, although one of them is so that the pool subnets can be automatically advertised to the network. These are connected routes and are advertised for all non-tunneling pools.

A configuration **explicit-route-advertise** is provided to the IP pool configuration and when this option is enabled, the subnet(s) of the pool are not added to routing table and routing protocols like OSPF and BGP do not know of these addresses and hence do not advertise the subnet(s).

As calls come up, and addresses from this pool (with the "explicit-route-advertise" flag) are used, the assigned addresses are added to the routing table and these addresses can be advertised by OSPF or BGP through the network or the "redistribute connected" command.

Example

A subscriber connecting to GGSN A with an IP address from a pool P1 will be assigned the IP address and the routing domain will be updated with the host route. When a subscriber connects to GGSN B with an IP address from the same pool, the subscriber will be assigned the requested IP address and the routing domain will then learn its host route. When the subscriber disconnects, the route is removed from the routing table and the routing domain is updated.

The explicit-route-advertise option can be applied and removed from the pool at any time and the routing tables are updated automatically.

The overlap and resource pool behavior does not change therefore it does not make sense to configure an overlap/resource pool with the "explicit-route-advertise" option.

IP Policy Forwarding

IP Policy Forwarding enables the routing of subscriber data traffic to specific destinations based on configuration. This functionality can be implemented in support of enterprise-specific applications (i.e. routing traffic to specific enterprise domains) or for routing traffic to back-end servers for additional processing.

The system can be configured to automatically forward data packets to a predetermined network destination. This can be done in one of three ways:

- **IP Pool-based Next Hop Forwarding** - Forwards data packets based on the IP pool from which a subscriber obtains an IP address.
- **ACL-based Policy Forwarding** - Forwards data packets based on policies defined in Access Control Lists (ACLs) and applied to contexts or interfaces.
- **Subscriber specific Next Hop Forwarding** - Forwards all packets for a specific subscriber.

The simplest way to forward subscriber data is to use IP Pool-based Next Hop Forwarding. An IP pool is configured with the address of a next hop gateway and data packets from all subscribers using the IP pool are forward to that gateway.

Subscriber Next Hop forwarding is also very simple. In the subscriber configuration a nexthop forwarding address is specified and all data packets for that subscriber are forwarded to the specified nexthop destination.

ACL-based Policy Forwarding gives you more control on redirecting data packets. By configuring an Access Control List (ACL) you can forward data packets from a context or an interface by different criteria, such as; source or destination IP address, ICMP type, or TCP/UDP port numbers.

ACLs are applied first. If ACL-based Policy Forwarding and Pool-based Next Hop Forwarding or Subscriber are configured, data packets are first redirected as defined in the ACL, then all remaining data packets are redirected to the next hop gateway defined by the IP pool or subscriber profile.

Important For more information on IP Policy Forwarding configuration, refer *Policy Forwarding* in this guide.

IP Header Compression - Van Jacobson

Implementing IP header compression provides the following benefits:

- Improves interactive response time
- Allows the use of small packets for bulk data with good line efficiency
- Allows the use of small packets for delay sensitive low data-rate traffic
- Decreases header overhead
- Reduces packet loss rate over lossy links

The system supports the Van Jacobson (VJ) IP header compression algorithms by default for subscriber traffic.

The VJ header compression is supported as per RFC 1144 (CTCP) header compression standard developed by V. Jacobson in 1990. It is commonly known as VJ compression. It describes a basic method for compressing the headers of IPv4/TCP packets to improve performance over low speed serial links.

By default IP header compression using the VJ algorithm is enabled for subscribers. You can also turn off IP header compression for a subscriber.

Important For more information on IP header compression support, refer *IP Header Compression* in this guide.

IPv6 Support

Native IPv6 support allows for the configuration of interfaces/routes with IPv6 (128 bit) addressing. The increased address space allows for future subscriber growth beyond what is currently possible in IPv4. Native IPv6 support on the Gi interface allows support for packets coming from or destined to a mobile over the Gi interface. IPv6 address assignment is supported from a dynamic or static pool via standard 3GPP attributes. The GGSN can communicate using DIAMETER as the transport protocol for Gx to the AAA. Overlapping address space or resource pools are supported if they are in different VPNs. The VPN subsystem is responsible

for the configuration and recovery of IP interfaces and routes. IP resources are grouped into separate routing domains know as contexts. The VPN subsystem creates and maintains each context and the resources associated with them. The existing IPv4 model of interface and route notification will be extended to support IPv6.

This feature allows IPv6 subscribers to connect via the GPRS/UMTS infrastructure in accordance with the following standards:

- RFC 2460: Internet Protocol, Version 6 (IPv6) Specification
- RFC 2461: Neighbor Discovery for IPv6
- RFC 2462: IPv6 Stateless Address Autoconfiguration
- RFC 3314: Recommendations for IPv6 in 3GPP Standards
- RFC 3316: Internet Protocol Version 6 (IPv6) for Some Second and Third Generation Cellular Hosts
- RFC 3056: Connection of IPv6 domains via IPv4 clouds
- 3GPP TS 23.060: General Packet Radio Service (GPRS) Service description
- 3GPP TS 27.060: Mobile Station Supporting Packet Switched Services
- 3GPP TS 29.061: Interworking between the Public Land Mobile Network (PLMN) supporting Packet Based Services and Packet Data Networks (PDN)

IP version 6 is enhanced version of IP version 4 with following modifications:

- Expanded addressing capabilities with 128 bit for address as compared to 32 bits in IPv4.
- Header format simplification
- Improved support of extensions and options
- Flow labeling capability
- Authentication and Privacy capabilities

IPv6 Neighbor Discovery protocol is used to dynamically discover the directly attached devices on IPv6 Interfaces. It facilitates the mapping of MAC addresses to IPv6 Addresses. The GGSN supports a subset of IPv6 Neighbor Discovery as defined by RFC 2461, including the following:

- The GGSN uses IPv6 Neighbor Discovery to learn the Ethernet link-layer addresses of the directly connected next-hop gateway.
- The GGSN supports configuration of the static IPv6 neighbor (next-hop gateway).
- Link-local addresses will be automatically added to Ethernet type interfaces.
- The GGSN performs Unsolicited Neighbor Advertisement on line card switchover.
- The GGSN will reply to neighbor discovery requests for the node's IPv6 addresses.

ICMPv6 is a protocol for IPv6 networks to allow error reporting and check connectivity via echo messages. The GGSN supports a subset of ICMPv6 as defined by [RFC-4443]. The GGSN replies to the link-local, configured IP address, and the all-hosts IP address.

Native IPv6 Routing allows the forwarding of IPv6 packets between IPv6 Networks. The forwarding lookup is based on a longest prefix match of the destination IPv6 address. The GGSN supports configuration of IPv6 routes to directly attached next hops via an IPv6 Interface.

Important Native IPv6 is only available on the ASR 5500 or higher platform.

MPLS Forwarding with LDP

Multi Protocol Label Switching (MPLS) is an operating scheme or a mechanism that is used to speed up the flow of traffic on a network by making better use of available network paths. It works with the routing protocols like BGP and OSPF and therefore it is not a routing protocol.

It generates a fixed-length label to attach or bind with the IP packet's header to control the flow and destination of data. The binding of the labels to the IP packets is done by the label distribution protocol (LDP). All the packets in a forwarding equivalence class (FEC) are forwarded by a label-switching router (LSR) which is also called an MPLS node. The LSR uses the LDP in order to signal its forwarding neighbors and distribute its labels for establishing a label switching path (LSP).

In order to support the increasing number of corporate APNs which have a number of different addressing models and requirements, MPLS is deployed to fulfill at least following two requirements:

- The corporate APN traffic must remain segregated from other APNs for security reasons.
- Overlapping of IP addresses in different APNs.

When deployed, MPLS backbone automatically negotiates the routes using the labels binded with the IP packets. Cisco GGSN as an LSR learns the default route from the connected provider edge (PE) while the PE populates its routing table with the routes provided by the GGSN.

Overlapping IP Address Pool Support

Overlapping IP Address Pools provides a mechanism for allowing operators to more flexibly support multiple corporate VPN customers with the same private IP address space without the expensive investments in physically separate routers, or expensive configurations using virtual routers.

The system supports two type of overlapping pools: resource and overlap. Resource pools are designed for dynamic assignment only, and use a VPN tunnel, such as a GRE tunnel, to forward and receive the private IP addresses to and from the VPN. Overlapping type pools can be used for both dynamic and static, and use VLANs and a next hop forwarding address to connect to the VPN customer.

To forward downstream traffic to the correct PDP context, the GGSN uses either the GRE tunnel ID, or the VLAN ID to match the packet. When forwarding traffic upstream, the GGSN uses the tunnel and forwarding information in the IP pool configuration, so overlapping pools must be configured in the APN for this feature to be used.

When a PDP context is created, the IP addresses is either assigned from the IP pool, in this case the forwarding rules are also configured into the GGSN at this point. If the address is assigned statically, when the GGSN confirms the IP address from the pool configured in the APN, the forwarding rules are also applied.

The GGSN can scale to as many actual overlapping pools as there are VLAN interfaces per context, and there can be multiple contexts per GGSN, or when using resource then the limit is the number of IP pools. This scalability allows operators, who wish to provide VPN services to customers using the customer's private IP address space, need not be concerned about escalating hardware costs, or complex configurations.

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

Caution The IP pools limit is 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.

Important For more information on IP pool overlapping configuration, refer *VLANs* in *System Administration Guide*.

PDP Context Support

Support for subscriber primary and secondary Packet Data Protocol (PDP) contexts in accordance with the following standards:

- **3GPP TS 23.060 v7.4.0 (2007-9)**: 3rd Generation Partnership project; Technical Specification Group Services and System Aspects; General Packet Radio Service (GPRS); Service description (Release 1999) as an additional reference for GPRS/UMTS procedures
- **3GPP TS 29.061 v7.6.0 (2008-09)**: 3rd Generation Partnership Project; Technical Specification Group Core Network; Packet Domain; Interworking between the Public Land Mobile Network (PLMN) supporting Packet Based Services and Packet Data Networks (PDN) (Release 4)

PDP context processing is based on the APN that the subscriber is attempting to access. Templates for all of the possible APNs that subscribers will be accessing must be configured within the system. Up to 2,048 APNs can be configured on the system.

Each APN template consists of parameters pertaining to how PDP contexts are processed such as the following:

- Type (IPv4, IPv6, IPv4v6, and/or PPP)
- Accounting protocol (GTPP or RADIUS)
- Authentication protocol (CHAP, MSCHAP, PAP, Allow-NOAUTH, IMSI-based, MSISDN-based)
- Charging characteristics (use SGSN-supplied or use configured)
- IP address allocation method (static or dynamic)
- PDP Context timers
- Quality of Service

A total of 11 PDP contexts are supported per subscriber. These could be all primaries, or 1 Primary and 10 secondaries or any combination of primary and secondary. Note that there must be at least one primary PDP context in order for secondaries to come up.

Per APN Configuration to Swap out Gn to Gi APN in CDRs

In order to allow for better correlation of CDRs with the network or application used by the subscriber, a configuration option has been added to the GGSN replace the Gn APN with the Gi (virtual) APN in emitted G-CDRs.

When virtual APNs are used, the operator can specify via EMS or a configuration command that the Gi APN should be used in the "Access Point Name Network Identifier" field of emitted G-CDRs, instead of the Gn APN.

Peer GTP Node Profile Configuration Support

Using this configuration, operator can also control some parameters associated with the configured SGSN; like RAT type. This would be taken from configuration, if CPC request doesn't have RAT type.

The GGSN service supports the peer profile to allow flexible profile based configuration to accommodate growing requirements of customizable parameters with default values and actions for peer nodes of GGSN. With this feature configuration of GTPC parameters and disabling/enabling of Lawful intercept per MCC/MNC or IP address based on rules defined.

With support of this functionality the GGSN service supports the peer profile to allow flexible profile based configuration to accommodate growing requirements of customizable parameters with default values and actions for peer nodes of GGSN. With this feature configuration of GTP-C parameters and disabling/enabling of Lawful intercept per MCC/MNC or IP address based on rules can be defined.

A new framework of peer-profile and peer-map is introduced for configuration. Peer-profile configuration captures the GTP-C specific configuration and/or Lawful Intercept enable/disable configuration. GTP-C configuration covers the configuration of GTP-C retransmission (maximum number of retries and retransmission timeout) and GTP echo configuration.

Peer-map config matches the peer-profile to be applied to a particular criteria. Peer-map supports criteria like MCC/MNC (PLMN-ID) of the peer or IP-address of the peer. Peer-map can then be associated with GGSN service.

With support of this feature the Operators can configure a profile which can be applied to a specific set of peers. For example, have a different retransmission timeout for foreign peers as compared to home peers.

Important For more information on Peer GTP Node Profile configuration, refer *GGSN Service Configuration* chapter.

Port Insensitive Rule for Enhanced Charging Service

This feature allows a single host or url rule to be applied to two different addresses, one with and one without the port number appended. As adding the port to the address is optional, this means that the number of rules could be halved.

Browser applications can sometimes appended the port number to the host or url when sending the host or URL fields. RFC 2616 for example states that port should be appended but if it is omitted then 80 should be assumed.

When configuring rules to define the content, as the web browser may provide the port number, even if it is the default one of 80 for HTTP, then two of each URL are needed.

Example

```
host = www.w3.org host = www.w3.org:80orhttp url = http://213.229.187.118:80/chat/c/wel.w.wml
 http url = http://213.229.187.118/chat/c/wel.w.wml
```

This feature provides a means to configure the rule such that the traffic is matched irrespective of the presence of a port number.

A new configurable has been added to the rulebase configuration that will ignore the port numbers embedded in the application headers of HTTP, RTSP, SIP, and WSP protocols.

When this feature is enabled, a single rule, such as "host = www.w3.org" would be matched even if the port number is appended and in this case the host field has the value www.w3.org:80, thereby cutting the number of rules needed by up to a half.

Important For more information on enhanced charging service, refer *Enhanced Charging Service Administration Guide*.

P-CSCF Discovery Support

P-CSCF discovery support ensures the parity between PGW and GGSN implementation for deriving P-CSCF addresses from the various interfaces and local configurations. Following is the order of sequence in which P-CSCF address is tobe fetched and returned subsequently:

- P-CSCF info from S6b FQDN based DNS query
- P-CSCF info from Config FQDN based DNS query
- P-CSCF info from IMSA configured table
- P-CSCF info from APN config

P-CSCF Discovery is performed inline with respect to the Call establishment Handoff Procedure and refers to the stored FQDN information. In addition to the above enhancements, following points have also been supported:

- Storing of discovered P-CSCF IPv4 and IPv6 addresses
- SR/ICSR Recovery of P-CSCF IP addresses
- Persistence of FQDN information
- Persistence of P-CSCF values across gngp handoff
- Unification of the P-CSCF Address Element

Quality of Service Support

Provides operator control over the prioritization of different types of traffic.

Quality of Service (QoS) support provides internal processing prioritization based on needs, and DiffServ remarking to allow external devices to perform prioritization.

Important The feature described here is internal prioritization and DiffServ remarking for external prioritization. For additional QoS capabilities of the GGSN, refer to Features and Functionality - Optional Enhanced Feature Software, on page 32.

External prioritization (i.e., the value to use for the DiffServ marking) is configured for the uplink and downlink directions. In the uplink direction, each APN is configurable for the DiffServ ToS value to use for each of the 3GPP traffic classes. Alternatively, you can configure "pass-through", whereby the ToS value will pass through unchanged.

In the downlink direction, the ToS value of the subscriber packet is not changed, but you can configure what to use for the ToS value of the outer GTP tunnel. The value for ToS is configurable for each of the 3GPP traffic classes. In addition, the connections between the GGSN and one or more SGSNs can be configured as a "GGSN Service", and different values for ToS for the same 3GPP traffic class may be configured for different GGSN Services.

RADIUS Support

Provides a mechanism for performing authorization, authentication, and accounting (AAA) for subscriber PDP contexts based on the following standards:

- RFC-2618, RADIUS Authentication Client MIB, June 1999
- RFC-2620, RADIUS Accounting Client MIB, June 1999
- RFC-2865, Remote Authentication Dial In User Service (RADIUS), June 2000
- RFC-2866, RADIUS Accounting, June 2000
- RFC-2867, RADIUS Accounting Modifications for Tunnel Protocol Support, June 2000
- RFC-2868, RADIUS Attributes for Tunnel Protocol Support, June 2000
- RFC-2869, RADIUS Extensions, June 2000

The Remote Authentication Dial-In User Service (RADIUS) protocol is used to provide AAA functionality for subscriber PDP contexts. (RADIUS accounting is optional since GTPP can also be used.)

Within context contexts configured on the system, there are AAA and RADIUS protocol-specific parameters that can be configured. The RADIUS protocol-specific parameters are further differentiated between RADIUS Authentication server RADIUS Accounting server interaction.

Among the RADIUS parameters that can be configured are:

- **Priority**: Dictates the order in which the servers are used allowing for multiple servers to be configured in a single context.
- **Routing Algorithm**: Dictate the method for selecting among configured servers. The specified algorithm dictates how the system distributes AAA messages across the configured AAA servers for new sessions. Once a session is established and an AAA server has been selected, all subsequent AAA messages for the session will be delivered to the same server.

In the event that a single server becomes unreachable, the system attempts to communicate with the other servers that are configured. The system also provides configurable parameters that specify how it should behave should all of the RADIUS AAA servers become unreachable.

The system provides an additional level of flexibility by supporting the configuration RADIUS server groups. This functionality allows operators to differentiate AAA services for subscribers based on the APN used to facilitate their PDP context.

In general, 128 AAA Server IP address/port per context can be configured on the system and it selects servers from this list depending on the server selection algorithm (round robin, first server). Instead of having a single list of servers per context, this feature provides the ability to configure multiple server groups. Each server group, in turn, consists of a list of servers.

This feature works in following way:

- All RADIUS authentication/accounting servers configured at the context-level are treated as part of a server group named "default". This default server group is available to all subscribers in that context through the realm (domain) without any configuration.
- It provides a facility to create "user defined" RADIUS server groups, as many as 399 (excluding "default" server group), within a context. Any of the user defined RADIUS server groups are available for assignment to a subscriber through the APN configuration within that context.

Since the configuration of the APN can specify the RADIUS server group to use as well as IP address pools from which to assign addresses, the system implements a mechanism to support some in-band RADIUS server implementations (i.e. RADIUS servers which are located in the corporate network, and not in the operator's network) where the NAS-IP address is part of the subscriber pool. In these scenarios, the GGSN supports the configuration of the first IP address of the subscriber pool for use as the RADIUS NAS-IP address.

For more information, refer to the *AAA Interface Administration and Reference*.

RADIUS VLAN Support

VPN customers often use private address space which can easily overlap with other customers. The subscriber addresses are supported with overlapping pools which can be configured in the same virtual routing context.

This feature now allows Radius Server and NAS IP addresses to also overlapping without the need to configure separate contexts, thereby simplifying APN and RADIUS configuration and network design.

This feature now allows Radius Server and NAS IP addresses to also overlapping without the need to configure separate contexts, thereby simplifying APN and RADIUS configuration and network design.

This feature supports following scenarios to be defined in the same context:

- Overlapping RADIUS NAS-IP address for various RADIUS server groups representing different APNs.
- Overlapping RADIUS server IP address for various RADIUS servers groups.

Previously, the above scenarios were supported, albeit only when the overlapping addresses were configured in different contexts. Moreover a static route was required in each context for IP connectivity to the RADIUS server.

The new feature utilizes the same concept as overlapping IP pools such that every overlapping NAS-IP address is giving a unique next-hop address which is then bound to an interface that is bound to a unique VLAN, thereby allowing the configuration to exist within the same context.

RADIUS access requests and accounting messages are forwarded to the next hop defined for that NAS-IP and it is then up to the connected router's forward the messages to the RADIUS server. The next hop address determines the interface and VLAN to use. Traffic from the server is identified as belonging to a certain NAS-IP by the port/VLAN combination.

The number of Radius NAS-IP addresses that can be configured is limited by the number of loopback addresses that can be configured.

Important For more information on VLAN support, refer *VLANs* in *System Administration Guide*.

Routing Protocol Support

The system's support for various routing protocols and routing mechanism provides an efficient mechanism for ensuring the delivery of subscriber data packets.

GGSN node supports Routing Protocol in different way to provide an efficient mechanism for delivery of subscriber data.

The following routing mechanisms and protocols are supported by the system:

- **Static Routes**: The system supports the configuration of static network routes on a per context basis. Network routes are defined by specifying an IP address and mask for the route, the name of the interface in the currant context that the route must use, and a next hop IP address.
- **Open Shortest Path First (OSPF) Protocol**: A link-state routing protocol, OSPF is an Interior Gateway Protocol (IGP) that routes IP packets based solely on the destination IP address found in the IP packet header using the shortest path first. IP packets are routed "as is", meaning they are not encapsulated in any further protocol headers as they transit the network.

  Variable length subnetting, areas, and redistribution into and out of OSPF are supported.

  OSPF routing is supported in accordance with the following standards:

  - RFC-1850, OSPF Version 2 Management Information Base, November 1995
  - RFC-2328, OSPF Version 2, April 1998
  - RFC-3101 OSPF-NSSA Option, January 2003

- **Border Gateway Protocol version 4 (BGP-4)**: The system supports a subset of BGP (RFC-1771, A Border Gateway Protocol 4 (BGP-4)), suitable for eBGP support of multi-homing typically used to support geographically redundant mobile gateways, is supported.

  EBGP is supported with multi-hop, route filtering, redistribution, and route maps. The network command is support for manual route advertisement or redistribution.

  BGP route policy and path selection is supported by the following means:

  - Prefix match based on route access list
  - AS path access-list
  - Modification of AS path through path prepend
  - Origin type
  - MED
  - Weight

- **Route Policy**: Routing policies modify and redirect routes to and from the system to satisfy specific routing needs. The following methods are used with or without active routing protocols (i.e. static or dynamic routing) to prescribe routing policy:
  - **Route Access Lists**: The basic building block of a routing policy, route access lists filter routes based upon a specified range of IP addresses.
  - **IP Prefix Lists**: A more advanced element of a routing policy. An IP Prefix list filters routes based upon IP prefixes
  - **AS Path Access Lists**: A basic building block used for Border Gateway Protocol (BGP) routing, these lists filter Autonomous System (AS) paths.
- **Route Maps**: Route-maps are used for detailed control over the manipulation of routes during route selection or route advertisement by a routing protocol and in route redistribution between routing protocols. This detailed control is achieved using IP Prefix Lists, Route Access Lists and AS Path Access Lists to specify IP addresses, address ranges, and Autonomous System Paths.
- **Equal Cost Multiple Path**: ECMP allows distribution of traffic across multiple routes that have the same cost to the destination. In this manner, throughput load is distributed across multiple paths, typically to lessen the burden on any one route and provide redundancy.

Important For more information on IP Routing configuration, refer *Routing* in *System Administration Guide*.

Subscriber Session Trace Support

The Subscriber Level Trace provides a 3GPP standards-based session-level trace function for call debugging and testing new functions and access terminals in an UMTS environment.

In general, the Session Trace capability records and forwards all control activity for the monitored subscriber on the monitored interfaces. This is typically all the signaling and authentication/subscriber services messages that flow when a UE connects to the access network.

The UMTS network entities like SGSN and GGSN support 3GPP standards based session level trace capabilities to monitor all call control events on the respective monitored interfaces including **Gn**, **Gi**, **Gx**, and **Gmb** interface on GGSN. The trace can be initiated using multiple methods:

- Management initiation via direct CLI configuration
- Management initiation at AAA with trace activation via authentication response messages over **Gx** reference interface
- Signaling based activation through signaling from subscriber access terminal

Important Once the trace is provisioned it can be provisioned through the access cloud via various signaling interfaces.

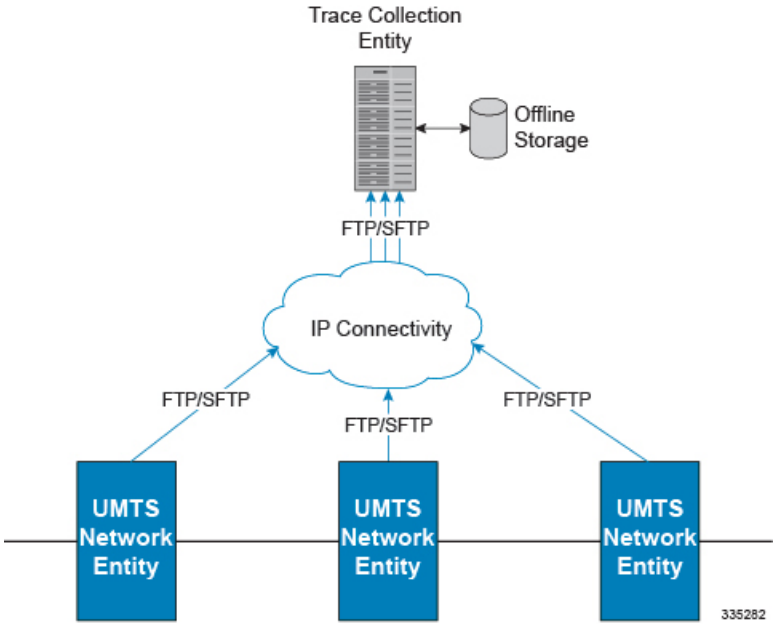
The session level trace function consists of trace activation followed by triggers. The time between the two events is treated much like Lawful Intercept where the UMTS network element buffers the trace activation

instructions for the provisioned subscriber in memory using camp-on monitoring. Trace files for active calls are buffered as XML files using non-volatile memory on the local dual redundant hard drives on the system. The Trace Depth defines the granularity of data to be traced. Six levels are defined including Maximum, Minimum and Medium with ability to configure additional levels based on vendor extensions.

Important Only Maximum Trace Depth is supported in the current release.

The following figure shows a high-level overview of the session-trace functionality and deployment scenario:

Figure 6: Session Trace Function and Interfaces



All call control activity for active and recorded sessions is sent to an off-line Trace Collection Entity (TCE) using a standards-based XML format over a FTP or secure FTP (SFTP) connection.

Note: In the current release the IPv4 interfaces are used to provide connectivity to the TCE. Trace activation is based on IMSI or IMEI.

Support of Charging Characteristics Provided by AAA Server

This feature provides the ability for operators to apply Charging Characteristics (CC) from the AAA server instead of a hard coded local profile during access authentication.

The RADIUS attribute **3GPP-Chrg-Char** can be used to get the charging characteristics from RADIUS in Access-Accept message. Accepting the RADIUS returned charging characteristic profile must be enabled per APN. The CC profile returned by AAA will override any CC provided by the SGSN, the GGSN or per APN configuration. All 16 profile behaviors can be defined explicitly or the default configuration for that profile is used.

Support of all GGSN generated causes for partial G-CDR closure

Provides more detailed eG-CDR and/or G-CDR closure causes as per 3GPP TS 32.298.

System handles the GGSN generated causes for partial closure of CDRs. It supports various type of causes including Radio Access Technology Change, MS Time Zone Change, Cell update, inter-PLMN SGSN change, PLMN id change, QoS, Routing-Area update etc.

Support of ULI/RAI Generation

User Location Information and Routing Area Identity (ULI/RAI) IEs in Create PDP Context Request message identify the Location Area for the UE. This information is passed on the interfaces like Gx, Gy, and Ga. There are circumstances when this information (ULI/RAI) does not come from SGSN, but it has to be relayed on these interfaces.

The support is provided to generate ULI/RAI based on certain CLI configurations on GGSN if it is not available from SGSN.

Threshold Crossing Alerts (TCA) Support

Thresholding on the system is used to monitor the system for conditions that could potentially cause errors or outage. Typically, these conditions are temporary (i.e high CPU utilization, or packet collisions on a network) and are quickly resolved. However, continuous or large numbers of these error conditions within a specific time interval may be indicative of larger, more severe issues. The purpose of thresholding is to help identify potentially severe conditions so that immediate action can be taken to minimize and/or avoid system downtime.

The system supports Threshold Crossing Alerts for certain key resources such as CPU, memory, IP pool addresses, etc. With this capability, the operator can configure threshold on these resources whereby, should the resource depletion cross the configured threshold, a SNMP Trap would be sent.

The following thresholding models are supported by the system:

- **Alert**: A value is monitored and an alert condition occurs when the value reaches or exceeds the configured high threshold within the specified polling interval. The alert is generated then generated and/or sent at the end of the polling interval.
- **Alarm**: Both high and low threshold are defined for a value. An alarm condition occurs when the value reaches or exceeds the configured high threshold within the specified polling interval. The alert is generated then generated and/or sent at the end of the polling interval.

Thresholding reports conditions using one of the following mechanisms:

- **SNMP traps**: SNMP traps have been created that indicate the condition (high threshold crossing and/or clear) of each of the monitored value.

  Generation of specific traps can be enabled or disabled on the chassis. Ensuring that only important faults get displayed. SNMP traps are supported in both Alert and Alarm modes.

- **Logs**: The system provides a facility called threshold for which active and event logs can be generated. As with other system facilities, logs are generated Log messages pertaining to the condition of a monitored value are generated with a severity level of WARNING

  Logs are supported in both the Alert and the Alarm models.

- **Alarm System**: High threshold alarms generated within the specified polling interval are considered "outstanding" until a the condition no longer exists or a condition clear alarm is generated. "Outstanding" alarms are reported to the system's alarm subsystem and are viewable through the Alarm Management menu in the Web Element Manager.

  The Alarm System is used only in conjunction with the Alarm model.

Important For more information on threshold crossing alert configuration, refer *Thresholding Configuration Guide*.

Virtual APN Selection

Virtual APNs allow differentiated services within a single APN.

The Virtual APN feature allows a carrier to use a single APN to configure differentiated services. The APN that is supplied by the MME is evaluated by the GGSN in conjunction with multiple configurable parameters. Then, the GGSN selects an APN configuration based on the supplied APN and those configurable parameters.

APN configuration dictates all aspects of a session at the GGSN. Different policies imply different APNs. After basic APN selection, however, internal re-selection can occur based on the following parameters:

- Service name
- Subscriber type
- MCC-MNC of IMSI
- Domain name part of username (user@domain)
- S-GW address

For Virtual APN configuration information, see *Virtual APN Configuration* section in *GGSN Service Configuration Procedures* chapter in this book.

Important For more information, refer to the **virtual-apn preference** command in *APN Configuration Mode Commands* in the *Command Line Interface Reference*.

Features and Functionality - Optional Enhanced Feature Software

This section describes the optional enhanced features and functions for GGSN service.

Each of the following features require the purchase of an additional license to implement the functionality with the GGSN service.

Common Gateway Access Support

Common Gateway Access support is a consolidated solution that combines 3G and 4G access technologies in a common gateway supporting logical services of HA, PGW, and GGSN to allow users to have the same user experience, independent of the access technology available.

In todays scenario an operator must have multiple access networks (CDMA, eHRPD and LTE) plus a GSM/UMTS solution for international roaming. Therefore, operator requires a solution to allow customers to access services with the same IP addressing behavior and to use a common set of egress interfaces, regardless of the access technology (3G or 4G).

This solution allows static customers to access their network services with the same IP addressing space assigned for wireless data, regardless of the type of connection (CDMA, eHRPD/LTE or GSM/UMTS). Subscribers using static IP addressing will be able to get the same IP address regardless of the access technology.

For more information on this product, refer *Common Gateway Access Support* section in GGSN Service Administration Guide.

Dynamic RADIUS Extensions (Change of Authorization)

Dynamic RADIUS extension support provide operators with greater control over subscriber PDP contexts by providing the ability to dynamically redirect data traffic, and or disconnect the PDP context.

This functionality is based on the RFC 3576, Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS), July 2003 standard.

The system supports the configuration and use of the following dynamic RADIUS extensions:

- **Change of Authorization**: The system supports CoA messages from the AAA server to change data filters associated with a subscriber session. The CoA request message from the AAA server must contain attributes to identify NAS and the subscriber session and a data filter ID for the data filter to apply to the subscriber session.
- **Disconnect Message**: The DM message is used to disconnect subscriber sessions in the system from a RADIUS server. The DM request message should contain necessary attributes to identify the subscriber session.

The above extensions can be used to dynamically re-direct subscriber PDP contexts to an alternate address for performing functions such as provisioning and/or account set up. This functionality is referred to as Session Redirection, or Hotlining.

Session redirection provides a means to redirect subscriber traffic to an external server by applying ACL rules to the traffic of an existing or a new subscriber session. The destination address and optionally the destination port of TCP/IP or UDP/IP packets from the subscriber are rewritten so the packet is forwarded to the designated redirected address.

Return traffic to the subscriber has the source address and port rewritten to the original values. The redirect ACL may be applied dynamically by means of the Radius Change of Authorization (CoA) extension.

Important For more information on dynamic RADIUS extensions support, refer *CoA, RADIUS, And Session Redirection (Hotlining)* in this guide.

GRE Protocol Interface Support

GGSN supports GRE generic tunnel interface support in accordance with RFC-2784, Generic Routing Encapsulation (GRE).

GRE protocol functionality adds one additional protocol on the system to support mobile users to connect to their enterprise networks through Generic Routing Encapsulation (GRE).

GRE tunnels can be used by the enterprise customers of a carrier 1) To transport AAA packets corresponding to an APN over a GRE tunnel to the corporate AAA servers and, 2) To transport the enterprise subscriber packets over the GRE tunnel to the corporation gateway.

The corporate servers may have private IP addresses and hence the addresses belonging to different enterprises may be overlapping. Each enterprise needs to be in a unique virtual routing domain, known as VRF. To differentiate the tunnels between same set of local and remote ends, GRE Key will be used as a differentiation.

GRE Tunneling is a common technique to enable multi-protocol local networks over a single-protocol backbone, to connect non-contiguous networks and allow virtual private networks across WANs. This mechanism encapsulates data packets from one protocol inside a different protocol and transports the data packets unchanged across a foreign network. It is important to note that GRE tunneling does not provide security to the encapsulated protocol, as there is no encryption involved (like IPSEC offers, for example).

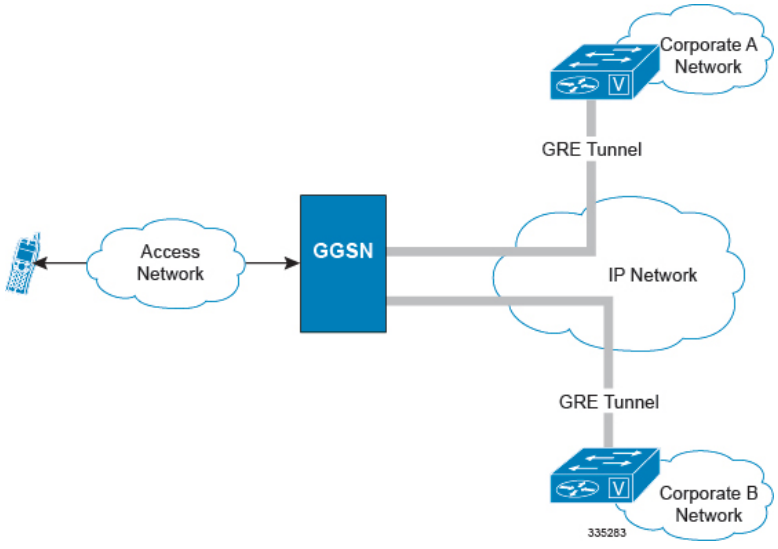
GRE Tunneling consists of three main components:

- Passenger protocol-protocol being encapsulated. For example: CLNS, IPv4 and IPv6.
- Carrier protocol-protocol that does the encapsulating. For example: GRE, IP-in-IP, L2TP, MPLS and IPSEC.
- Transport protocol-protocol used to carry the encapsulated protocol. The main transport protocol is IP.

The most simplified form of the deployment scenario is shown in the following figure, in which GGSN has two APNs talking to two corporate networks over GRE tunnels.

The following figure shows a high-level overview of the GRE deployment scenario:

Figure 7: GRE Deployment Scenario



GTP Throttling

The GGSN supports PDP throttling to help control the rate of incoming/outgoing messages on GGSN. This functionality is used in ensuring GGSN doesn't get overwhelmed by the GTP control plane messages. Also it will help in ensuring the GGSN will not overwhelm the peer GTP-C node with GTP Control plane messages.

This feature covers over-load protection of GGSN nodes and other external nodes with which it communicates.

External node overload can happen in a scenario where GGSN generates signaling requests at a higher rate than other nodes can handle. Also if the incoming rate is high at GGSN node, we might flood any of the external nodes. Hence throttling of both incoming and outgoing control messages is required.

Important GTP throttling will be done only for session level control messages. Path management messages will not be rate limited.

Important For more information on GTP throtling configuration, refer *GGSN Service Configuration* chapter.

Bypass Rate Limit Function

The Bypass Rate Limit Function is an enhancement to the existing GTP Throttling feature.

This enhancement requires no additional license. Existing licenses for the GTP-Throttling Feature (RLF License) and the VoLTE Prioritized Handling feature have been applied and used as follows:

- **RLF License:** The GTP-Throttling feature license has been enhanced to accomodate the message-types based RLF throttling bypass.
- **VoLTE Prioritized Handling Feature License:** This license has been enhanced to accomodate the emergency call, priority call, and apn-names based RLF throttling bypass.

The GTP Throttling feature helps control the rate of incoming/outgoing messages on GGSN. It prevents the message flood from P-GW towards S-GW and MME. Currently, following outgoing messages are throttled by GGSN using the RLF framework:

- Create Bearer Request (CBR)
- Delete Bearer Request (DBR)
- Update Bearer Request (UBR)
- NRUPC
- IPCA
- NRDPC

Once thorttling is enabled for outgoing messages, all outgoing messages are throttled except the Create Bearer Request (CBR) message, which is piggybacked with Create Session Response message.

This feature has been enhanced 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.

Important For more information on these commands, refer to the *CLI Reference Guide.*

Gx Interface Support

Gx interface support on the system enables the wireless operator to:

- Implement differentiated service profiles for different subscribers
- Intelligently charge the services accessed depending on the service type and parameters

This interface is particularly suited to control and charge multimedia applications and IMS services. This interface support is compliant to following standards:

- 3GPP TS 23.203 V7.6.0 (2008-03): 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Policy and charging control architecture (Release 7)
- 3GPP TS 29.210 V6.2.0 (2005-06): 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Charging rule provisioning over Gx interface; (Release 6)
- 3GPP TS 29.212 V7.4.0 (2008-03): 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Policy and Charging Control over Gx reference point (Release 7)
- 3GPP TS 29.213 V7.4.0 (2008-03): 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Policy and Charging Control signalling flows and QoS parameter mapping; (Release 7)
- RFC 3588, Diameter Base Protocol
- RFC 4006, Diameter Credit-Control Application

In addition to the above RFCs and standards IMS authorization partially supports 3GPP TS 29.212 for Policy and Charging Control over Gx reference point functionality.

The goal of the Gx interface is to provide network based QoS control as well as dynamic charging rules on a per bearer basis. The Gx interface is in particular needed to control and charge multimedia applications.

QoS Parameter ARP Setting via Gx Interface: GGSN controls the assignment of different radio interface QoS priorities (gold/silver/bronze) via the PCRF Gx interface during PDP context setup (CCR/CCA-I). This is performed using the Allocation Retention Priority (ARP) parameter (AVP code 1034) as specified in 3GPP TS 29.212, with values = 0-3; ARP values from the PCRF other than 0-3 are ignored. During PDP context setup the PCRF returns the ARP value in CCA-I and this ARP is then assigned/negotiated with the SGSN and RNC.

The Gx interface is located between the GGSN and the E-PDF / PCRF. It is a Diameter- based interface and provides the functions provided earlier by the Gx and Go interfaces:

- QoS control based on either a token-based or token-less mechanism. In the token-based mechanism, the E-PDF or PCRF dynamically assign network resources to the different bearers used by the subscriber. These resource assignments are transmitted in Tokens carried over the Gx interface. The authorization tokens are allocated by the network (E-PDF/PCRF), hence the network is in full control of the mechanism since it only authorizes resources. The token-less mechanism is for further study.
- Dynamic rules for Flexible Bearer Charging. These dynamic charging rules are carried in the resource assignment tokens and provide 5-tuple type charging rules that enables to implement a specific charging

policy for each subscriber bearer. These charging rules will be applied by the FBC function of the GGSN, and produce the appropriate eG-CDRs or the appropriate messages on the Gy interface to the OCS.

Important For more information on Gx interface support, refer *Gx Interface Support* in this guide.

Inter-Chassis Session Recovery

The ST16 and chassis provides industry leading carrier class redundancy. The systems protects against all single points of failure (hardware and software) and attempts to recover to an operational state when multiple simultaneous failures occur.

The system provides several levels of system redundancy:

- Under normal N+1 packet processing card hardware redundancy, if a catastrophic packet processing card failure occurs all affected calls are migrated to the standby packet processing card if possible. Calls which cannot be migrated are gracefully terminated with proper call-termination signaling and accounting records are generated with statistics accurate to the last internal checkpoint
- If the Session Recovery feature is enabled, any total packet processing card failure will cause a packet processing card switchover and all established sessions for supported call-types are recovered without any loss of session.

Even though chassis provides excellent intra-chassis redundancy with these two schemes, certain catastrophic failures which can cause total chassis outages, such as IP routing failures, line-cuts, loss of power, or physical destruction of the chassis, cannot be protected by this scheme. In such cases, the GGSN Inter-Chassis Session Recovery feature provides geographic redundancy between sites. This has the benefit of not only providing enhanced subscriber experience even during catastrophic outages, but can also protect other systems such as the RAN from subscriber re-activation storms.

The Inter-chassis Session Recovery feature allows for continuous call processing without interrupting subscriber services. This is accomplished through the use of redundant chassis. The chassis are configured as primary and backup with one being active and one in recovery mode. A checkpoint duration timer is used to control when subscriber data is sent from the active chassis to the inactive chassis. If the active chassis handling the call traffic goes out of service, the inactive chassis transitions to the active state and continues processing the call traffic without interrupting the subscriber session. The chassis determines which is active through a propriety TCP-based connection called a redundancy link. This link is used to exchange **Hello** messages between the primary and backup chassis and must be maintained for proper system operation.

Interchassis Session Recovery uses following for failur handling and communication:

- **Interchassis Communication**:

  Chassis configured to support Interchassis Session Recovery communicate using periodic **Hello** messages. These messages are sent by each chassis to notify the peer of its current state. The **Hello** message contains information about the chassis such as its configuration and priority. A dead interval is used to set a time limit for a **Hello** message to be received from the chassis' peer. If the standby chassis does not receive a **Hello** message from the active chassis within the dead interval, the standby chassis transitions to the active state. In situations where the redundancy link goes out of service, a priority scheme is used to determine which chassis processes the session. The following priority scheme is used:

  - router identifier

- chassis priority
- SPIO MAC address

- **Checkpoint Message**:

  Checkpoint messages are sent from the active chassis to the inactive chassis. Checkpoint messages are sent at specific intervals and contain all the information needed to recreate the sessions on the standby chassis, if that chassis were to become active. Once a session exceeds the checkpoint duration, checkpoint data is collected on the session. The checkpoint parameter determines the amount of time a session must be active before it is included in the checkpoint message.

Important For more information on inter-chassis session recovery support, refer *Interchassis Session Recovery* in *System Administration Guide*.

IP Security (IPSec)

IP Security provides a mechanism for establishing secure tunnels from mobile subscribers to pre-defined endpoints (i.e. enterprise or home networks) in accordance with the following standards:

- RFC 2401, Security Architecture for the Internet Protocol
- RFC 2402, IP Authentication Header (AH)
- RFC 2406, IP Encapsulating Security Payload (ESP)
- RFC 2409, The Internet Key Exchange (IKE)
- RFC-3193, Securing L2TP using IPSEC, November 2001

GGSN supports IPSec features that you may wish to include in your configuration. Refer to the StarOS IP Security (IPSec) Reference for additional information.

IPNE Service Support

The GGSN supports the IP Network Enabler (IPNE) service. IPNE is a Mobile and IP Network Enabler (MINE) client component that collects and distributes session and network information to MINE servers. The MINE cloud service provides a central portal for wireless operators and partners to share and exchange session and network information to realize intelligent services. For detailed information on IPNE, refer to the IP Network Enabler appendix in this guide.

IPv6 Prefix Delegation from the RADIUS Server and the Local Pool

This feature adds support to obtain the DHCPv6 Prefix Delegation from the RADIUS server or a local pool configured on the GGSN/P-GW/SAEGW. Interface-ID allocation from RADIUS Server is also supported along with this feature.

A User Equipment (UE) or a Customer Premises Equipment (CPE) requests Prefix-Delegation. The P-GW or the GGSN then obtains this prefix from the RADIUS server or the local pool. P-GW and GGSN then advertise the prefix obtained by either RADIUS server or the local pool toward the UE client or the CPE.

This feature is divided into following three features:

- IPv6 Prefix Delegation from the RADIUS Server
- IPv6 Prefix Delegation from the Local Pool
- IPv6 Interface ID from the RADIUS Server

Important For more information on IPv6 Prefix Delegation, refer *IPv6 Prefix Delegation from the RADIUS Server and the Local Pool* chapter.

L2TP LAC Support

The system configured as a Layer 2 Tunneling Protocol Access Concentrator (LAC) enables communication with L2TP Network Servers (LNSs) for the establishment of secure Virtual Private Network (VPN) tunnels between the operator and a subscriber's corporate or home network.

The use of L2TP in VPN networks is often used as it allows the corporation to have more control over authentication and IP address assignment. An operator may do a first level of authentication, however use PPP to exchange user name and password, and use IPCP to request an address. To support PPP negotiation between the GGSN and the corporation, an L2TP tunnel must be setup in the GGSN running a LAC service.

L2TP establishes L2TP control tunnels between LAC and LNS before tunneling the subscriber PPP connections as L2TP sessions. The LAC service is based on the same architecture as the GGSN and benefits from dynamic resource allocation and distributed message and data processing. This design allows the LAC service to support over 4000 setups per second or a maximum of over 3G of throughput. There can be a maximum up to 65535 sessions in a single tunnel and as many as 500,000 L2TP sessions using 32,000 tunnels per system.

Important While establishing the L2TP session from LAC to LNS, the PPP connection for the user is established. The server uses CHAP authentication protocol to authenticate the connection. While calculating the CHAP response for the CHAP challenge received by the server, the server does not consider the CHAP password.

The LAC sessions can also be configured to be redundant, thereby mitigating any impact of hardware of software issues. Tunnel state is preserved by copying the information across processor cards.

Important For more information on this feature support, refer *L2TP Access Concentrator* in this guide.

L2TP LNS Support

The system configured as a Layer 2 Tunneling Protocol Network Server (LNS) supports the termination secure Virtual Private Network (VPN) tunnels between from L2TP Access Concentrators (LACs).

The LNS service takes advantage of the high performance PPP processing already supported in the system design and is a natural evolution from the LAC. The LNS can be used as a standalone, or running alongside a GGSN service in the same platform, terminating L2TP services in a cost effective and seamless manner.

L2TP establishes L2TP control tunnels between LAC and LNS before tunneling the subscriber PPP connections as L2TP sessions. There can be a maximum of up to 65535 sessions in a single tunnel and up to 500,000 sessions per LNS.

Important While establishing the L2TP session from LAC to LNS, the PPP connection for the user is established. The server uses CHAP authentication protocol to authenticate the connection. While calculating the CHAP response for the CHAP challenge received by the server, the server does not consider the CHAP password.

The LNS architecture is similar to the GGSN and utilizes the concept of a de-multiplexer to intelligently assign new L2TP sessions across the available software and hardware resources on the platform without operator intervention.

Important For more information on this feature support, refer *L2TP Network Server* in this guide.

Lawful Intercept

The system supports the Lawful Interception (LI) of subscriber session information. This functionality provides Telecommunication Service Providers (TSPs) with a mechanism to assist Law Enforcement Agencies (LEAs) in the monitoring of suspicious individuals (referred to as targets) for potential criminal activity.

The following standards were referenced for the system's LI implementation:

- TR-45 Lawfully Authorized Electronic Surveillance TIA/EIA J-STD-025 PN4465 RV 1.7
- 3GPP TS 33.106 V6.1.0 (2004-06): 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G security; Lawful Interception requirements (Release 6)
- 3GPP TS 33.107 V6.2.0 (2004-06): 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G security; Lawful interception architecture and functions (Release 6)
- 3GPP TS 33.108 V9.0.0 (2009-09): 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G security; Handover interface for Lawful Interception (LI) (Release 9)
- Technical Directive: Requirements for implementing statutory telecommunications interception measures (TR TKÜ), Version 4.0

LEAs provide one or more TSPs with court orders or warrants requesting the monitoring of a particular target. The target is identified by information such as their mobile station Integrated Services Digital Network (MSISDN) number, or their International Mobile Subscriber Identification (IMSI) number.

Once the target has been identified, the system, functioning as either a GGSN or HA, serves as an Access Function (AF) and performs monitoring for both new PDP contexts or PDP contexts that are already in progress. While monitoring, the system intercepts and duplicates Content of Communication (CC) and/or Intercept Related Information (IRI) and forwards it to a Delivery Function (DF) over an extensible, proprietary interface. Note that when a target establishes multiple, simultaneous PDP contexts, the system intercepts CC and IRI for each of them. The DF, in turn, delivers the intercepted content to one or more Collection Functions (CFs).

Lawful intercept supports TCP transport on node interfaces along with support for IPv6 address link between chassis and LI server.

On the system with StarOS version 9.0 or later, this feature enhanced to allow 20,000 LI targets to be provisioned as well as monitored.

Caution This capacity improvement impacts performance over various network scenario and in order to reach the full target of 20000 LI targets, it is required that the used platform have at least 12 active packet processing cards installed.

Important For more information on this feature support, refer *Lawful Intercept Configuration Guide*.

Mobile IP Home and Foreign Agents

Consolidation of GGSN, HA and/or FA services on the same platform eliminates CapEx and OpEx requirements for separate network elements and devices under management. Service integration also enables seamless mobility and inter-technology roaming between 1xEV-DO and UMTS/W-CDMA/GPRS/EDGE radio access networks. This shared configuration also enables common address pools to be applied across all service types. In addition, this combination of collapsed services does not create dependencies for Mobile IP client software on the user access device and consequently does not introduce additional requirements for Mobile IP signaling in the 3GPP radio access network.

This functionality provides the following benefits:

- Timely release of Mobile IP resources at the FA and/or HA
- Accurate accounting
- Timely notification to mobile node of change in service

The system is capable of supporting both GGSN and Mobile IP functions on a single chassis. For Mobile IP applications, the system can be configured to provide the function of a Gateway GPRS Support Node/Foreign Agent (GGSN/FA) and/or a Home Agent (HA).

HA and FA components are defined by RFC 2002 in support of Mobile IP. Mobile IP provides a network-layer solution that allows Mobile Nodes (MNs, i.e. mobile phones, wireless PDAs, and other mobile devices) to receive routed IP packets from their home network while they are connected to any visitor network using their permanent or home IP address. Mobile IP allows mobility in a dynamic method that allows nodes to maintain ongoing communications while changing links as the user traverses the global Internet from various locations outside their home network.

When configured to support HA functionality, the system is capable of supporting following enhanced features:

- **Mobile IP HA Session Rejection/Redirection**: Enables the HA service to either reject new calls or redirect them to another HA when a destination network connection failure is detected. When network connectivity is re-established, the HA service begins to accept calls again in the normal manner. This feature provides the benefit of reducing OpEx through increased operational efficiency and limiting of system downtime.
- **Mobile IP Registration Revocation**: Registration Revocation is a general mechanism whereby the HA providing Mobile IP or Proxy Mobile IP functionality to a mobile node can notify the GGSN/FA of the

termination of a binding. Mobile IP Registration Revocation can be triggered at the HA by any of the following:

- Administrative clearing of calls
- Session Manager software task outage resulting in the loss of FA sessions (sessions that could not be recovered)
- Session Idle timer expiry (when configured to send Revocation)
- Any other condition under which a binding is terminated due to local policy (duplicate IMSI detected, duplicate home address requested)

Important For more information on Mobile IP HA service and FA service configuration, refer *HA Administration Guide* and *GGSN Administration Guide* respectively

Mobile IP NAT Traversal

This functionality enables converged WiFi-cellular data deployments in which the system is used to concentrate and switch traffic between WiFi hotspots. UDP/IP tunneling enables NAT firewalls in WLAN hotspots to maintain state information for address translation between NATed public address/UDP ports and addresses that are privately assigned for the mobile access device by a local DHCP server.

The Mobile IP protocol does not easily accommodate subscriber mobile nodes that are located behind WLAN or WAN-based NAT devices because it assumes that the addresses of mobile nodes or FA's are globally routable prefixes. However, the mobile node's co-located care of address (CCoA/CoA) is a private address. This presents a problem when remote hosts try to reach the mobile node via the public advertised addresses. The system provides a solution that utilizes UDP tunneling subject to subscriber reservation requests. In this application, the HA uses IP UDP tunneling to reach the mobile subscriber and includes the same private address that was provided in original reservation request in the encapsulated IP payload packet header.

Important For more information on this feature, refer *MIP NAT Traversal* in *System Administration Guide*.

NEMO Service Support

Use of NEMO requires a valid license key be installed. Contact your local Sales or Support representative for information on how to obtain a license.

The GGSN provides the configuration support to enable or disable the Network Mobility (NEMO) service on chassis.

When enabled, the system includes NEMO support for a Mobile IPv4 Network Mobility (NEMO-HA) on the GGSN platform to terminate Mobile IPv4 based NEMO connections from Mobile Routers (MRs) that attach to an Enterprise PDN. The NEMO functionality allows bi-directional communication that is application-agnostic between users behind the MR and users or resources on Fixed Network sites.

The same NEMO4G-HA service and its bound Loopback IP address supports NEMO connections whose underlying PDN connection comes through GTP S5 (4G access) or PMIPv6 S2a (eHRPD access).

Important For more information on NEMO support, refer to the *Network Mobility (NEMO)*chapter in this guide.

Multimedia Broadcast Multicast Services Support

Multimedia services are taking on an ever-increasing role in the wireless carriers' plans for an application centric service model. As such, any next generation GGSN platform must be capable of supporting the requirements of multimedia service delivery, including:

- Higher bandwidth requirements of streaming audio and video delivery
- Efficient broadcast and multicast mechanisms, to conserve resources in the RAN

MBMS represents the evolutionary approach to multicast and broadcast service delivery. MBMS uses spectrum resources much more efficiently than Multicast-over-Unicast by optimizing packet replication across all critical components in the bearer path. Thus, services requiring largely uni-directional multicast flows towards the UE are particularly well suited to the MBMS approach. These would include news, event streaming, suitably encoded/compressed cable/radio programs, video-on-demand, multi-chat / group-push-to-talk/video-conferencing sessions with unicast uplink and multicast downlink connections, and other applications.

For MBMS functionality, the system supports the Gmb interface, which is used signal to the BM-SC

Important For more information on this feature, refer *Multicast Broadcast Service* in this guide.

Overcharging Protection on Loss of Coverage

This solution provides the ability to configure mobile carriers to maximize their network solutions and balancing the requirements to accurately bill their customer.

Considering a scenario where a mobile is streaming or downloading very large files from external sources and the mobile goes out of radio coverage. If this download is happening on Background/Interactive traffic class then the GGSN is unaware of such loss of connectivity as SGSN does not perform the Update PDP Context procedure to set QoS to 0kbps (this is done when traffic class is either Streaming or Conversational only). The GGSN continues to forward the downlink packets to SGSN. In the loss of radio coverage, the SGSN will do paging request and find out that the mobile is not responding; SGSN will then drops the packets. In such cases, the G-CDR will have increased counts but S-CDR will not. This means that when operators charge the subscribers based on G-CDR the subscribers may be overcharged. This feature is implemented to avoid the overcharging in such cases.

This implementation is based on Cisco-specific private extension to GTP messages and/or any co-relation of G-CDRs and S-CDRs. It also does not modify any RANAP messages.

Important For more information on this feature, refer *Subscriber Overcharging Protection* in this guide.

Proxy Mobile IP

Mobility for subscriber sessions is provided through the Mobile IP protocol as defined in RFCs 2002-2005. However, some older Mobile Nodes (MNs) do not support the Mobile IP protocol. The Proxy Mobile IP feature provides a mobility solution for these MNs.

For IP PDP contexts using Proxy Mobile IP, the MN establishes a session with the GGSN as it normally would. However, the GGSN/FA performs Mobile IP operations with an HA (identified by information stored in the subscriber's profile) on behalf of the MN (i.e. the MN is only responsible for maintaining the IP PDP context with the GGSN, no Agent Advertisement messages are communicated with the MN).

The MN is assigned an IP address by either the HA, an AAA server, or on a static-basis. The address is stored in a Mobile Binding Record (MBR) stored on the HA. Therefore, as the MN roams through the service provider's network, each time a hand-off occurs, the MN will continue to use the same IP address stored in the MBR on the HA.

Proxy Mobile IP can be performed on a per-subscriber basis based on information contained in their user profile, or for all subscribers facilitated by a specific APN. In the case of non-transparent IP PDP contexts, attributes returned from the subscriber's profile take precedence over the configuration of the APN.

Important For more information on this feature, refer *Proxy Mobile IP* in this guide.

Session Persistence

Important Other licenses (i.e. IP Security and L2TP) may be additionally required depending on your network deployment and implementation.

Provides seamless mobility to mobile subscribers as they roam between WLAN and 3G cellular access networks. This type of inter-technology roaming is ordinarily not possible as wireline access networks do not include SGSNs to permit inter-SGSN call hand-offs with cellular access networks.

The Cisco Session Persistence Solution maintains consistent user identities and application transparency for your mobile subscribers as they roam across bearer access networks. This is accomplished through the integration of Home Agent (HA) and GGSN functionality on the wireless access gateway in the packet network and the use of standards-based protocols such as Mobile IP and Mobile IP NAT Traversal. The solution also includes Session Persistence client software that runs on dual-mode WiFi/GPRS/EDGE and/or UMTS/W-CDMA access devices including cellular phones and laptop computers with wireless data cards.

The Session Persistence client is designed to permit Mobile IP tunneling over the applicable underlying network including cellular access connections and cable or XDSL broadband access networks. When the user is attached to a WiFi access network, the Session Persistence client utilizes a Mobile IP Co-located Care of Address Foreign Agent Service (CCoA FA) and establishes a MIP tunnel to the HA service in the platform. This scenario is completely transparent to the GGSN service that operates in the same system. The Mobile IP protocol requires a publicly addressable FA service; however, this is a problem when the mobile subscriber is located behind a NAT firewall. In this case, the NAT firewall has no way of maintaining state to associate the public NATed address with the private address assigned to the user by local DHCP server. Mobile IP NAT Traversal solves this problem by establishing a UDP/IP tunnel between the subscriber access device and Home Agent. The NAT firewall uses the UDP port address to build state for the subscriber session. During this Mobile IP transaction, the HA establishes a mobility binding record for the subscriber session.

When the subscriber roams to a 3GPP cellular access network, it uses the IP address from normal PDP IP context establishment as its new Mobile IP Care of Address to refresh the mobility binding record at the Home Agent. For reduced latency between access hand-offs, it is also possible to utilize a permanent 'always-on' PDP IP context with the IP address maintained in the MIP session persistence client. In this scenario, the mobile access device only needs to re-establish the dormant RAB wireless connection with the 3GPP access network prior to transmitting a new Mobile IP registration.

The system also enables network-provisioned VPNs for Session Persistence applications by permitting use of overlapping address pools on the HA and using various tunneling protocols including IPSEC, Layer 2 Tunneling Protocol (L2TP) and Ethernet IEEE 802.1Q VLANs for separation of subscriber traffic. This application may be further augmented by additional features such as 800 RADIUS Server Groups to permit use of enterprise controlled AAA servers and custom dictionaries.

Session Recovery Support

The Session Recovery feature provides seamless failover and reconstruction of subscriber session information in the event of a hardware or software fault within the system preventing a fully connected user session from being disconnected.

Session recovery is performed by mirroring key software processes (e.g. session manager and AAA manager) within the system. These mirrored processes remain in an idle state (in standby-mode), wherein they perform no processing, until they may be needed in the case of a software failure (e.g. a session manager task aborts). The system spawns new instances of "standby mode" session and AAA managers for each active Control Processor (CP) being used.

Additionally, other key system-level software tasks, such as VPN manager, are performed on a physically separate packet processing card to ensure that a double software fault (e.g. session manager and VPN manager fails at same time on same card) cannot occur. The packet processing card used to host the VPN manager process is in active mode and is reserved by the operating system for this sole use when session recovery is enabled.

The additional hardware resources required for session recovery include a standby System Processor Card (SPC) and a standby packet processing card.

There are following modes of Session Recovery:

- **Task recovery mode**: Wherein one or more session manager failures occur and are recovered without the need to use resources on a standby packet processing card. In this mode, recovery is performed by using the mirrored "standby-mode" session manager task(s) running on active packet processing cards. The "standby-mode" task is renamed, made active, and is then populated using information from other tasks such as AAA manager.
- **Full packet processing card recovery mode**: Used when a packet processing card hardware failure occurs, or when a packet processing card migration failure happens. In this mode, the standby packet processing card is made active and the "standby-mode" session manager and AAA manager tasks on the newly activated packet processing card perform session recovery.

Session/Call state information is saved in the peer AAA manager task because each AAA manager and session manager task is paired together. These pairs are started on physically different packet processing cards to ensure task recovery.

Important For more information on this feature, refer *Session Recovery* in *System Administration Guide*.

Traffic Policing and Rate Limiting

Allows the operator to proportion the network and support Service-level Agreements (SLAs) for customers.

The Traffic-Policing feature enables configuring and enforcing bandwidth limitations on individual PDP contexts of a particular 3GPP traffic class. Values for traffic classes are defined in 3GPP TS 23.107 and are negotiated with the SGSN during PDP context activation using the values configured for the APN on the GGSN. Configuration and enforcement is done independently on the downlink and the uplink directions for each of the 3GPP traffic classes. Configuration is on a per-APN basis, but may be overridden for individual subscribers or subscriber tiers during RADIUS authentication/authorization.

A Token Bucket Algorithm (a modified trTCM, as specified in RFC2698) is used to implement the Traffic-Policing feature. The algorithm measures the following criteria when determining how to mark a packet:

- **Committed Data Rate (CDR)**: The guaranteed rate (in bits per second) at which packets may be transmitted/received for the subscriber during the sampling interval.
- **Peak Data Rate (PDR)**: The maximum rate (in bits per second) that packets may be transmitted/received for the subscriber during the sampling interval.
- **Burst-size**: The maximum number of bytes that may be transmitted/received for the subscriber during the sampling interval for both committed (CBS) and peak (PBS) rate conditions. This represents the maximum number of tokens that can be placed in the subscriber's "bucket". Note that the committed burst size (CBS) equals the peak burst size (PBS) for each subscriber.

Tokens are removed from the subscriber's bucket based on the size of the packets being transmitted/received. Every time a packet arrives, the system determines how many tokens need to be added (returned) to a subscriber's CBS (and PBS) bucket. This value is derived by computing the product of the time difference between incoming packets and the CDR (or PDR). The computed value is then added to the tokens remaining in the subscriber's CBS (or PBS) bucket. The total number of tokens can not be greater than the configured burst-size. If the total number of tokens is greater than the burst-size, the number is set to equal the burst-size. After passing through the Token Bucket Algorithm, the packet is internally classified with a color, as follows:

- There are not enough tokens in the PBS bucket to allow a packet to pass, then the packet is considered to be in violation and is marked "red" and the violation counter is incremented by one.
- There are enough tokens in the PBS bucket to allow a packet to pass, but not in the CBS "bucket", then the packet is considered to be in excess and is marked "yellow", the PBS bucket is decremented by the packet size, and the exceed counter is incremented by one.
- There are more tokens present in the CBS bucket than the size of the packet, then the packet is considered as conforming and is marked "green" and the CBS and PBS buckets are decremented by the packet size.

The APN on the GGSN can be configured with actions to take for red and yellow packets. Any of the following actions may be specified:

- **Drop**: The offending packet is discarded.
- **Transmit**: The offending packet is passed.
- **Lower the IP Precedence**: The packet's ToS octet is set to "0", thus downgrading it to Best Effort, prior to passing the packet.
- **Buffer the Packet**: The packet stored in buffer memory and transmitted to subscriber once traffic flow comes in allowed bandwidth.

Different actions may be specified for red and yellow, as well as for uplink and downlink directions and different 3GPP traffic classes.

Important For more information on this feature, refer *Traffic Policing* in this guide.

User Location Change Reporting Support

The user information change reporting is enabled on GGSN via PCRF using GPRS specific event triggers and GPRS specific credit re-authorization triggers. The user information to be reported include Location Change Reporting (ULI) and Closed Subscriber Group Information Change reporting (UCI)

For Location change reporting for a subscriber session requested by GGSN, the SGSN includes the User Location Information (ULI) if the MS is located in a RAT Type of GERAN, UTRAN or GAN. It also includes the CGI, SAI or RAI depending on whether the MS is in a cell, a service or a routing area respectively. The SGSN may optionally include the User Location Information for other RAT Types.

Closed Subscriber Group (CSG) identifies a group of subscribers who are permitted to access one or more CSG cells of the PLMN as a member of the CSG. A CSG ID is a unique identifier within the scope of PLMN which identifies a CSG in the PLMN associated with a CSG cell or group of CSG cells. For CSG info change reporting for a subscriber session requested by GGSN, the SGSN includes the User CSG Information if the MS is located in the CSG cell or the hybrid cell.

Release 20.0 and later, support has been added to process and handle a MS Info Change notification received with valid information to identify a PDN (non-zero TEID and/or IMSI+NSAPI) and with appropriate ULI and/or UCI information. In case of collision between MS-Info-change message and NRUPC, GGSN will process MS-info-change request first and send out its MS-info-change response. Then the NRUPC will be retried again.

Important CSG reporting is not yet supported on GGSN, P-GW, or SAEGW.

Limitations

Following are the limitations of this feature:

- UCI trigger from PCRF is not supported.
- The MS Info Change reporting action trigger will not be recovered if trigger if:
  - trigger is changed
  - MS reporting action has not gone in CPC/UPC/NRUPC
  - session manager (SM) recovery happens
- The MS Change info message is not supported if it comes on UE level.

3GPP ULI Reporting Support Enhanced

This feature enhancement covers ULI related gaps in P-GW and GGSN as per 3GPP standards.

Feature Change

This feature enhancement covers ULI related gaps in P-GW and GGSN as per 3GPP standards.

S4SGSN reports ULI to the P-GW through S-GW. P-GW determines the changes in the ULI with previously received ULI. If any change is detected and same change has been requested by the PCRF as an event trigger then the ULI is reported to the PCRF.

SGSN reports ULI to the GGSN. GGSN determines the changes in the ULI with previously received ULI. If any change is detected and same change has been requested by the PCRF as an event trigger, then the ULI is reported to the PCRF. Support has also been added to detect the change in RAI received as part of the ULI field at GGSN.

Following table summarizes the Change Reporting Action (CRA) values based on Event Triggers received from the PCRF, which the P-GW communicates with S4 SGSN.

Event Trigger From PCRF	CRA Sent to S4 SGSN
USER_LOCATION_CHANGE (13)	Start Reporting CGI/SAI and RAI (5)
RAI_CHANGE (12)	Start Reporting RAI (2)
USER_LOCATION_CHANGE + RAI_CHANGE	Start Reporting CGI/SAI and RAI (5)

Following table summarizes the MS Info Change Reporting Action values based on Event Triggers received from the PCRF which GGSN communicates to SGSN.

Event Trigger from PCRF	MS Info Change Reporting Actiontowards SGSN
USER_LOCATION_CHANGE (13)	Start Reporting CGI/SAI (1)
RAI_CHANGE (12)	Start Reporting RAI (2)
BOTH (12,13)	Start Reporting CGI/SAI (1)

P-GW/GGSN reports the CRA/MS Info Change Reporting Action immediately on receiving the Event Triggers without waiting for other events like APN/AMBR update or QoS update.

Behavior Change

Previous of Change Reporting Action: Following table illustrates the old and new behavior of Change Reporting Action with respect to the Event Triggers received from PCRF, when the Access Node is S4SGSN.

Event Trigger From PCRF	CRA Sent to S4SGSN	CRA Sent to S4SGSN
ULI_CHANGE(13)	6 (START_REPORTING_TAI_ECGI)	5(START_REPORTING_CGI_RAI)
RAI_CHANGE(12)	No CRA Sent	2 (START_REPORTING_RAI)
BOTH (12,13)	6 (START_REPORTING_TAI_ECGI)	5 (START_REPORTING_CGI_RAI)

Behavior of MS Info Change Reporting Action: Following table illustrates the old and new behavior of MS Info CRA with respect to the Event Triggers received from PCRF, when the Access Node is SGSN.

Event Trigger From PCRF	CRA Sent to SGSN	CRA Sent to SGSN
ULI_CHANGE(13)	1 (START_REPORTING_CGI/SAI)	1 (START_REPORTING_CGI/SAI)
RAI_CHANGE(12)	No CRA Sent	2 (START_REPORTING_RAI)
BOTH (12,13)	1 (START_REPORTING_CGI/SAI)	1 (START_REPORTING_CGI/SAI)

Limitations

1. In GGSN, when a new ULI is received in the Network Request Updated PDP Context (NRUPC) Response, it is not reported to the PCRF.
2. In GGSN, when a dedicated bearer is deleted or call is dropped, ULI change is not detected.

How GGSN Works

This section provides information on the function of the GGSN in a GPRS/UMTS network and presents call procedure flows for different stages of session setup.

The following topics and procedure flows are included:

- PDP Context Processing
- Dynamic IP Address Assignment, on page 50
- Subscriber Session Call Flows, on page 51

PDP Context Processing

PDP context processing is based on the APN that the subscriber is attempting to access. Templates for all of the possible APNs that subscribers will be accessing must be configured within the system. Up to 2,048 APNs can be configured on the system.

Each APN template consists of parameters pertaining to how PDP contexts are processed such as the following:

- **Type**: The system supports IPv4, IPv6, IPv4v6, and PPP PDP contexts. For IPv6 PDP configuration to work, at least one IPv6 interface needs to be configured in the destination context.
- **Accounting protocol**: Support is provided for using either the GTPP or Remote Authentication Dial-In User Service (RADIUS) protocols. In addition, an option is provided to disable accounting if desired.
- **Authentication protocol**: Support is provided for using any of the following:
  - Challenge Handshake Authentication Protocol (CHAP)
  - Microsoft CHAP (MSCHAP)
  - Password Authentication Protocol (PAP)
  - IMSI-based authentication
  - MSISDN-based authentication

In addition, an option is provided to disable authentication if desired.

- **Charging characteristics**: Each APN template can be configured to either accept the charging characteristics it receives from the SGSN for a PDP context or use it's own characteristics.
- **IP address allocation method**: IP addresses for PDP contexts can be assigned using one of the following methods:
  - **Statically**: The APN template can be configured to provide support for MS-requested static IP addresses. Additionally, a static address can be configured in a subscriber's profile on an authentication server and allocated upon successful authentication.
  - **Dynamically**: The APN template can be configured to dynamically assign an IP address from locally configured address pools or via a Dynamic Host Control Protocol (DHCP) server. Additional information on dynamic address assignment can be found in the *Dynamic IP Address Assignment* section that follows.

Important Static IP addresses configured in subscriber profiles must also be part of a static IP address pool configured locally on the system.

- **Selection mode**: The MS's right to access the APN can be either verified or unverified. For verified access, the SGSN specifies the APN that should be used. For unverified access, the APN can be specified by either the SGSN or the MS.
- **Timeout**: Absolute and idle session timeout values specify the amount of time that an MS can remain connected.
- **Mobile IP configuration**: Mobile IP requirements, HA address, and other related parameters are configured in the APN template.
- **Proxy Mobile IP support**: Mobile IP support can be enabled for all subscribers facilitated by the APN. Alternatively, it can be enabled for individual subscribers via parameters in their RADIUS or local-user profiles.
- **Quality of Service**: Parameters pertaining to QoS feature support such as for Dynamic Renegotiation, Traffic Policing, and DSCP traffic class.

A total of 11 PDP contexts are supported per subscriber. These could be all primaries, or 1 Primary and 10 secondaries or any combination of primary and secondary. Note that there must be at least one primary PDP context in order for secondaries to come up.

Dynamic IP Address Assignment

IP addresses for PDP contexts can either be static—an IP address is permanently assigned to the MS—or dynamic—an IP address is temporarily assigned to the MS for the duration of the PDP context.

As previously described in the *PDP Context Processing* section of this chapter, the method by which IP addresses are assigned to a PDP context is configured on an APN-by-APN basis. Each APN template dictates whether it will support static or dynamic addresses. If dynamic addressing is supported, the following methods can be implemented:

- **Local pools:** The system supports the configuration of public or private IP address pools. Addresses can be allocated from these pools as follows:
  - **Public pools:** Provided that dynamic assignment is supported, a parameter in the APN configuration mode specifies the name of the local public address pool to use for PDP contexts facilitated by the APN.
  - **Private pools:** Provided that dynamic assignment is supported, the name of the local private pool can be specified in the subscriber's profile. The receipt of a valid private pool name will override the APN's use of addresses from public pools.
- **Dynamic Host Control Protocol (DHCP):** The system can be configured to use DHCP PDP context address assignment using either of the following mechanisms:
  - **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.
  - **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.

In addition to the above methods, IP addresses for subscriber Mobile IP sessions are also dynamically assigned by the subscriber's home network upon registration. The GGSN/FA, in turn, provide the assigned address to the mobile station.

Subscriber Session Call Flows

This section provides information on how GPRS/UMTS subscriber data sessions are processed by the system GGSN. The following data session scenarios are provided:

- **Transparent IP:** The subscriber is provided basic access to a 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 (PDU) 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 subscriber's 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.

  Limitations:
  - Secondary PDP context creation for GGSN PDP type PPP session is not supported.
  - PDP type PPP for GnGp GGSN is not supported.
  - Routing Behind Mobile Station functionality for GGSN PDP-type PPP is not supported.
  - Inter-Chassis session recovery of GGSN PDP-type PPP sessions is not supported.

  - Multi-PDN with PDP-type PPP is not supported.
  - Inter-RAT handovers with PDP-type PPP is not supported.
  - L2TP with PDP-type PPP is not supported in this release.
  - Lawful Interception with PDP-type PPP is not supported.
  - Static IP address allocation with PDP-type PPP is not supported.
  - IPv6 address allocation with PDP-type PPP is not supported.

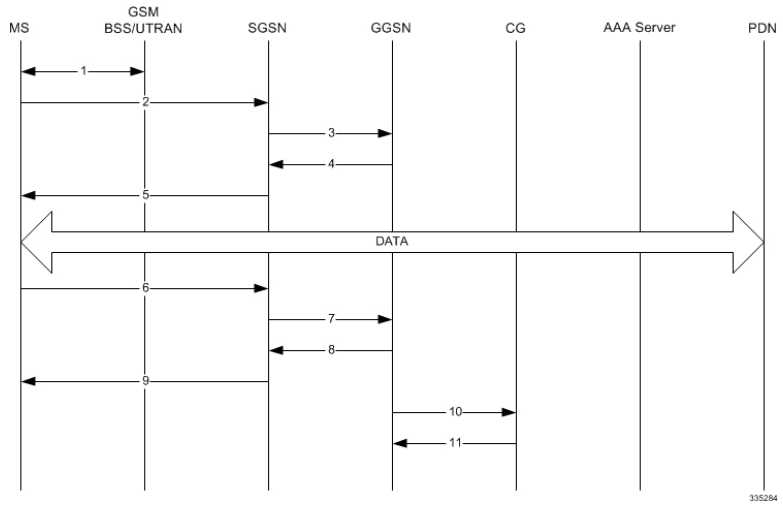
- **Virtual Dialup Access**: The GGSN functions as an LAC, encapsulates subscriber packets using L2TP, and tunnels them directly to an LNS for processing.
- **Corporate IP VPN Connectivity**: Similar to the Virtual Dialup Access model, however, the GGSN is configured to tunnel subscriber packets to a corporate server using IP-in-IP.
- **Mobile IP**: Subscriber traffic is routed to their home network via a tunnel between the GGSN/FA and an HA. The subscriber's IP PDP context is assigned an IP address from the HA.
- **Proxy Mobile IP**: Provides a mobility solution for subscribers whose Mobile Nodes (MNs) do not support the Mobile IP protocol. The GGSN/FA proxy the Mobile IP tunnel with the HA on behalf of the MS. The subscriber receives an IP address from their home network. As the subscriber roams through the network, the IP address is maintained providing the subscriber with the opportunity to use IP applications that require seamless mobility such as transferring files.
- **IPv6 Stateless Address Auto Configuration**: The mobile station may select any value for the interface identifier portion of the address. The only exception is the interface identifier for the link-local address used by the mobile station. This interface identifier is assigned by the GGSN to avoid any conflict between the mobile station link-local address and the GGSN address. The mobile station uses the interface ID assigned by the GGSN during stateless address auto-configuration procedure (e.g., during the initial router advertisement messages). Once this is over, the mobile can select any interface ID for further communication as long as it does not conflict with the GGSN's interface ID (that the mobile would learn through router advertisement messages from the GGSN).

Additionally, information about the process used by the system to dynamically assign IP addresses to the MS is provided in following sections.

Transparent Session IP Call Flow

The following figure and the text that follows describe the call flow for a successful transparent data session.

Figure 8: Transparent IP Session Call Flow



1. The Mobile Station (MS) goes through the process of attaching itself to the GPRS/UMTS network.
2. The MS sends an Activate PDP Context Request message that is received by an SGSN. The message contains information about the subscriber such as the Network layer Service Access Point Identifier (NSAPI), PDP Type, PDP Address, Access Point Name (APN), Quality of Service (QoS) requested, and PDP configuration options.
3. The SGSN authenticates the request message and sends a Create PDP Context Request message to a GGSN using the GPRS Tunneling Protocol (GTPC, "C" indicates the control signaling aspect of the protocol). The recipient GGSN is selected based on either the request of the MS or is automatically selected by the SGSN. The message consists of various information elements including: PDP Type, PDP Address, APN, charging characteristics, and Tunnel Endpoint Identifier (TEID, if the PDP Address was static).
4. The GGSN determines if it can facilitate the session (in terms of memory or CPU resources, configuration, etc.) and creates a new entry in its PDP context list and provides a Charging ID for the session.

   If the MS required the dynamic assignment of an IP address (i.e., the PDP Address received from the mobile was null), the GGSN will assign one. The IP address assignment methods supported by the system GGSN are described in the *Dynamic IP Address Assignment* section of this guide.

   The GGSN replies with an affirmative Create PDP Context Response using GTPC. The response will contain information elements such as the PDP Address representing either the static address requested by the MS or the address assigned by the GGSN, the TEID used to reference PDP Address, and PDP configuration options specified by the GGSN.
5. The SGSN returns an Activate PDP Context Accept response to the MS.

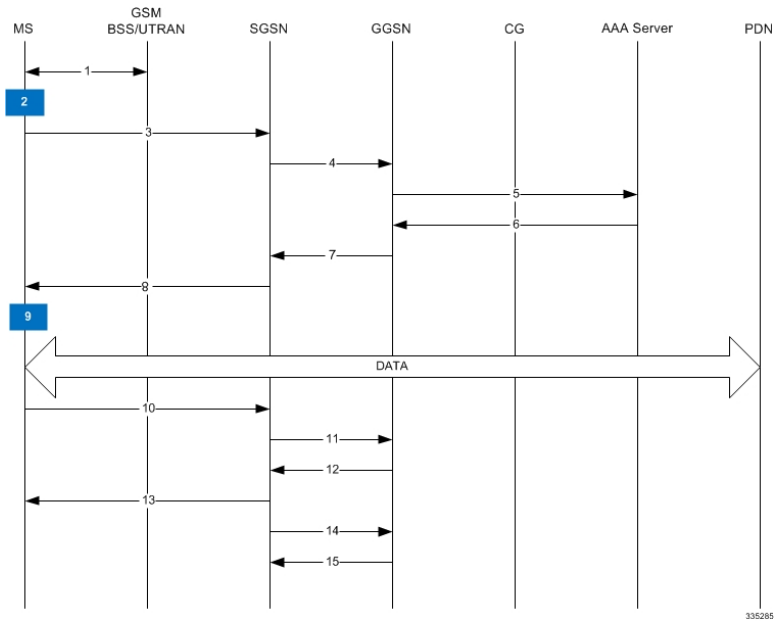
   The MS can now send and receive data to or from the PDN until the session is closed or times out. The MS can initiate multiple PDP contexts if desired and supported by the system. Each additional PDP context can share the same IP address or use alternatives.
6. The MS can terminate the data session at any time. To terminate the session, the MS sends a Deactivate PDP Context Request message that is received by the SGSN.

7. The SGSN sends a Delete PDP Context Request message to the GGSN facilitating the data session. The message includes the information elements necessary to identify the PDP context (i.e., TEID, and NSAPI).
8. The GGSN removes the PDP context from memory and returns a Delete PDP Context Response message to the SGSN. If the PDP context was the last associated with a particular dynamically assigned PDP Address, the GGSN will re-claim the IP address for use by subsequent PDP contexts.
9. The SGSN returns a Deactivate PDP Context Accept message to the MS.
10. The GGSN delivers the GGSN Charging Detail Records (G-CDRs) to a Charging Gateway (CG) using GTP Prime (GTPP). Note that, though not shown in this example, the GGSN could optionally be configured to send partial CDRs while the PDP context is active.
11. For each accounting message received from the GGSN, the CG responds with an acknowledgement.

Non-Transparent IP Session Call Flow

The following figure and the text that follows describe the call flow for a successful non-transparent data session.

Figure 9: Non-Transparent IP Session Call Flow



1. The Mobile Station (MS) goes through the process of attaching itself to the GPRS/UMTS network.
2. The Terminal Equipment (TE) aspect of the MS sends AT commands to the Mobile Terminal (MT) aspect of the MS to place it into PPP mode.

   The Link Control Protocol (LCP is then used to configure the Maximum-Receive Unit size and the authentication protocol (Challenge-Handshake Authentication Protocol (CHAP), Password Authentication Protocol (PAP), or none). If CHAP or PAP is used, the TE will authenticate itself to the MT, which, in turn, stores the authentication information.

Upon successful authentication, the TE sends an Internet Protocol Control Protocol (IPCP) Configure-Request message to the MT. The message will either contain a static IP address to use or request that one be dynamically assigned.

3. The MS sends an Activate PDP Context Request message that is received by an SGSN. The message contains information about the subscriber such as the Network layer Service Access Point Identifier (NSAPI), PDP Type, PDP Address, Access Point Name (APN), Quality of Service (QoS) requested, and PDP configuration options.
4. The SGSN authenticates the request message and sends a Create PDP Context Request message to a GGSN using the GPRS Tunneling Protocol (GTPC, "C" indicates the control signaling aspect of the protocol). The recipient GGSN is selected based on either the request of the MS or is automatically selected by the SGSN. The message consists of various information elements including: PDP Type, PDP Address, APN, charging characteristics, and tunnel endpoint identifier (TEID, if the PDP Address was static).
5. The GGSN determines if it can facilitate the session (in terms of memory or CPU resources, configuration, etc.) and creates a new entry in its PDP context list and provides a Charging ID for the session.

   From the APN specified in the message, the GGSN determines whether or not the subscriber is to be authenticated, how an IP address should be assigned if using dynamic allocation, and how to route the session.

   If authentication is required, the GGSN attempts to authenticate the subscriber locally against profiles stored in memory or send a RADIUS Access-Request message to an AAA server.

   If the MS required the dynamic assignment of an IP address (i.e., the PDP Address received from the mobile was null), the GGSN will assign one. The IP address assignment methods supported by the system GGSN are described in the *Dynamic IP Address Assignment* section of this chapter.
6. If the GGSN authenticated the subscriber to an AAA server, the AAA server responds with a RADIUS Access-Accept message indicating successful authentication.
7. The GGSN replies with an affirmative Create PDP Context Response using GTPC. The response will contain information elements such as the PDP Address representing either the static address requested by the MS or the address assigned by the GGSN, the TEID used to reference PDP Address, and PDP configuration options specified by the GGSN.
8. The SGSN returns an Activate PDP Context Accept message to the MS. The message includes response to the configuration parameters sent in the initial request.
9. The MT, will respond to the TE's IPCP Config-request with an IPCP Config-Ack message.

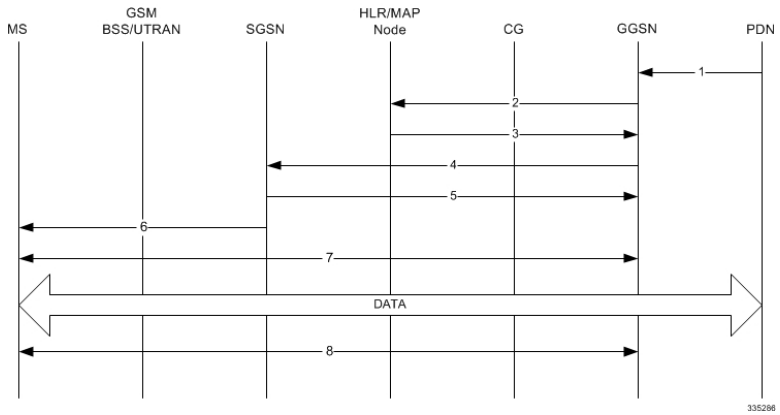
   The MS can now send and receive data to or from the PDN until the session is closed or times out. The MS can initiate multiple PDP contexts if desired and supported by the system. Each additional PDP context can share the same IP address or use alternatives.
10. The MS can terminate the data session at any time. To terminate the session, the MS sends a Deactivate PDP Context Request message that is received by the SGSN.
11. The SGSN sends a Delete PDP Context Request message to the GGSN facilitating the data session. The message includes the information elements necessary to identify the PDP context (i.e., TEID, and NSAPI).
12. The GGSN removes the PDP context from memory and returns a Delete PDP Context Response message to the SGSN. If the PDP context was the last associated with a particular dynamically assigned PDP Address, the GGSN will re-claim the IP address for use by subsequent PDP contexts.

13. The SGSN returns a Deactivate PDP Context Accept message to the MS.
14. The GGSN delivers the GGSN Charging Detail Records (G-CDRs) to a Charging Gateway (CG) using GTP Prime (GTPP). Note that, though not shown in this example, the GGSN could optionally be configured to send partial CDRs while the PDP context is active.
15. For each accounting message received from the GGSN, the CG responds with an acknowledgement.

Network-Initiated Session Call Flow

The following figure and the text that follows describe the call flow for a successful network-initiated data session.

Figure 10: Network-initiated Session Call Flow



1. An IP Packet Data Unit (PDU) is received by the GGSN from the PDN. The GGSN determines if it is configured to support network-initiated sessions. If not, it will discard the packet. If so, it will begin the Network-Requested PDP Context Activation procedure.
2. The GGSN may issue a Send Routing Information for GPRS request to the HLR to determine if the MS is reachable. The message includes the MS's International Mobile Subscriber Identity (IMSI).
3. If the MS is reachable, the HLR returns a Send Routing Information for GPRS Ack containing the address of the SGSN currently associated with the MS's IMSI.
4. The GGSN sends a PDU Notification Request message to the SGSN address supplied by the HLR. This message contains the IMSI, PDP Type, PDP Address, and APN associated with the session.
5. The SGSN sends a PDU Notification Response to the GGSN indicating that it will attempt to page the MS requesting that it activate the PDP address indicated in the GGSN's request.
6. The SGSN sends a Request PDP Context Activation message to the MS containing the information supplied by the GGSN.
7. The MS begins the PDP Context Activation procedure as described in *step 2* through *step 5* of the *Transparent Session IP Call Flow* section of this chapter.

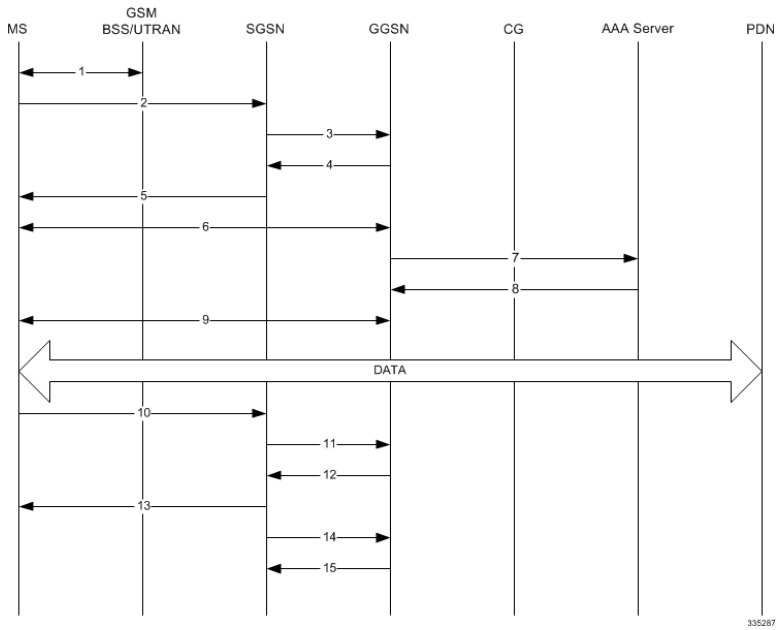
   Upon PDP context establishment, the MS can send and receive data to or from the PDN until the session is closed or times out.

8. The MS can terminate the data session at any time. To terminate the session, the MS begins the PDP Context De-Activation procedure as described in *step 6* through *step 11* of the *Transparent Session IP Call Flow* section of this chapter.

PPP Direct Access Call Flow

The following figure and the text that follows describe the call flow for a successful PPP Direct Access data session.

Figure 11: PPP Direct Access Call Flow



1. The Mobile Station (MS) goes through the process of attaching itself to the GPRS/UMTS network.
2. The MS sends an Activate PDP Context Request message that is received by an SGSN. The message contains information about the subscriber such as the Network layer Service Access Point Identifier (NSAPI), PDP Type, PDP Address, Access Point Name (APN), Quality of Service (QoS) requested, and PDP configuration options.
3. The SGSN authenticates the request message and sends a Create PDP Context Request message to a GGSN using the GPRS Tunneling Protocol (GTPC, "C" indicates the control signaling aspect of the protocol). The recipient GGSN is automatically selected by the SGSN. The message consists of various information elements including: PDP Type, PDP Address, APN, and charging characteristics.
4. The GGSN determines if it can facilitate the session (in terms of memory or CPU resources, configuration, etc.) and creates a new entry in its PDP context list and provides a Charging ID for the session. It determines that the PDP context type is PPP and based on the APN, what authentication protocol to use and how to perform IP address assignment.

   The GGSN replies with an affirmative Create PDP Context Response using GTPC.
5. The SGSN returns an Activate PDP Context Accept response to the MS.
6. The MS and the GGSN negotiate PPP.

7. The GGSN forwards authentication information received from the MS as part of PPP negotiation to the AAA server in the form of an Access-Request.
8. The AAA server authenticates the MS and sends an Access-Accept message to the GGSN.
9. The GGSN assigns an IP address to the MS and completes the PPP negotiation process. More information about IP addressing for PDP contexts is located in the *PDP Context Processing* and *Dynamic IP Address Assignment* sections of this chapter.

   Once the PPP negotiation process is complete, the MS can send and receive data.
10. The MS can terminate the data session at any time. To terminate the session, the MS sends a Deactivate PDP Context Request message that is received by the SGSN.
11. The SGSN sends a Delete PDP Context Request message to the GGSN facilitating the data session. The message includes the information elements necessary to identify the PDP context.
12. The GGSN removes the PDP context from memory and returns a Delete PDP Context Response message to the SGSN. If the PDP context was the last associated with a particular dynamically assigned PDP Address, the GGSN will re-claim the IP address for use by subsequent PDP contexts.
13. The SGSN returns a Deactivate PDP Context Accept message to the MS.
14. The GGSN delivers the GGSN Charging Detail Records (G-CDRs) to a Charging Gateway (CG) using GTP Prime (GTPP). Note that, though not shown in this example, the GGSN could optionally be configured to send partial CDRs while the PDP context is active.
15. For each accounting message received from the GGSN, the CG responds with an acknowledgment.

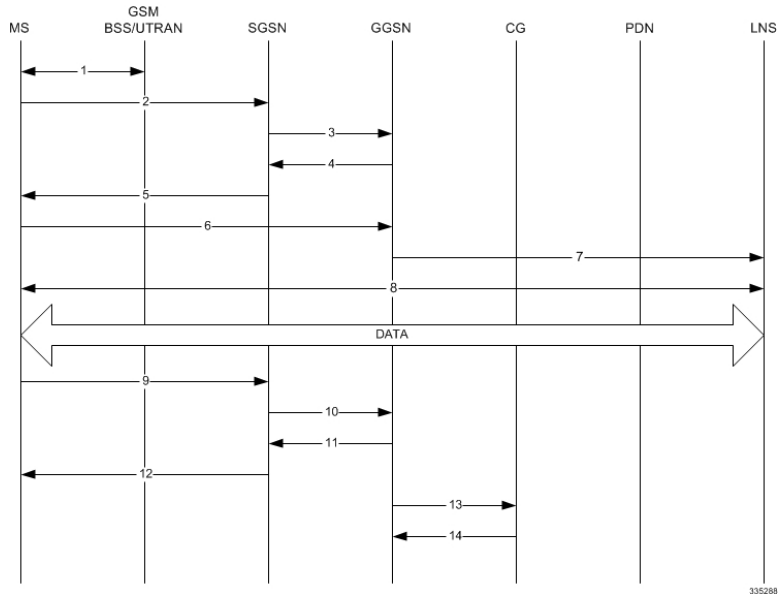
Limitations:

- Secondary PDP context creation for GGSN PDP type PPP session is not supported.
- PDP type PPP for GnGp GGSN is not supported.
- Routing Behind Mobile Station functionality for GGSN PDP-type PPP is not supported.
- Inter-Chassis session recovery of GGSN PDP-type PPP sessions is not supported.
- Multi-PDN with PDP-type PPP is not supported.
- Inter-RAT handovers with PDP-type PPP is not supported.
- L2TP with PDP-type PPP is not supported in this release.
- Lawful Interception with PDP-type PPP is not supported.
- Static IP address allocation with PDP-type PPP is not supported.
- IPv6 address allocation with PDP-type PPP is not supported.

Virtual Dialup Access Call Flow

The following figure and the text that follows describe the call flow for a successful VPN Dialup Access data session.

Figure 12: Virtual Dialup Access Call Flow



1. The Mobile Station (MS) goes through the process of attaching itself to the GPRS/UMTS network.
2. The MS sends an Activate PDP Context Request message that is received by an SGSN. The message contains information about the subscriber such as the Network layer Service Access Point Identifier (NSAPI), PDP Type, PDP Address, Access Point Name (APN), Quality of Service (QoS) requested, and PDP configuration options.
3. The SGSN authenticates the request message and sends a Create PDP Context Request message to a GGSN using the GPRS Tunneling Protocol (GTPC, "C" indicates the control signaling aspect of the protocol). The recipient GGSN is automatically selected by the SGSN. The message consists of various information elements including: PDP Type, PDP Address, APN, and charging characteristics.
4. The GGSN determines if it can facilitate the session (in terms of memory or CPU resources, configuration, etc.) and creates a new entry in its PDP context list and provides a Charging ID for the session. It determines the PDP context type and based on the APN, what authentication protocol to use and how to perform IP address assignment.

   The GGSN replies with an affirmative Create PDP Context Response using GTPC.
5. The SGSN returns an Activate PDP Context Accept response to the MS.
6. The MS sends packets which are received by the GGSN.
7. The GGSN encapsulates the packets from the MS using L2TP and tunnels them to the LNS.
8. The LNS terminates the tunnel and un-encapsulates the packets.

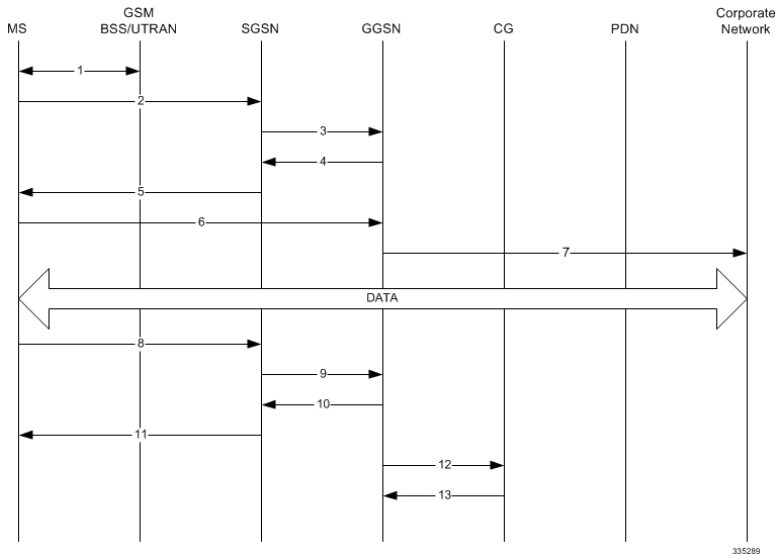
   The MS can send and receive data over the L2TP tunnel facilitated by the GGSN.
9. The MS can terminate the data session at any time. To terminate the session, the MS sends a Deactivate PDP Context Request message that is received by the SGSN.
10. The SGSN sends a Delete PDP Context Request message to the GGSN facilitating the data session. The message includes the information elements necessary to identify the PDP context.

11. The GGSN removes the PDP context from memory and returns a Delete PDP Context Response message to the SGSN. If the PDP context was the last associated with a particular dynamically assigned PDP Address, the GGSN will re-claim the IP address for use by subsequent PDP contexts.
12. The SGSN returns a Deactivate PDP Context Accept message to the MS.
13. The GGSN delivers the GGSN Charging Detail Records (G-CDRs) to a Charging Gateway (CG) using GTP Prime (GTPP). Note that, though not shown in this example, the GGSN could optionally be configured to send partial CDRs while the PDP context is active.
14. For each accounting message received from the GGSN, the CG responds with an acknowledgement.

Corporate IP VPN Connectivity Call Flow

The following figure and the text that follows describe the call flow for a successful Corporate IP Connectivity data session.

Figure 13: Corporate IP VPN Connectivity Call Flow



1. The Mobile Station (MS) goes through the process of attaching itself to the GPRS/UMTS network.
2. The MS sends an Activate PDP Context Request message that is received by an SGSN. The message contains information about the subscriber such as the Network layer Service Access Point Identifier (NSAPI), PDP Type, PDP Address, Access Point Name (APN), Quality of Service (QoS) requested, and PDP configuration options.
3. The SGSN authenticates the request message and sends a Create PDP Context Request message to a GGSN using the GPRS Tunneling Protocol (GTPC, "C" indicates the control signaling aspect of the protocol). The recipient GGSN is automatically selected by the SGSN. The message consists of various information elements including: PDP Type, PDP Address, APN, and charging characteristics.
4. The GGSN determines if it can facilitate the session (in terms of memory or CPU resources, configuration, etc.) and creates a new entry in its PDP context list and provides a Charging ID for the session. It determines the PDP context type and based on the APN, what authentication protocol to use and how to perform IP address assignment.

If the MS required the dynamic assignment of an IP address (i.e., the PDP Address received from the mobile was null), the GGSN will assign one. The IP address assignment methods supported by the system GGSN are described in the *Dynamic IP Address Assignment* section of this chapter.

The GGSN replies with an affirmative Create PDP Context Response using GTPC.

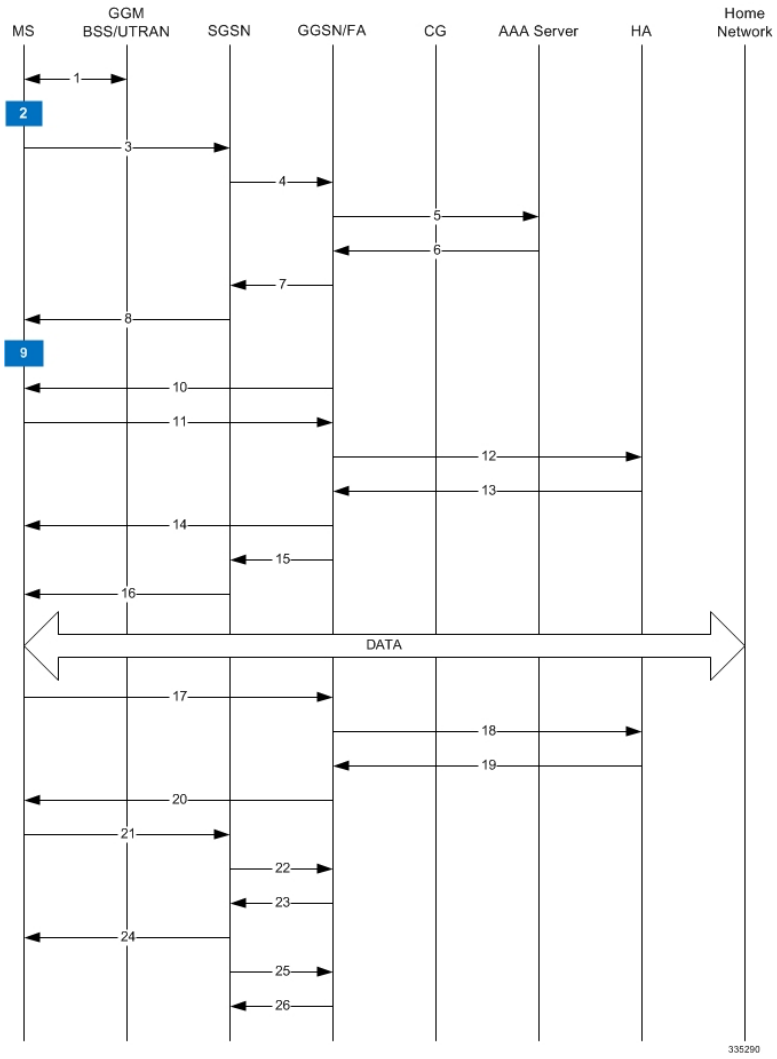
5. The SGSN returns an Activate PDP Context Accept response to the MS.
6. The MS sends IP packets which are received by the GGSN.
7. The GGSN encapsulates the IP packets from the MS using IP-in-IP and tunnels them to the subscriber's corporate network.

   All data sent and received by the MS over the IP-in-IP tunnel facilitated by the GGSN.
8. The MS can terminate the data session at any time. To terminate the session, the MS sends a Deactivate PDP Context Request message that is received by the SGSN.
9. The SGSN sends a Delete PDP Context Request message to the GGSN facilitating the data session. The message includes the information elements necessary to identify the PDP context.
10. The GGSN removes the PDP context from memory and returns a Delete PDP Context Response message to the SGSN. If the PDP context was the last associated with a particular dynamically assigned PDP Address, the GGSN will re-claim the IP address for use by subsequent PDP contexts.
11. The SGSN returns a Deactivate PDP Context Accept message to the MS.
12. The GGSN delivers the GGSN Charging Detail Records (G-CDRs) to a Charging Gateway (CG) using GTP Prime (GTPP). Note that, though not shown in this example, the GGSN could optionally be configured to send partial CDRs while the PDP context is active.
13. For each accounting message received from the GGSN, the CG responds with an acknowledgement.

Mobile IP Call Flow

The following figure and the text that follows describe the call flow for a successful Corporate IP Connectivity data session.

Figure 14: Mobile IP Call Flow



1. The Mobile Station (MS) goes through the process of attaching itself to the GPRS/UMTS network.
2. The Terminal Equipment (TE) aspect of the MS sends AT commands to the Mobile Terminal (MT) aspect of the MS to place it into PPP mode.

   The Link Control Protocol (LCP is then used to configure the Maximum-Receive Unit size and the authentication protocol (Challenge-Handshake Authentication Protocol (CHAP), Password Authentication Protocol (PAP), or none). If CHAP or PAP is used, the TE will authenticate itself to the MT, which, in turn, stores the authentication information.

   Upon successful authentication, the TE sends an Internet Protocol Control Protocol (IPCP) Configure-Request message to the MT. The message will either contain a static IP home address to use or request that one be dynamically assigned.
3. The MS sends an Activate PDP Context Request message that is received by an SGSN. The message contains information about the subscriber such as the Network layer Service Access Point Identifier (NSAPI), PDP Type, Access Point Name (APN), Quality of Service (QoS) requested, and PDP configuration options.

Note that regardless of whether or not the MS has a static address or is requesting a dynamic address, the "Requested PDP Address" field is omitted from the request when using Mobile IP.

4. The SGSN authenticates the request message and sends a Create PDP Context Request message to a GGSN using the GPRS Tunneling Protocol (GTPC, "C" indicates the control signaling aspect of the protocol). The recipient GGSN is selected based on either the request of the MS or is automatically selected by the SGSN. The message consists of various information elements including: PDP Type, Requested PDP con, APN, charging characteristics, and Tunnel Endpoint Identifier (TEID).
5. The GGSN determines if it can facilitate the session (in terms of memory or CPU resources, configuration, etc.) and creates a new entry in its PDP context list and provides a Charging ID for the session.

   From the APN specified in the message, the GGSN determines how to handle the PDP context including whether or not Mobile IP should be used.

   If authentication is required, the GGSN attempts to authenticate the subscriber locally against profiles stored in memory or send a RADIUS Access-Request message to an AAA server.
6. If the GGSN authenticated the subscriber to an AAA server, the AAA server responds with a RADIUS Access-Accept message indicating successful authentication.
7. The GGSN replies to the SGSN with a PDP Context Response using GTPC. The response will contain information elements such as the PDP Address, and PDP configuration options specified by the GGSN. Note that for Mobile IP, the GGSN returns a PDP Address of 0.0.0.0 indicating that it will be reset with a Home address after the PDP context activation procedure.
8. The SGSN returns an Activate PDP Context Accept message to the MS. The message includes response to the configuration parameters sent in the initial request.
9. The MT, will respond to the TE's IPCP Config-request with an IPCP Config-Ack message. This ends the PPP mode between the MT and TE components of the MS.

   Data can now be transmitted between the MS and the GGSN.
10. The FA component of the GGSN sends an Agent Advertisement message to the MS. The message contains the FA parameters needed by the mobile such as one or more card-of addresses. The message is sent as an IP limited broadcast message (i.e. destination address 255.255.255.255), however only on the requesting MS's TEID to avoid broadcast over the radio interface.
11. The MS sends a Mobile IP Registration request to the GGSN/FA. This message includes either the MS's static home address or it can request a temporary address by sending 0.0.0.0 as its home address. Additionally, the request must always include the Network Access Identifier (NAI) in a Mobile-Node-NAI Extension.
12. The FA forwards the registration request from the MS to the HA while the MS's home address or NAI and TEID are stored by the GGSN.
13. The HA sends a registration response to the FA containing the address assigned to the MS.
14. The FA extracts the home address assigned to the MS by the HA from the response and the GGSN updates the associated PDP context. The FA then forwards it to the MS (identified by either the home address or the NAI and TEID).
15. The GGSN issues a PDP context modification procedure to the SGSN in order to update the PDP address for the MS.
16. The SGSN forwards the PDP context modification message to the MS.

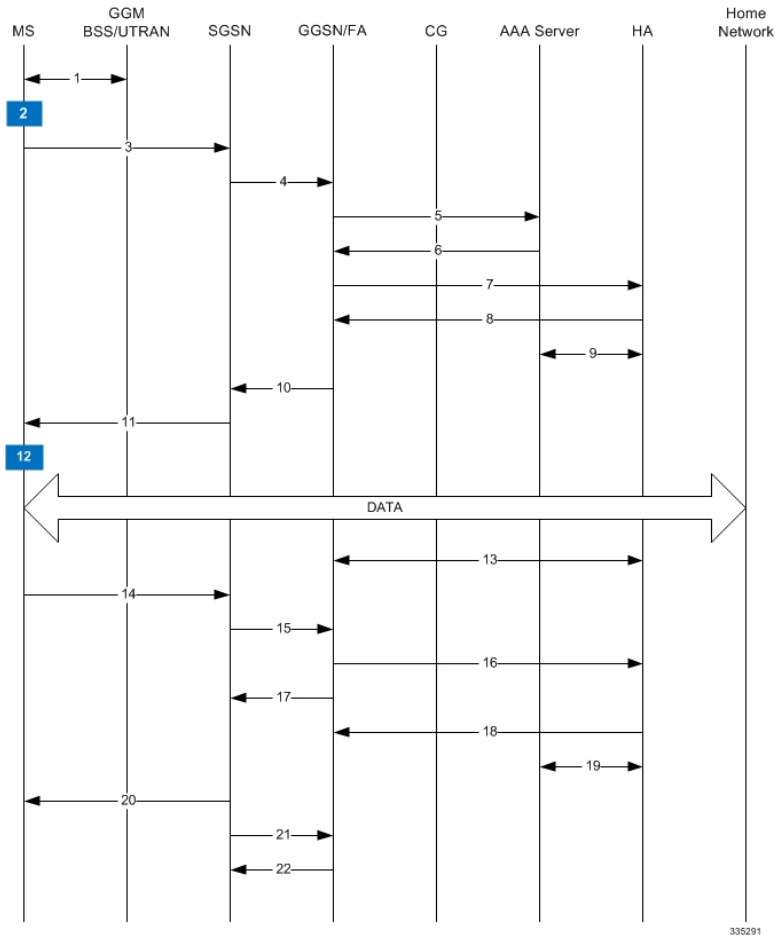
The MS can now send and receive data to or from their home network until the session is closed or times out. Note that for Mobile IP, only one PDP context is supported for the MS.

17. The MS can terminate the Mobile IP data session at any time. To terminate the Mobile IP session, the MS sends a Registration Request message to the GGSN/FA with a requested lifetime of 0.
18. The FA component forwards the request to the HA.
19. The HA sends a Registration Reply to the FA accepting the request.
20. The GGSN/FA forwards the response to the MN.
21. The MS sends a Deactivate PDP Context Request message that is received by the SGSN.
22. The SGSN sends a Delete PDP Context Request message to the GGSN facilitating the data session. The message includes the information elements necessary to identify the PDP context.
23. The GGSN removes the PDP context from memory and returns a Delete PDP Context Response message to the SGSN.
24. The SGSN returns a Deactivate PDP Context Accept message to the MS.
25. The GGSN delivers the GGSN Charging Detail Records (G-CDRs) to a Charging Gateway (CG) using GTP Prime (GTPP). Note that, though not shown in this example, the GGSN could optionally be configured to send partial CDRs while the PDP context is active.
26. For each accounting message received from the GGSN, the CG responds with an acknowledgement.

Proxy Mobile IP Call Flows

The following figure and the text that follows describe a sample successful Proxy Mobile IP session setup call flow in which the MS receives its IP address from the HA.

Figure 15: HA Assigned IP Address Proxy Mobile IP Call Flow



1. The Mobile Station (MS) goes through the process of attaching itself to the GPRS/UMTS network.
2. The Terminal Equipment (TE) aspect of the MS sends AT commands to the Mobile Terminal (MT) aspect of the MS to place it into PPP mode.

   The Link Control Protocol (LCP is then used to configure the Maximum-Receive Unit size and the authentication protocol (Challenge-Handshake Authentication Protocol (CHAP), Password Authentication Protocol (PAP), or none). If CHAP or PAP is used, the TE will authenticate itself to the MT, which, in turn, stores the authentication information.

   Upon successful authentication, the TE sends an Internet Protocol Control Protocol (IPCP) Configure-Request message to the MT. The message will either contain a static IP address to use or request that one be dynamically assigned.
3. The MS sends an Activate PDP Context Request message that is received by an SGSN. The message contains information about the subscriber such as the Network layer Service Access Point Identifier (NSAPI), PDP Type, PDP Address, Access Point Name (APN), Quality of Service (QoS) requested, and PDP configuration options.
4. The SGSN authenticates the request message and sends a Create PDP Context Request message to a GGSN using the GPRS Tunneling Protocol (GTPC, "C" indicates the control signaling aspect of the protocol). The recipient GGSN is selected based on either the request of the MS or is automatically

selected by the SGSN. The message consists of various information elements including: PDP Type, PDP Address, APN, charging characteristics, and Tunnel Endpoint Identifier (TEID, if the PDP Address was static).

5. The GGSN determines if it can facilitate the session (in terms of memory or CPU resources, configuration, etc.) and creates a new entry in its PDP context list and provides a Charging ID for the session.

   From the APN specified in the message, the GGSN determines whether or not the subscriber is to be authenticated, if Proxy Mobile IP is to be supported for the subscriber, and if so, the IP address of the HA to contact.

   Note that Proxy Mobile IP support can also be determined by attributes in the user's profile. Attributes in the user's profile supersede APN settings.

   If authentication is required, the GGSN attempts to authenticate the subscriber locally against profiles stored in memory or send a RADIUS Access-Request message to an AAA server.

6. If the GGSN authenticated the subscriber to an AAA server, the AAA server responds with a RADIUS Access-Accept message indicating successful authentication and any attributes for handling the subscriber PDP context.

7. If Proxy Mobile IP support was either enabled in the APN or in the subscriber's profile, the GGSN/FA forwards a Proxy Mobile IP Registration Request message to the specified HA. The message includes such things as the MS's home address, the IP address of the FA (the care-of-address), and the FA-HA extension (Security Parameter Index (SPI)).

8. The HA responds with a Proxy Mobile IP Registration Response. The response includes an IP address from one of its locally configured pools to assign to the MS (its Home Address). The HA also creates a Mobile Binding Record (MBR) for the subscriber session.

9. The HA sends a RADIUS Accounting Start request to the AAA server which the AAA server responds to.

10. The GGSN replies with an affirmative Create PDP Context Response using GTPC. The response will contain information elements such as the PDP Address representing either the static address requested by the MS or the address assigned by the GGSN, the TEID used to reference PDP Address, and PDP configuration options specified by the GGSN.

11. The SGSN returns an Activate PDP Context Accept message to the MS. The message includes response to the configuration parameters sent in the initial request.

12. The MT, will respond to the TE's IPCP Config-request with an IPCP Config-Ack message.

    The MS can now send and receive data to or from the PDN until the session is closed or times out. Note that for Mobile IP, only one PDP context is supported for the MS.

13. The FA periodically sends Proxy Mobile IP Registration Request Renewal messages to the HA. The HA sends responses for each request.

14. The MS can terminate the data session at any time. To terminate the session, the MS sends a Deactivate PDP Context Request message that is received by the SGSN.

15. The SGSN sends a Delete PDP Context Request message to the GGSN facilitating the data session. The message includes the information elements necessary to identify the PDP context (i.e., TEID, and NSAPI).

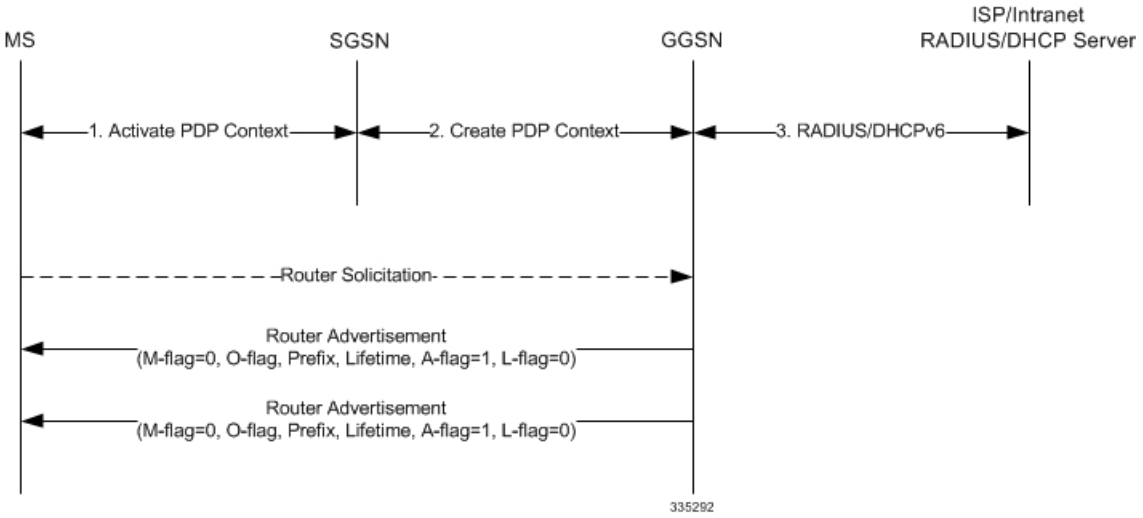
16. The GGSN removes the PDP context from memory and the FA sends a Proxy Mobile IP Deregistration Request message to the HA.

17. The GGSN returns a Delete PDP Context Response message to the SGSN.
18. The HA replies to the FA with a Proxy Mobile IP Deregistration Request Response.
19. The HA sends a RADIUS Accounting Stop request to the AAA server which the AAA server responds to.
20. The SGSN returns a Deactivate PDP Context Accept message to the MS.
21. The GGSN delivers the GGSN Charging Detail Records (G-CDRs) to a Charging Gateway (CG) using GTP Prime (GTPP). Note that, though not shown in this example, the GGSN could optionally be configured to send partial CDRs while the PDP context is active.
22. For each accounting message received from the GGSN, the CG responds with an acknowledgement.

IPv6 Stateless Address Auto Configuration Flows

The following figure and the text that follows describe a sample IPv6 stateless address auto configuration session setup call flow in which the MS receives its IP address from the RADIUS DHCP server.

Figure 16: IPv6 Stateless Address Auto Configuration Flow



1. The MS uses the IPv6 interface identifier provided by the GGSN to create its IPv6 link-local unicast address. Before the MS communicates with other hosts or mobile stations on the intranet/ISP, the MS must obtain an IPv6 global or site-local unicast address.
2. After the GGSN sends a create PDP context response message to the SGSN, it starts sending router advertisements periodically on the new MS-GGSN link established by the PDP context.
3. When creating a global or site-local unicast address, the MS may use the interface identifier received during the PDP context activation or it generates a new interface identifier. There is no restriction on the value of the interface identifier of the global or site-local unicast address, since the prefix is unique.

Supported Standards

The GGSN complies with the following standards for 3GPP wireless data services.

3GPP References

- 3GPP TS 09.60 v7.10.0 (2001-09): 3rd Generation Partnership project; Technical Specification Group Core Network; General Packet Radio Services (GPRS); GPRS Tunneling Protocol (GTP) across the Gn and Gp Interface (Release 1998) for backward compatibility with GTPv0
- 3GPP TS 23.060 v7.6.0 (2007-9): 3rd Generation Partnership project; Technical Specification Group Services and System Aspects; General Packet Radio Service (GPRS); Service description (Release 1999) as an additional reference for GPRS/UMTS procedures
- 3GPP TS 23.107 v7.1.0 (2007-09): 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; QoS Concept and Architecture
- 3GPP TS 23.203 V7.7.0 (2006-08): 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Policy and charging control architecture (Release 7)
- 3GPP TS 23.246 v7.4.0 (2007-09): 3rd Generation Partnership Project, Technical Specification Group Services and System Aspects; Multimedia Broadcast/Multicast Service (MBMS); Architecture and functional description (Release 7)
- 3GPP TS 24.008 v7.11.0 (2001-06): Mobile radio interface layer 3 specification; Core Network Protocols-Stage 3 (Release 1999) as an additional reference for GPRS/UMTS procedures
- 3GPP TS 29.060 v7.9.0 (2008-09): 3rd Generation Partnership Project; Technical Specification Group Core Network; General Packet Radio Services (GPRS); GRPS Tunneling Protocol (GTP) across the Gn and Gp Interface (Release 4) for the Core GTP Functionality
- 3GPP TS 29.061 v7.7.0 (2008-09): 3rd Generation Partnership Project; Technical Specification Group Core Network; Packet Domain; Interworking between the Public Land Mobile Network (PLMN) supporting Packet Based Services and Packet Data Networks (PDN)
- 3GPP 29.212 v7.6.0 (2008-09) 3rd Generation Partnership Project, Technical Specification Group Core Network and Terminals; Policy and Charging Control over Gx reference point (Release 7)
- 3GPP TS 29.213 V7.5.0 (2005-08): 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Policy and Charging Control signalling flows and QoS parameter mapping; (Release 7)
- 3GPP TS 29.281 V10.0.0 (2010-12): 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; General Packet Radio System (GPRS) Tunnelling Protocol User Plane (GTPv1-U) (Release 10)
- 3GPP TR 29.846 6.0.0 (2004-09) 3rd Generation Partnership Project, Technical Specification Group Core Networks; Multimedia Broadcast/Multicast Service (MBMS); CN1 procedure description (Release 6)

- 3GPP TS 32.015 v3.12.0 (2003-12): 3rd Generation Partnership Project, Technical Specification Group Services and System Aspects; Telecommunication Management; Charging management; Call and event data for the Packet Switched (PS) domain (Release 1999) for support of Charging on GGSN
- 3GPP TS 32.215 v5.9.0 (2005-06): 3rd Generation Partnership Project, Technical Specification Group Services and System Aspects; Telecommunication Management; Charging Management; Charging data description for the Packet Switched (PS) domain (Release 5)
- 3GPP 32.251 v7.5.1 (2007-10) 3rd Generation Partnership Project, Technical Specification Group Services and System Aspects; Telecommunication management; Charging management; Packet Switched (PS) domain charging (Release 7)
- 3GPP TS 32.298 v7.4.0 (2007-09): 3rd Generation Partnership Project; Technical Specification Group Service and System Aspects; Telecommunication management; Charging management; Charging Data Record (CDR) parameter description
- 3GPP TS 32.299 v7.7.0 (2007-10): 3rd Generation Partnership Project; Technical Specification Group Service and System Aspects; Telecommunication management; Charging management; Diameter charging applications (Release 7)
- 3GPP TS 32.403 V7.1.0: Technical Specification Performance measurements - UMTS and combined UMTS/GSM
- 3GPP TS 33.106 V7.0.1 (2001-06): 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G security; Lawful Interception requirements (Release 7)
- 3GPP TS 33.107 V7.7.0 (2007-09): 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G security; Lawful interception architecture and functions (Release 7)

IETF References

- RFC-768, User Datagram Protocol (UPD), August 1980
- RFC-791, Internet Protocol (IP), September 1982
- RFC-793, Transmission Control Protocol (TCP), September 1981
- RFC-894, A Standard for the Transmission of IP Datagrams over Ethernet Networks, April 1984
- RFC-1089, SNMP over Ethernet, February 1989
- RFC-1144, Compressing TCP/IP headers for low-speed serial links, February 1990
- RFC-1155, Structure & identification of management information for TCP/IP-based Internets, May 1990
- RFC-1157, Simple Network Management Protocol (SNMP) Version 1, May 1990
- RFC-1212, Concise MIB Definitions, March 1991
- RFC-1213, Management Information Base for Network Management of TCP/IP-based Internets: MIB-II, March 1991
- RFC-1215, A Convention for Defining Traps for use with the SNMP, March 1991
- RFC-1224, Techniques for managing asynchronously generated alerts, May 1991
- RFC-1256, ICMP Router Discovery Messages, September 1991

- RFC-1305, Network Time Protocol (Version 3) Specification, Implementation and Analysis, March 1992
- RFC-1332, The PPP Internet Protocol Control Protocol (IPCP), May 1992
- RFC-1398, Definitions of Managed Objects for the Ethernet-Like Interface Types, January 1993
- RFC-1418, SNMP over OSI, March 1993
- RFC-1570, PPP LCP Extensions, January 1994
- RFC-1643, Definitions of Managed Objects for the Ethernet-like Interface Types, July 1994
- RFC-1661, The Point to Point Protocol (PPP), July 1994
- RFC-1662, PPP in HDLC-like Framing, July 1994
- RFC-1701, Generic Routing Encapsulation (GRE), October 1994
- RFC-1850, OSPF Version 2 Management Information Base, November 1995
- RFC-1901, Introduction to Community-based SNMPv2, January 1996
- RFC-1902, Structure of Management Information for Version 2 of the Simple Network Management Protocol (SNMPv2), January 1996
- RFC-1903, Textual Conventions for Version 2 of the Simple Network Management Protocol (SNMPv2), January 1996
- RFC-1904, Conformance Statements for Version 2 of the Simple Network Management Protocol (SNMPv2), January 1996
- RFC-1905, Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2), January 1996
- RFC-1906, Transport Mappings for Version 2 of the Simple Network Management Protocol (SNMPv2), January 1996
- RFC-1907, Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2), January 1996
- RFC-1908, Coexistence between Version 1 and Version 2 of the Internet-standard Network Management Framework, January 1996
- RFC-1918, Address Allocation for Private Internets, February 1996
- RFC-1919, Classical versus Transparent IP Proxies, March 1996
- RFC-1962, The PPP Compression Control Protocol (CCP), June 1996
- RFC-1974, PPP STAC LZS Compression Protocol, August 1996
- RFC-2002, IP Mobility Support, May 1995
- RFC-2003, IP Encapsulation within IP, October 1996
- RFC-2004, Minimal Encapsulation within IP, October 1996
- RFC-2005, Applicability Statement for IP Mobility Support, October 1996
- RFC-2118, Microsoft Point-to-Point Compression (MPPC) Protocol, March 1997

- RFC 2131, Dynamic Host Configuration Protocol
- RFC 2132, DHCP Options and BOOTP Vendor Extensions
- RFC-2136, Dynamic Updates in the Domain Name System (DNS UPDATE)
- RFC-2211, Specification of the Controlled-Load Network Element Service
- RFC-2246, The Transport Layer Security (TLS) Protocol Version 1.0, January 1999
- RFC-2290, Mobile-IPv4 Configuration Option for PPP IPCP, February 1998
- RFC-2328, OSPF Version 2, April 1998
- RFC-2344, Reverse Tunneling for Mobile IP, May 1998
- RFC-2394, IP Payload Compression Using DEFLATE, December 1998
- RFC 2401, Security Architecture for the Internet Protocol
- RFC 2402, IP Authentication Header (AH)
- RFC 2406, IP Encapsulating Security Payload (ESP)
- RFC 2409, The Internet Key Exchange (IKE)
- RFC-2460, Internet Protocol Version 6 (IPv6)
- RFC-2461, Neighbor Discovery for IPv6
- RFC-2462, IPv6 Stateless Address Autoconfiguration
- RFC-2474, Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers, December 1998
- RFC-2475, An Architecture for Differentiated Services, December 1998
- RFC-2484, PPP LCP Internationalization Configuration Option, January 1999
- RFC-2486, The Network Access Identifier (NAI), January 1999
- RFC-2571, An Architecture for Describing SNMP Management Frameworks, April 1999
- RFC-2572, Message Processing and Dispatching for the Simple Network Management Protocol (SNMP), April 1999
- RFC-2573, SNMP Applications, April 1999
- RFC-2574, User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3), April 1999
- RFC-2597, Assured Forwarding PHB Group, June 1999
- RFC-2598, Expedited Forwarding PHB, June 1999
- RFC-2618, RADIUS Authentication Client MIB, June 1999
- RFC-2620, RADIUS Accounting Client MIB, June 1999
- RFC-2661, Layer Two Tunneling Protocol "L2TP", August 1999
- RFC-2697, A Single Rate Three Color Marker, September 1999

- RFC-2698, A Two Rate Three Color Marker, September 1999
- RFC-2784, Generic Routing Encapsulation (GRE) - March 2000, IETF
- RFC-2794, Mobile IP Network Access Identifier Extension for IPv4, March 2000
- RFC-2809, Implementation of L2TP Compulsory Tunneling via RADIUS, April 2000
- RFC-2845, Secret Key Transaction Authentication for DNS (TSIG), May 2000
- RFC-2865, Remote Authentication Dial In User Service (RADIUS), June 2000
- RFC-2866, RADIUS Accounting, June 2000
- RFC-2867, RADIUS Accounting Modifications for Tunnel Protocol Support, June 2000
- RFC-2868, RADIUS Attributes for Tunnel Protocol Support, June 2000
- RFC-2869, RADIUS Extensions, June 2000
- RFC-3007, Secure Domain Name System (DNS) Dynamic Update, November 2000
- RFC-3012, Mobile IPv4 Challenge/Response Extensions, November 2000
- RFC-3056, Connection of IPv6 Domains via IPv4 Clouds, February 2001
- RFC-3101 OSPF-NSSA Option, January 2003
- RFC-3143, Known HTTP Proxy/Caching Problems, June 2001
- RFC-3193, Securing L2TP using IPSEC, November 2001
- RFC-3314, Recommendations for IPv6 in Third Generation Partnership Project (3GPP) Standards, September 2002
- RFC-3316, Internet Protocol Version 6 (IPv6) for Some Second and Third Generation Cellular Hosts, April 2003
- RFC-3706, A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers, February 2004
- RFC-3543, Registration Revocation in Mobile IPv4, August 2003
- RFC 3588, Diameter Base Protocol, September 2003
- RFC 4006, Diameter Credit-Control Application, August 2005
- Draft, Route Optimization in Mobile IP
- Draft, Generalized Key Distribution Extensions for Mobile IP
- Draft, AAA Keys for Mobile IP

Object Management Group (OMG) Standards

CORBA 2.6 Specification 01-09-35, Object Management Group