



CHAPTER 1

Overview of GPRS and UMTS

This chapter provides a brief introduction to the 2.5G general packet radio service (GPRS) and the 3G Universal Mobile Telecommunication System (UMTS) technologies and their implementation in Cisco IOS GGSN software.

This chapter includes the following sections:

- [Overview, page 1-1](#)
- [Benefits, page 1-4](#)
- [New Features in this Release, page 1-5](#)
- [Features from Previous Releases, page 1-9](#)

Overview

GPRS and UMTS are evolutions of the global system for mobile communication (GSM) networks. GSM is a digital cellular technology that is used worldwide, predominantly in Europe and Asia. GSM is the world's leading standard in digital wireless communications.

GPRS is a 2.5G mobile communications technology that enables mobile wireless service providers to offer their mobile subscribers packet-based data services over GSM networks. Common applications of GPRS include the following: Internet access, intranet/corporate access, instant messaging, and multimedia messaging. GPRS was standardized by the European Telecommunications Standards Institute (ETSI), but today is standardized by the Third Generation Partnership Program (3GPP).

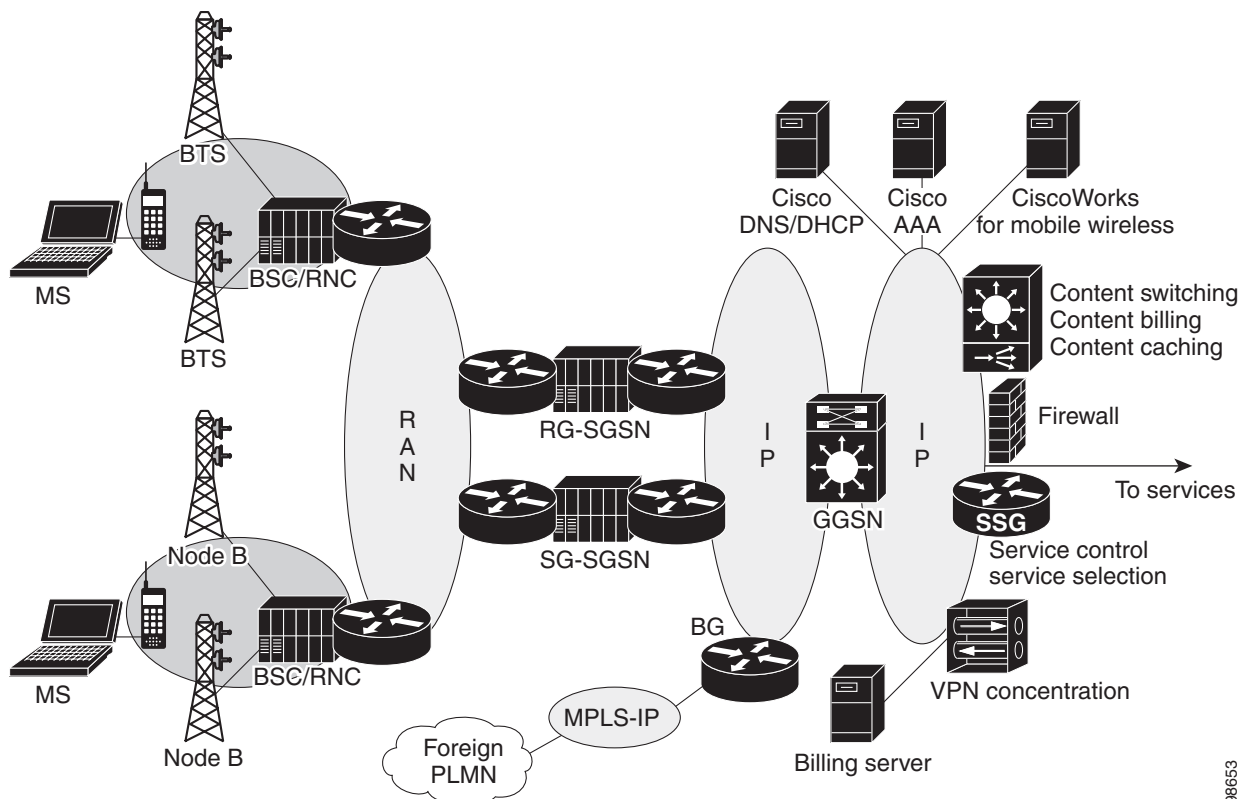
UMTS is a 3G mobile communications technology that provides wideband code division multiple access (W-CDMA) radio technology. The W-CDMA technology offers higher throughput, real-time services, and end-to-end quality of service (QoS), and delivers pictures, graphics, video communications, and other multimedia information as well as voice and data to mobile wireless subscribers. UMTS is standardized by the 3GPP.

The GPRS/UMTS packet core comprises two major network elements:

- Gateway GPRS support node (GGSN)—a gateway that provides mobile cell phone users access to a public data network (PDN) or specified private IP networks. The GGSN is implemented via Cisco IOS software on the Cisco Service and Application Module for IP (SAMI) installed in a Cisco 7600 series router.
- Serving GPRS support node (SGSN)—connects the radio access network (RAN) to the GPRS/UMTS core and tunnels user sessions to the GGSN. The SGSN sends data to and receives data from mobile stations, and maintains information about the location of a mobile station (MS). The SGSN communicates directly with the MS and the GGSN. SGSN support is available from Cisco partners or other vendors.

Figure 1-1 shows the network components with the GGSNs implemented on the Cisco SAMI in the Cisco 7600 series router.

Figure 1-1 GPRS/UMTS Network Components with GGSNs Implemented on the Cisco SAMI in the Cisco 7600 Series Router



Note that, as Figure 1-1 shows, the RAN is made up of different components for 2.5G and 3G.

In a 2.5G environment, the RAN is composed of mobile stations that connect to a base transceiver station (BTS) that connects to a base station controller (BSC). In a 3G environment, the RAN is made up of mobile stations that connect to NodeB, which connects to a radio network controller (RNC).

The RAN connects to the GPRS/UMTS core through an SGSN, which tunnels user sessions to a GGSN that acts as a gateway to the services networks (for example, the Internet and intranet). The connection between the SGSN and the GGSN is enabled through a tunneling protocol called the GPRS tunneling

protocol (GTP)—GTP Version 0 (GTPv0) for 2.5G applications, and GTP Version 1 (GTPv1) for 3G applications. GTP is carried over IP. Multiple SGSNs and GGSNs within a network are referred to collectively as GPRS support nodes (GSNs).

**Note**

Depending on the specific operator configuration, the RAN, the GPRS/UMTS core, and the services networks can be made up of IP or Multiprotocol Label Switching (MPLS) networks.

To assign mobile sessions an IP address, the GGSN uses the Dynamic Host Configuration Protocol (DHCP), Remote Authentication Dial-In User Service (RADIUS) server, or a local address pool defined specified on an access point configured on the GGSN. The GGSN can use a RADIUS server to authorize and authenticate remote users. DHCP and RADIUS services can be specified either at the global configuration level or for each access point configured on the GGSN.

With the Cisco SAMI installed in a Cisco 7600 series router, IPsec encryption is performed on the IPsec Virtual Private Network (VPN) Acceleration Services Module.

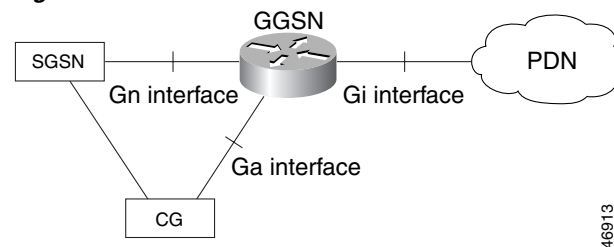
GPRS Interface Reference Model

The 2.5G GPRS and 3G UMTS standards use the term *interface* to label (or identify) the communication path between different network elements. The GPRS/UMTS standards define the requirements and characteristics of communication between different GPRS/UMTS network elements over these interfaces. These interfaces are commonly referred to in descriptions of GPRS/UMTS networks.

Figure 1-2 shows the primary interfaces that are implemented in the Cisco GGSN feature:

- Gn interface—Interface between GSNs within the same public land mobile network (PLMN) in a GPRS/UMTS network. GTP is a protocol defined on the Gn interface between GSNs in a GPRS/UMTS network.
- Gi interface—Reference point between a GPRS/UMTS network and an external packet data network.
- Ga interface—Interface between a GGSN and charging gateway (CG) in a GPRS/UMTS network.

Figure 1-2 GGSN Interfaces

**Virtual Template Interface**

To facilitate configuration of connections between the GGSN and SGSN, and the GGSN and PDNs, the Cisco IOS GGSN software uses an internal interface called a virtual template interface. A virtual template is a logical interface that is not tied directly to a specific interface, but that can be associated dynamically with a interface.

As with a physical interface on a router, you can assign an IP address to the virtual template interface. You can also configure IP routing characteristics on the virtual template interface. You are required to configure certain GPRS/UMTS-specific elements on the virtual template interface, such as GTP encapsulation (which is necessary for communicating with the SGSN) and the access list that the GGSN uses to determine which PDNs are accessible on the network.

Access Points

The GPRS/UMTS standards define a network identity called an access point name (APN). An APN identifies the service or network to which a user can connect from a GGSN in a GPRS/UMTS network.

To configure APNs, the Cisco IOS GGSN software uses the following configuration elements:

- Access point—Defines an APN and its associated access characteristics, including security and method of dynamic addressing.
- Access point list—Logical interface that is associated with the virtual template of the GGSN. The access-point list contains one or more access points.
- Access group—An additional level of security that is configured at an access point to control access to and from a PDN. When an MS is permitted access to the GGSN as defined by a traditional IP access list, the IP access group further defines whether access is permitted to the PDN (at the access point). The IP access group configuration can also define whether access from a PDN to an MS is permitted.

For more detailed information on access-point configuration, refer to the [“Configuring Access Points on the GGSN” section on page 8-7](#).

Benefits

The 2.5G GPRS technology provides the following benefits:

- Enables the use of a packet-based air interface over the existing circuit-switched GSM network, which allows greater efficiency in the radio spectrum because the radio bandwidth is used only when packets are sent or received
- Supports minimal upgrades to the existing GSM network infrastructure for network service providers who want to add GPRS services on top of GSM, which is currently widely deployed
- Supports enhanced data rates in comparison to the traditional circuit-switched GSM data service
- Supports larger message lengths than Short Message Service (SMS)
- Supports a wide range of access to data networks and services, including VPN/Internet service provider (ISP) corporate site access and Wireless Application Protocol (WAP).

In addition to the above, the 3G UMTS technology includes the following:

- Enhanced data rates of approximately
 - 144 kbps—Satellite and rural outdoor
 - 384 kbps—Urban outdoor
 - 2048 kbps—Indoor and low-range outdoor
- Supports connection-oriented Radio Access Bearers with specified QoS, enabling end-to-end QoS

New Features in this Release

Cisco GGSN Release 8.0, Cisco IOS Release 12.4(15)XQ, introduces support for the following features:

- [GGSN-Initiated Update PDP Context Requests, page 1-5](#)
- [RADIUS Change of Authorization Message, page 1-5](#)
- [Downloadable QoS Profile, page 1-6](#)
- [PPP-Regeneration Scalability, page 1-6](#)
- [AAA Enhancements, page 1-6](#)
- [Anonymous User Access for PPP-Regeneration, page 1-7](#)
- [Downloadable Pool Name Support, page 1-7](#)
- [Direct Tunnel Support, page 1-7](#)
- [Configuring a Charging Source Interface, page 1-8](#)
- [Suppressing Echo Requests per SGSN, page 1-8](#)
- [iSCSI Transport Protocol Support, page 1-9](#)
- [MIB Enhancements, page 1-9](#)

GGSN-Initiated Update PDP Context Requests

With this release, a Cisco GGSN can send an Update PDP Context Request (as defined in 3GPP TR 29.060 v7.5.1, section 7.3.3) to an SGSN to negotiate the QoS of a PDP context.

An external entity, such as the Cisco Content Services Gateway (CSG) in an Gx environment, can push a new QoS profile to the GGSN to apply on a particular PDP context. The GGSN then pushes the changes to the RAN in an Update PDP Context Request to the SGSN.

Additionally, when a direct tunnel is being used for a PDP context, the GGSN sends an Update PDP Context Request to an SGSN in response to an error indication message from a Radio Network Controller (RNC).

For detailed information about GGSN-initiated Update PDP Context Requests, see the [“Configuring Support for GGSN-Initiated Update PDP Context Requests”](#) section on page 3-26.

RADIUS Change of Authorization Message

The RADIUS Change of Authorization (CoA) message contains information for dynamically changing session authorizations. With Cisco GGSN Release 8.0, the GGSN utilizes the base Cisco IOS AAA to support the RADIUS CoA message, as defined by RFC 3576, but with an additional 3GPP QoS attribute indicates the updated QoS and the Acct-Session-ID to identify the PDP context.

The QoS vendor-specific attribute (VSA) is a string with bytes encoded with QoS attributes as defined by 3GPP TS 24.008, and the Accounting-session-id is a string using the standard attribute type 44.

The following is an example, using VSA vendor-ID 10415 code 5 string:

```
99-1333172B7BEAF52312C6C701
```

The CoA is received on port 1700.

For detailed information about AAA and RADIUS, see the *Cisco IOS Security Configuration Guide, Release 12.4*.

To ensure that the interim accounting record is generated as a part of the CoA procedure, confirm that the following exists:

- Globally, the **aaa accounting update newinfo** global configuration command has been configured.
- Under the APN, the **aaa-accounting** access-point configuration command has been configured with the **interim update** keyword option specified.

No commands have been introduced for the RADIUS CoA message support.

Downloadable QoS Profile

With Release 8.0, the Cisco GGSN supports downloading QoS profiles from an AAA server.

If an APN is configured in non-transparent mode, a user is authenticated before the PDP context is created. GGSN sends an access-request to AAA server with parameters in the user provided PCO option (or using anonymous authentication if anonymous user is enabled on APN).

In the access-accept message from the RADIUS server, user-specific attributes such as the session and idle timeout values, can be downloaded and applied to the PDP context. In addition to these attributes, the Cisco GGSN supports downloading the QoS profile via the QoS VSA (as defined by 3GPP TS 24.008). If a 3GPP QoS profile attribute is received from an AAA server in an access-accept message, the GGSN retrieves the attribute and applies it to the PDP context. If the attribute is not valid, or there is a format error in the attribute, the attribute is ignored and the SGSN requested QoS profile is used for QoS negotiation.

The 3GPP QoS attribute has a vendor-id of 10415 and code 5:

```
99-1333172B7BEAF52312C6C701
```

No commands have been introduced for the downloadable QoS profile support.

PPP-Regeneration Scalability

This release of the Cisco GGSN allows PDPs regenerated to a PPP session to run on software interface description blocks (IDBs). Allowing PPP sessions to run on software IDBs, can increase the number of supported sessions.

No commands have been introduced for the PPP-regeneration scalability support.

AAA Enhancements

Cisco GGSN Release 8.0 utilizes the base Cisco IOS AAA functionality introduced to provide support for the following:

- Simultaneous method list level broadcast and wait accounting
- Per-session timer for interim accounting records (periodic accounting timer)

For detailed information about configuring broadcast and wait accounting to work together, see the [“Configuring Simultaneous Broadcast and Wait Accounting”](#) section on page 11-30.

For detailed information about configuring a periodic accounting timer, see [“Periodic Accounting Timer”](#) section on page 11-32.

Anonymous User Access for PPP-Regeneration

Anonymous user access for PPP-regenerated PDPs is supported with Cisco GGSN Release 8.0 and later.

Anonymous user access support for PPP-regenerated PDPs enables PDPs to be created for users who cannot send a username and password (for example, WAP users).

When the **anonymous user** access-point user configuration command is configured under an APN that is configured for PPP regeneration, when a create PDP context request is received (for a PPP-regenerated PDP) that contains no username and password in the PCO IE, then the anonymous user configuration under that APN is sent to the LNS for authentication. However, if the PCO IE contains a username and password, the tunnel to the LNS is created using the supplied username and password, even though anonymous user is configured under the APN.

The username and password in the create PDP context request takes higher precedence than the anonymous user configuration.

No commands have been introduced or modified to support this feature.

For information about configuring anonymous user access under an APN, see the [“Configuring Additional Real Access Point Options”](#) section on page 8-20.

Downloadable Pool Name Support

When the **ip-address-pool radius-client** access-point configuration command is configured under an APN, if an address pool name is received as a part of the Access-Accept message while authenticating the user, the address pool is used to assign the IP address to the mobile station. If the Access-Accept message also includes an IP address, the IP address takes precedent over the address pool name, and the IP address in the Access-Accept message is used instead of being allocated from the pool.

No commands have been introduced or modified to support this feature on the GGSN.

To configure downloadable pool names, ensure that the **ip-address pool** access-point configuration command with the **radius-client** keyword option is configured under the APN as in the following example:

```
gprs access-point-list gprs
  access-point 3
    access-point-name qos1.com
    ip-address-pool radius-client
  ...

ip local pool pool1500 ipaddress ipaddress
```

For more information about the **ip-address-pool** access-point configuration command, see [“Configuring Additional Real Access Point Options”](#) section on page 8-20. For more information about configuring RADIUS, see the *Cisco IOS Security Configuration Guide*.

Direct Tunnel Support

Direct tunnels is an optional feature that enables an SGSN to establish a direct user plane tunnel between the radio network controller (RNC) and a GGSN.

The SGSN functions as the gateway between the RNC and the core network, handling both signaling traffic to keep track of the location of mobile devices, as well as the actual data packets being exchanged between the mobile device and the Internet.

Prior to Cisco GGSN Release 8.0, a tunnel could only exist between the GGSN and the SGSN and another tunnel between the SGSN and the RNC. With this tunnel configuration, all data packets have to pass through the SGSN, which has to terminate one tunnel, extract the packet, and put it into another tunnel. This process takes time and processing power.

With direct tunnel support, the SGSN can initiate a direct tunnel between the RNC and the GGSN and no longer have to process data packets. The SGSN will continue to manage location issues by modifying the tunnel if a mobile device moves to an area served by another RNC.

Specifically, direct tunnels processing is as follows:

1. The SGSN initiates the direct tunnel with an Update PDP Context Request that contains the following elements:
 - Direct Tunnel Flags IE with the DTI bit set to 1.
 - The RNC user traffic address
 - Data TEID
2. The GGSN updates the RNC user traffic address and Data TEID and uses the updated information when sending G-PDUs for the MS.
3. If the GGSN receives an Error Indication message from the RNC user traffic address, the GGSN initiates an Update PDP Context Request that includes the Direct Tunnel Flags IE with the Error Indication bit set.
4. The GGSN drops subsequent packet to the MS address until the Update PDP Context response is received from the SGSN.
5. When the Update PDP Context Response is received from the SGSN, if the cause is “Request Accepted,” the PDP is preserved. If the cause is “Not Request Accepted,” the PDP is deleted locally.


Note

Direct tunnel support does not apply to international roaming or when the SGSN is asked by a prepaid system to count the traffic flow.

No commands have been introduced or modified to support this feature on the GGSN.

Configuring a Charging Source Interface

By default, the global GTP virtual template interface is used for all charging messages. With this release of the Cisco GGSN, you can configure a loopback interface, and configure the GGSN to use that loopback interface for all charging messages. This feature enables charging network traffic to be segregated into a VRF or private VLAN. Once the charging source interface is specified, the GTP path to the charging gateways will be recreated with the new address obtained from the loopback interface.

For detailed information about configuring a charging source interface, see [“Configuring a Charging Source Interface”](#) section on page 6-5.

Suppressing Echo Requests per SGSN

Echo requests can be disabled per SGSN and/or UDP port. This feature enables operators to selectively disable echo requests to GSNs that might not have the capability to respond to echo requests from the GGSN entirely, or only those echo requests received on certain UDP ports, while keeping the echo requests intact for the other SGSNs.

When a new path is created, the GGSN checks to see if the path parameters, namely the destination address and port, matches any of the conditions configured when suppressing echo requests. If the parameters match, the GGSN sets the path echo interval to 0 for that path. Otherwise, the global path echo interval configuration is used to send echo requests.

For detailed information about suppressing echo requests, see [“Suppressing Echo Requests per SGSN” section on page 3-25](#).

iSCSI Transport Protocol Support

With Cisco GGSN Release 8.0 and later, you can configure the GGSN to backup G-CDRs to, and retrieve G-CDRs from, a storage target on a Storage Area Network (SAN) when a charging gateway is unavailable.

The Cisco GGSN utilizes the Cisco IOS software Small Computer Systems Interface over IP (iSCSI) support, as defined in RFC 3720, to enable G-CDR storage and retrieval from SAN storage.

For detailed information about configuring G-CDR back on an iSCSI target, see [“Configuring G-CDR Backup and Retrieval using iSCSI” section on page 6-18](#).

MIB Enhancements

New configuration, status, and statistic MIB objects have been added to support following Cisco GGSN Release 8.0 features:

- APN-level Periodic Accounting Timer
- PPP-Regeneration Scalability
- Direct tunnels
- Change of Authorization
- GGSN-initiated Update PDP Contexts

For detailed information about Configuring MIB support, see [Appendix A, “Monitoring Notifications.”](#)

Features from Previous Releases

In addition to the features introduced in this release, the Cisco GGSN also supports the following features and functionality introduced in prior releases:

- Release 99 (R99), Release 98 (R98), and Release 97 (R97) support and compliance
- GTPv0 and GTPv1 messaging
- IP Packet Data Protocol (PDP) and PPP PDP types
- Cisco Express Forwarding (CEF) switching for both GTPv0 and GTPv1, and for IP and PPP PDP types
- For GTPv1 PDPs, support of up to 11 secondary PDP contexts
- Virtual APNs
- VRF per APN support
- Multiple APNs per VRF

- VPN support
 - Generic routing encapsulation (GRE) tunneling
 - Layer 2 Tunneling Protocol (L2TP) extension for PPP PDP type
 - PPP Regeneration for IP PDP type
 - 802.1Q virtual LANs (VLANs)
- Security features
 - Duplicate IP address protection
 - PLMN range checking
 - Blocking of foreign mobile stations
 - Anti-spoofing
 - Mobile-to-mobile redirection
- Quality of service (QoS)
 - UMTS classes and interworking with differentiated services (DiffServ)
 - Delay QoS
 - Canonical QoS
 - GPRS QoS (R97/R98) conversion to UMTS QoS (R99) and the reverse
 - Call Admission Control (CAC)
 - Per-PDP policing
- Dynamic address allocation
 - External DHCP server
 - External RADIUS server
 - Local pools
- Per-APN statistics
- Anonymous access
- RADIUS authentication and accounting
- Accounting
 - Wait accounting
 - Per-PDP accounting
 - Authentication and accounting using RADIUS server groups mapped to APNs
 - 3GPP vendor-specific attributes (VSAs) for IP PDP type
 - Transparent mode accounting
 - Class attribute
 - Interim updates
 - Session idle timer
 - Packet of Disconnect (PoD)
- Dynamic Echo Timer
- GGSN interworking between 2.5G and 3G SGSNs with registration authority (RA) update from
 - 2.5G to 2.5G SGSN

- 2.5G to 3G SGSN
 - 3G to 3G SGSN
 - 3G to 2.5G SGSN
- Charging
 - Time trigger
 - Charging profiles
 - Tertiary charging gateway
 - Switchback to primary charging gateway
- Maintenance mode
- Multiple trusted PLMN IDs
- GGSN-IOS SLB messaging
- Session timeout
- High Speed Downlink Data Packet Access (HSDPA) and associated 3GPP R5 (as required).
- Enhanced Virtual APN
- New information elements (IEs) sent from the SGSN (user location, radio access technology [RAT], MS time zone (MSTZ), Customized Application for Mobile Enhanced Logic [CAMEL] charging information, and user location information IEs)
- GTP SLB stickiness
- P-CSCF Discovery
- Enhanced MIBs for Cisco Content Services Gateway (CSG) and Diameter Credit Control Application (DCCA)

