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

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 mutlimedia messaging. GPRS was standardized by the European Telecommunications Standards Institute (ETSI), but today is standardized by the Third Generation Partnership Program (3GPP).

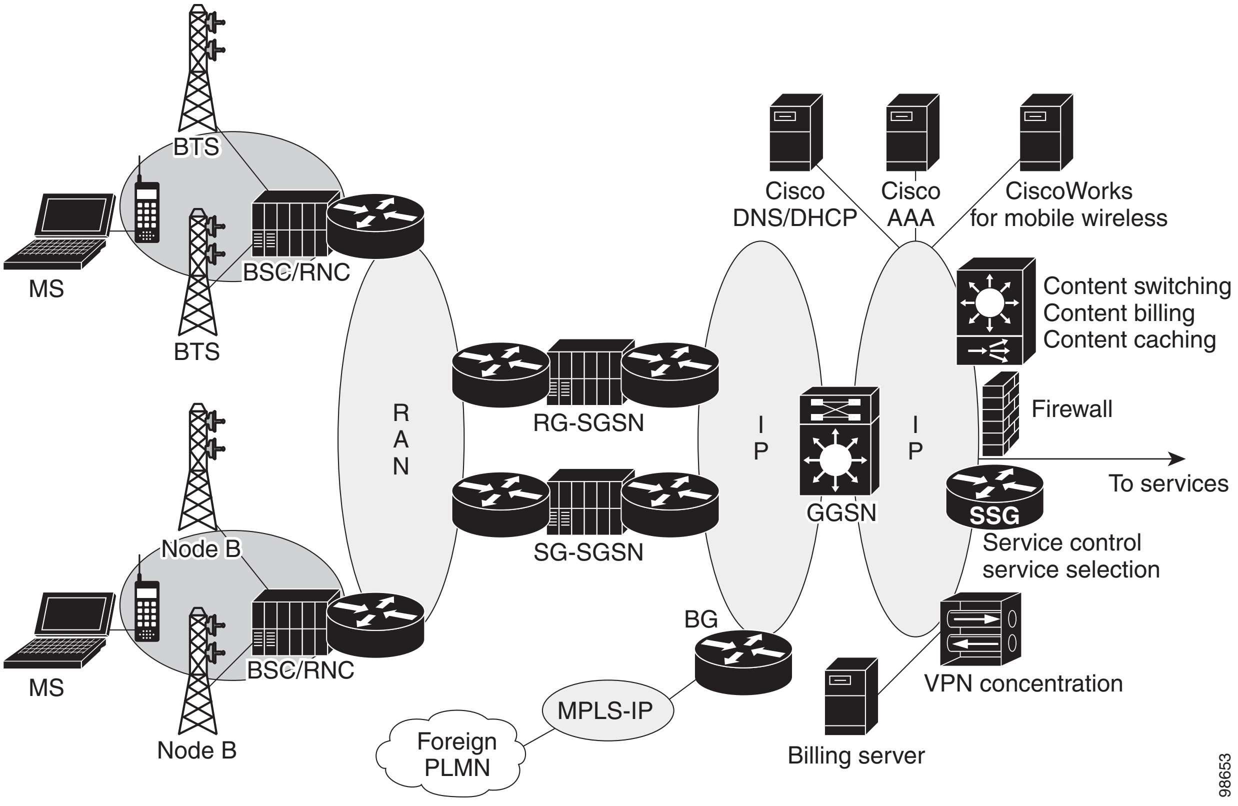
UMTS is a 3G mobile communications technology that provides wideband code division multiple access (W-CDMA) radio technology. The W-CDMA technology offers higher throughput, real-time services, and end-to-end quality of service (QoS), and delivers pictures, graphics, video communications, and other multimedia 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 function is implemented via Cisco IOS software on the Cisco Multi-Processor WAN Application Module (MWAM) installed in a Cisco 7600 series router. Cisco IOS GGSN Release 4.0 and later provides both the 2.5G GPRS and 3G UMTS GGSN functions.
- 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 MWAM in the Cisco 7600 series router.

Figure 1-1 GPRS/UMTS Network Components with GGSNs Implemented on the Cisco MWAM 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 (GTP V0) for 2.5G applications, and GTP Version 1 (GTP V1) 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.

On the Cisco MWAM installed in a Cisco 7600 series router, IPSec encryption is performed on the IPSec Virtual Private Network (VPN) Acceleration Services Module.

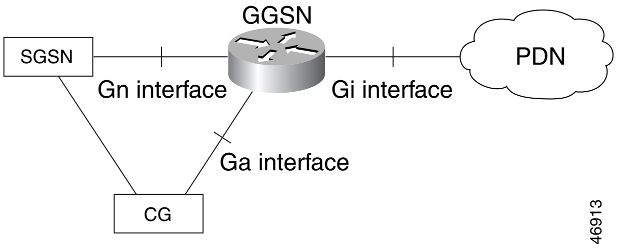
GPRS Interface Reference Model

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 interfaces that are implemented in the Cisco IOS 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 GPRS 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 7-7.

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 7.0, Cisco IOS Release 12.4(9)XG, introduces support for the following features:

- AAA Enhancements, page 1-5
- Hold Back Timer, page 1-5
- IPv6 PDP Context Support, page 1-6
- GTP APN-Aware Load Balancing, page 1-6
- PLMN and RAT Trigger Support for Service-Aware PDPs, page 1-6
- Command Line Interface Enhancements, page 1-6
- MIB Enhancements for IPv6 PDP Support, page 1-7

AAA Enhancements

The maximum number of AAA method lists supported by the GGSN has been increased to 500. This enables up to 500 access-points to each have their own AAA method list.

Note Increasing the maximum number of AAA method lists supported on the GGSN to 500 can result in a very large router configuration file. Therefore, all configurations stored locally on the MWAM will automatically be compressed. If the configuration is stored on the supervisor engine, it is stored in the decompressed format. Therefore, the **service compress-configuration** command is disabled.

Additionally, with this release of the Cisco GGSN, you can display and clear RADIUS counters by server group using the **show aaa servers sg** privileged EXEC command and the **clear aaa counters servers sg** privileged EXEC command. For more information about using these commands, refer to the command description in the *Cisco GGSN Command Reference*.

Hold Back Timer

The IP local pool holdback timer enables you to configure the GGSN to wait a specific amount of time before returning a newly-released IP address to the local pool when using a local IP address pool for allocating addresses to mobile stations.

The hold back timer ensures that an IP address recently released when a PDP session was deleted is not re-assigned to another PDP context before the IP-to-user relationship has been deleted from all back-end components of the system. If an IP address is reassigned to a new PDP context immediately, the back-end system might incorrectly associate the new user with the record of the previous user, and thereby associate the charging and service access of the new user to the previous user.

The hold back timer is unique per pool, and the pool is assigned to the access point. The hold back functionality is delivered by the support of a new timestamp field added to the pool element data structure.

For more information on the hold back timer, including how to configure the timer, see the "Configuring MS Addressing via Local Pools on the GGSN" section on page 11-10.

IPv6 PDP Context Support

Cisco GGSN supports IPv6 primary PDP context activation, and SGSN-initiated modification and deactivation procedures via IPv6 stateless autoconfiguration (as specified by RFC 2461 and RFC 2462). IPv6 over IPv4 tunnels configured on the Cisco 7600 supervisor engine establish connectivity between isolated or remote IPv6 networks over an existing IPv4 infrastructure.

For information on configuring IPv6 support on the Cisco GGSN, and a complete list of IPv6 PDP supported features and restrictions, see Chapter 4, "Configuring IPv6 PDP Support on the GGSN.".

GTP APN-Aware Load Balancing

GTP APN-aware load balancing enables requests to be balanced across APNs. With GTP APN-aware load balancing, Cisco IOS SLB GTP maps that group APNs can be created and associated with a server farm under the virtual template. Multiple server farms can be defined in one virtual server, each supporting a different set of APNs.

For information on configuring GTP APN-aware load balancing, see Chapter 1, "Configuring Load Balancing on the GGSN."

PLMN and RAT Trigger Support for Service-Aware PDPs

The Cisco GGSN supports public land mobile network ID (PLMN-ID) and radio access technology (RAT) triggers for service-aware PDPs.

Using the **content postpaid** charging profile command for postpaid users, and the **trigger** DCCA profile configuration command for prepaid users, you can configure the GGSN to send a quota reauthorization request when a PLMN-ID or RAT change occurs.

Support for the PLMN-ID and RAT triggers requires that the GGSN be configured to include the PLMN ID and/or RAT fields using the **gprs service record include** global configuration command.

Note With this release of the Cisco GGSN, all triggers must be explicitly enabled for both prepaid and postpaid users.

For more information on configuring triggers for service-aware PDPs, see the "Configuring Enhanced Service-Aware Billing" chapter.

Command Line Interface Enhancements

New commands have been introduced or existing commands have been modified, to support the following featurettes introduced in Cisco GSSN Release 7.0, Cisco IOS Release 12.4(9)XG.

Clearing Global and Per-APN GPRS Statistics

The new **clear gprs statistics all** command clears all global and per-APN GPRS statistics cleared by the following commands:

- **clear gprs gtp statistics**
- **clear per-path statistics**

- **clear gprs access-point statistics all**
- **clear gprs service-aware statistics (includes CSG statistics)**
- **clear ggsn quota-server statistics**

Displaying Per-SGSN Statistics

To assist in troubleshooting and diagnostics, the Cisco GGSN tracks various GTP global statistics on a per SGSN-path basis. These data path and control path counters can be displayed using the **show gprs gtp path statistics remote-address** privileged EXEC command.

Additionally, the GGSN can be configured to maintain a *history* for deleted paths. The data path and control path statistics for a deleted path can be displayed using the **show gprs gtp path statistics history** privileged EXEC command. To configure the maximum number of path entries for which you want the GGSN to maintain a history of the statistics, use the **gprs gtp path history** global configuration command.

For detailed information about the counters displayed using the **show gprs gtp path statistics history** command and the **show gprs gtp path statistics** command, refer to the command descriptions in the *Cisco GGSN Command Reference*.

MIB Enhancements for IPv6 PDP Support

To support IPv6 PDPs, the cgprsAccPtSecSrcViolNotif trap, sent when a security violation has occurred, has been enhanced to send the notifications for IPv6 PDPs in addition to IPv4 PDPs.

The IPv6 support requires that the **ipv6 security verify source** access-point configuration command has been configured.

For detailed information about the GGSN SNMP notifications, see Appendix A, "Monitoring Notifications."

Fast Delete PDP Support

To eliminate delays when deleting PDP contexts that occur because the SGSN is not responding to the delete PDP context requests, with Cisco IOS Release 12.4(9)XG2 and later, the GGSN can be configured to delete a PDP context without waiting for a response from the SGSN, or the GGSN can be configured to delete PDP contexts locally without sending a delete PDP context requests to the SGSN at all.

For detailed information about the Fast PDP Delete features, see the "Controlling Sessions on the GGSN" section on page 3-18.

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
  - Auto-retrieval of charging data records (CDRs) from a Cisco Persistent Storage Device (PSD)
- 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, 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), Diameter Credit Control Application (DCCA), Persitent Storage Device (PSD) Client