CHAPTER 1

Overview of GPRS and UMTS

This chapter briefly introduces the 2.5G general packet radio service (GPRS) and the 3G Universal Mobile Telecommunications System (UMTS) technologies, and their implementation in Cisco Gateway GPRS Support Node (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. 2.5G 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). Today, GPRS 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. W-CDMA technology offers higher throughput, real-time services, and end-to-end Quality of Service (QoS). W-CDMA technology also delivers pictures, graphics, video communications, and other multimedia information, and 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)

  Provides mobile cell phone users access to a public data network (PDN) or specified private IP networks.

  The Cisco GGSN is implemented via Cisco IOS software.

- Serving GPRS support node (SGSN)

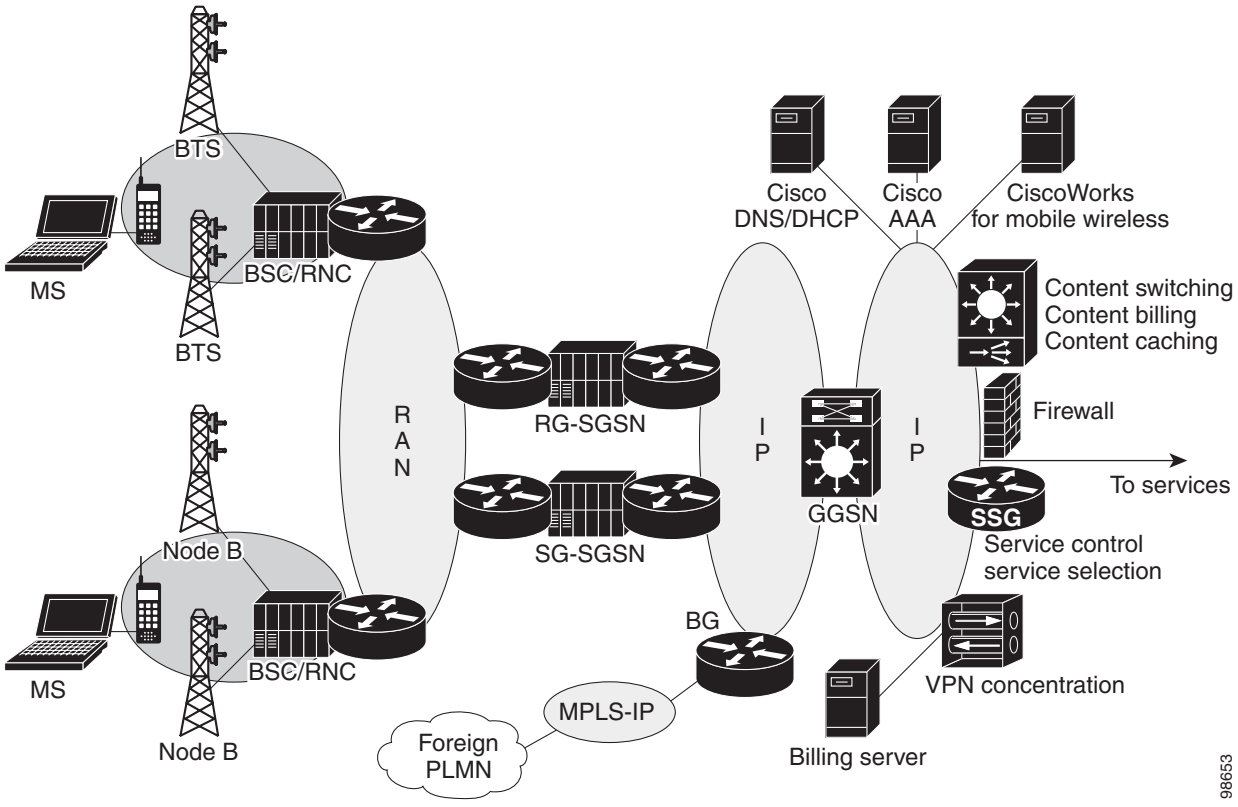
  Connects the radio access network (RAN) to the GPRS/UMTS core. The SGSN:

  - Tunnels user sessions to the GGSN.
  - Sends data to and receives data from mobile stations
  - Maintains information about the location of a mobile station (MS)
  - 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



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 comprises mobile stations that connect to a base transceiver station (BTS). The BTS connects to a base station controller (BSC). In a 3G environment, the RAN is comprises mobile stations that connect to a NodeB. The Node B connects to a radio network controller (RNC).

The RAN connects to the GPRS/UMTS core through an SGSN. The SGSN 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) enables 2.5G applications, and GTP Version 1 (GTPv1) enables 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 IP or Multiprotocol Label Switching (MPLS) networks.

To assign mobile sessions an IP address, the GGSN uses one of the following methods defined on an access point:

- Dynamic Host Configuration Protocol (DHCP)
- Remote Authentication Dial-In User Service (RADIUS) server
- Local address pool configured on the GGSN

The GGSN can use a RADIUS server to authorize and authenticate remote users. DHCP and RADIUS services can be configured at the global level, or for each access point configured on the GGSN.

IPSec encryption is performed on the IPSec Virtual Private Network (VPN) Acceleration Services Module.

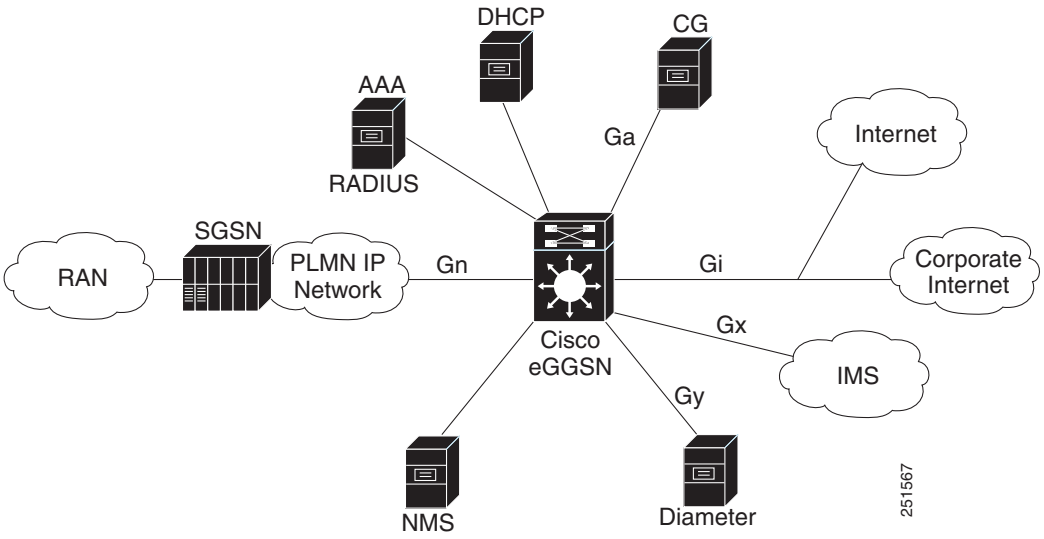
GPRS Interface Reference Model

The 2.5G GPRS and 3G UMTS standards use the term *interface* to 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/Gp interface—Interface between the GGSN and the SGSN. The Gn interface is between two GSNs within the same public land mobile network (PLMN) in a GPRS/UMTS network. The Gp interface is between two GSNs in different PLMNs. GTP is a protocol defined on the Gn/Gp interface.
- Gi interface—Reference point between a GPRS/UMTS network and an external packet data network (PDN).
- Ga interface—Interface between a GGSN and charging gateway (CG) in a GPRS/UMTS network.

Figure 1-2 GGSN Interfaces



Additional interfaces implemented in the Cisco GGSN features, include:

- Gy—Interface to the Diameter server for Diameter Credit Control Application (DCCA) support for enhanced service-aware billing.
- Gx—Reference point between the Policy and Charging Rules Function (PCRF) and the Policy and Charging Enforcement Function (PCEF). The Gx interface is use for provisioning and removal of Policy Charging Control (PCC) rules. The Gx interface uses the Diameter protocol.
- AAA Interface—Interface to AAA server. The AAA interface uses the RADIUS protocol.
- DHCP—DHCP server interface.
- NMS—Network management interface.

Virtual Template Interface

To configure the connections between the GGSN and SGSN, and the GGSN and PDNs, the Cisco GGSN software uses an internal interface called a *virtual template* interface. A virtual template is a logical interface. It is not tied directly to a specific interface, but it can be associated dynamically with an 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 must configure certain GPRS/UMTS-specific elements on the virtual template interface. For example, you must configure GTP encapsulation (necessary for communicating with the SGSN) and the access list the GGSN uses to determine which PDNs are accessible on the network.

Access Point Configuration

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—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 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 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 data rates at are faster than those offered by 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. This access includes 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 256 Mbps
- Supports connection-oriented Radio Access Bearers with specified QoS, enabling end-to-end QoS

Features Introduced in Cisco IOS Release 12.4(22)YE1

Cisco GGSN Release 9.0, Cisco IOS Release 12.4(22)YE1, introduces support for the following features:

- Layer 3 Geographical Redundancy
- Passive Route Suppression

Layer 3 Geographical Redundancy

Cisco GGSN Release 9.0, Cisco IOS Release 12.4(22)YE1 introduces support for Layer 3 geographical GTP session redundancy.

The Cisco GGSN software uses the Cisco IOS Hot Standby Routing Protocol (HSRP), the Cisco IOS Check-point Facility (CF) and Redundancy Framework (RF), and the Stream Control Transmission Protocol (SCTP) to support Layer 2 (L2) local GTP-SR and Layer 3 (L3) geographical GTP-SR (remote redundancy) implementations.

The HSRP provides network redundancy for IP networks, ensuring that user traffic immediately and transparently recovers from first hop failures in network edge devices or access circuits.

In a geographical redundancy implementation (using L3 HSRP), the active and standby Cisco GGSNs are configured on Cisco SAMIs that are connected over a wide area network (WAN). With prior releases of the Cisco GGSN software, connectivity between the active and standby GGSNs was limited to LANs only (L2 HSRP).

Either local redundancy or geographical redundancy can be implemented; however, the implementations are mutually exclusive (a GGSN cannot be configured for both types of redundancy at the same time).

For information on implementing a geographical redundant configuration, see Chapter 5, “Configuring GGSN GTP Session Redundancy.”.

Passive Route Suppression

In a geographical redundancy implementation, only the active GGSN needs to send routing updates. Therefore, when implementing geographical redundancy, you must configure the GGSN interfaces to not send routing updates when the GGSN is in standby mode.

For information on enabling passive route suppression see Chapter 5, “Configuring GGSN GTP Session Redundancy.”

Features Introduced in Cisco IOS Release 12.4(22)YE

Cisco GGSN Release 9.0, Cisco IOS Release 12.4(22)YE, introduces support for the following features:

- Lawful Intercept, page 1-9
- Proxy-CSCF Load Balancing, page 1-9
- Standalone GGSN Prepaid Quota Enforcement, page 1-10

and enhancements to the following existing features:

- Debugging, page 1-10
- DFP Weight, page 1-11
- HSPA QoS Extensions, page 1-11
- MIBs, page 1-12
- Multiple Subnets Behind the Mobile Station, page 1-12
- Statistics, page 1-12

Granular Charging and Storage

The Cisco GGSN supports two levels of charging configurations: global level and access-point level (granular charging).

With granular charging, up to 30 *charging groups* can be configured per GGSN. In each group, a unique primary, secondary, and tertiary charging gateway, and iSCSI target can be defined. The charging group can then be associated with an APN.

Charging groups enable you to send charging records belonging to different APNs to different destinations.

If there is no charging group associated with an APN, the default charging group is used. The default charging group is the charging gateways, iSCSI target, switchover priority, etc., configured at the global level.

Charging group 0 is the default charging group defined at the global level. Charging groups 1 to 29 can be configured and associated with an APN.

For information about configuring granular charging and storage see the "Configuring Granular Charging and Storage" section on page 6-24.

GRX Traffic Segregation

The Cisco GGSN receives traffic from the SGSN on the Gn and Gp interfaces. Gn traffic is from SGSNs within the same PLMN. Gp traffic is from SGSNs within different PLMNs. It is received via GPRS Roaming Exchange (GRX) to the GGSN.

To ensure privacy and security, the Cisco GGSN supports VRFs on the Gn interface. With VRF support on the Gn interface, GRX traffic can be segregated and be part of separate routing tables.

For information about configuring VRFs to segregate GRX traffic on the Gn interface, see the "Segregating GRX Traffic on GGSN Gn Interface" section on page 11-30.

Gx Interface

With Cisco GGSN Release 9.0 and later, APNs can be enabled for Policy Charging Control (PCC).

A PCC-enabled APN (the Gx interface) is a reference point between the PCRF and the PCEF. It is used for provisioning and removal of Policy Charging Control (PCC) files from PCRF to PCEF.

For information about PPC-enabled APNs on the Cisco GGSN, see the "Enabling PPC on an APN" section on page 7-29.

Gy Interface

When configured with the Cisco Content Services Gateway - 2nd Generation (CSG2) application, the Cisco GGSN supports online charging. The Cisco GGSN supports online charging using the Cisco IOS Diameter protocol on a Diameter Credit Control Application (DCCA) interface. The DCCA interface is also called the Gy interface.

In prior releases, the Cisco GGSN supported generic DCCA (as defined in RFC 4006, *Diameter Credit-Control Application)*, and some 3GPP attributes (as defined in 3GPP Technical Specification 32.299, *Telecommunication Management; Charging management; Diameter Charging Applications*.)

With Cisco GGSN Release 9.0 and later, the Gy interface has been enhanced to support the following additional 3GPP functionality:

- Support for the Trigger-type AVP with the following Trigger Types for a prepaid PDP:
  - CHANGE_IN_SGSN_IP_ADDDRESS
  - CHANGE_IN_QOS
  - CHANGE_IN_LOCATION
  - CHANGE_IN_RAT

  3GPP trigger-type AVPs are included in the Multiple-Service-Credit-Control (MSCC) AVP. The MSCC AVP is in the Credit Control Answer (CCA) sent from the DCCA server to the Cisco GGSN functioning. The Cisco GGSN is functioning as the DCCA client.

  A CCA can contain more than one MSCC AVP. When the GGSN receives one of the supported categories, a trigger is enabled for each of the associated categories. Alternatively, these categories can be enabled using Cisco GGSN commands. See the "Configuring Enhanced Service-Aware Billing" chapter of the *Cisco GGSN Configuration Guide* for information.

  The quota granted in an MSCC AVP is associated with a category (that is, a service). Each of the MSCC AVPs can contain 3GPP trigger-type AVPs. These 3GPP trigger-type AVPS specify the events that cause the DCCA client to reauthorize the associated quota.

  Note MSCCs received with unsupported 3GPP trigger types are ignored by the GGSN. When an unsupported trigger type is received, the previously installed triggers are applied.

- Support for following reauthorization thresholds:
  - Time-Quota-Threshold
  - Volume-Quota-Threshold
  - Time-Quota-Mechanism

  Optionally, the DCCA server can send CCAs with an MSCC AVP that contains the above 3GPP AVPs. These AVPs tell the GGSN to request reauthorization when the remaining quota is reached.

Note The Time-Quota-Mechanism is not fully supported in Cisco GGSN Release 9.0.

For more information, see the "Enabling Support for Vendor-Specific AVPs in DCCA Messages" section on page 7-22.

The following commands have been modified to support the enhancements to the Cisco GGSN Gy interface:

- **content postpaid**
- **gprs charging service-record include**
- **gprs dcca**
- **trigger**

Lawful Intercept

Lawful intercept enables a Law Enforcement Agency (LEA) to perform electronic surveillance on an individual as authorized by a judicial or administrative order. To facilitate the lawful intercept process, certain legislation and regulations require service providers (SPs) and Internet service providers (ISPs) to implement their networks to explicitly support authorized electronic surveillance.

With Cisco GGSN Release 9.0 and later, you can implement Lawful Intercept support on the Cisco GGSN. For more information about Lawful Intercept support on the Cisco GGSN, see the "Implementing Lawful Intercept Support on the Cisco GGSN" section on page 11-35.

Proxy-CSCF Load Balancing

The Cisco GGSN supports Proxy Call Session Control Function (P-CSCF) load balancing.

When P-CSCF load balancing is enabled, the Cisco GGSN uses a round-robin algorithm to select the Proxy-CSCF server it sends in a Create PDP response. The Proxy-CSCF server is sent when the P-CSCF address request field in the protocol configuration option (PCO) IE is included in the Create PDP Context request.

When P-CSCF load balancing is not enabled, the Cisco GGSN sends an entire list of preconfigured P-CSCF servers.

For information about enabling Proxy-CSCF load balancing, see the "Configuring Proxy-CSCF Discovery Support on an APN" section on page 8-47.

Standalone GGSN Prepaid Quota Enforcement

The Cisco GGSN supports two types of prepaid quota enforcement.

Prepaid quota enforcement can be provided by an eGGSN configuration (Cisco GGSN configured with the Cisco CSG2) or provided by a Cisco GGSN operating in standalone mode.

When a Cisco GGSN in standalone mode provides prepaid quota enforcement, the GGSN monitors the data packets on a volume basis, time basis, or both for prepaid users.

For information about configuring Standalone GGSN Prepaid Quota Enforcement, see the "Configuring Standalone GGSN Prepaid Quota Enforcement" section on page 7-28.

Enhancements

The following features have been enhanced in Cisco GGSN Release 9.0:

Debugging

With Cisco Release 9.0, you can perform the following debugging actions:

- Control the verbosity level of debug commands using the **debug gprs verbose** privileged EXEC command.
- Set next-call conditional debugging for a GGSN using the **debug condition** privileged EXEC command with the **next-call** keyword option specified.

  Up to 5 next-call conditional debugs settings, or PDPs with next-call debug conditions can be set at any given time.

  To monitor and manage the next-call conditional debugging, use the following commands:

  - **show debugging condition** command to display existing debug next-call conditions or PDPs with next-call debug conditions
  - **clear gprs gtp debug next-call** command to clear debugs set for existing PDPs
  - **no debug condition** command with the **next-call** keyword specified to remove a next-call debug condition

DFP Weight

Cisco GGSN Dynamic Feedback Protocol (DFP) support has been enhanced. With Cisco GGSN Release 9.0, CPU load and memory load are included as factors for calculating weights for DFP.

In GTP load balancing, the Cisco IOS SLB is defined as a DFP manager, and a DFP agent is defined on each GGSN in the server farm. The DFP agent reports the weights of the GGSNs. The DFP agents calculate the weight of each GGSN, based on CPU utilization, processor memory, and the maximum PDP contexts that can be activated for each GGSN.

The GGSN weight is based primarily on the ratio of the GGSNs existing PDP contexts to the maximum number of PDP contexts allowed.

By default, the CPU and memory utilization become part of the DFP weight calculation only after the utilization exceeds 85%. With Cisco GGSN Release 9.0, the percentage of utilization at which the CPU and memory loads are included in the weight calculation can be configured. To customize the percentage, use the **gprs dfp** global configuration command's **cpu-load** and **mem-load** keyword options.

The **gprs dfp** command has been modified to support the DFP weight enhancements.

For information about configuring the weight for DFP, see the "Configuring DFP Support on the GGSN" section on page 13-20.

HSPA QoS Extensions

Together, High-Speed Uplink Packet Access (HSUPA) and High-Speed Downlink Packet Access (HSDPA) are known as High-Speed Packet Access (HSPA).

HSPA is a packet-based data service in W-CDMA extends and improves the performance of existing protocols by

- Supporting data transmissions of up to 8-256 Mbps over a 5MHz bandwidth
- Enabling mobile devices to transmit and receive large amounts of data from the PDN, such as video clips
- Supporting data-intensive services such as video conferencing

The Cisco GGSN receives QoS information in service requests sent to the network by an MS. The QoS information determines the type of service the MS is requesting. Based on the current operating conditions, the GGSN returns a negotiated QoS. The negotiated QoS determines the actual quality of service the user experiences.

Note HSPA is supported only for GTPv1 PDP contexts.

For information about configuring a CAC Maximum QoS policy, see "Configuring a CAC Maximum QoS Policy" section on page 10-13.

The following Cisco GGSN CAC maximum QoS policy configuration commands have been modified to support higher values for HSPA:

- **gbr traffic-class**
- **mbr traffic-class**

MIBs

Cisco GGSN Release 9.0 and later supports the CISCO-ISCSI MIB.

Multiple Subnets Behind the Mobile Station

In prior releases of the Cisco GGSN software, the Routing Behind the Mobile Station feature supported the configuration of only one subnet behind the MS. If the Framed-Route (attribute 22) contained multiple routes, the GGSN used the first route, and ignored all subsequent routes.

With Cisco GGSN Release 9.0 and later, the Cisco GGSN supports the configuration of up to 16 subnets per MS.

For more information about configuring multiple subnets behind the MS, see "Configuring Routing Behind the Mobile Station on an APN" section on page 8-44.

Statistics

Cisco GGSN Release 9.0 introduces support for the following statistics enhancements:

- **GPRS Throughput**

  To configure the number of history items to maintain for throughput statistics collected during the two intervals configured using the **gprs throughput intervals** global configuration command, use the **gprs throughput history** command in global configuration mode.

  To display the latest throughput statistics, use the **show gprs throughput history** privileged EXEC command. To display a history of throughput statistics, use the **show gprs throughput history** privileged EXEC command.

- **Call Setup Rate**

  To configure the interval at which call rate statistics are collected for APNs, use the **gprs callrate interval** command in global configuration mode. To configure the number of history items to maintain for call rate statistics collected during the configured interval, use the **gprs callrate history** command in global configuration mode.

  To display the latest call rate statistics, use the **show gprs callrate** privileged EXEC command. To display a history of call rate statistics, use the **show gprs callrate history** command.

Features Introduced in Prior Releases

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
- VPN routing and forwarding (VRF) per APN
- Multiple APNs per VRF instance
- 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
- GGSN-Initiated Update PDP Context Requests
- P-CSCF Discovery
- Enhanced MIBs for:
  - Cisco Content Services Gateway (CSG)
  - Diameter Credit Control Application (DCCA)
  - APN-level Periodic Accounting Timer
  - PPP-Regeneration Scalability

  - Direct tunnels
  - Change of Authorization
  - GGSN-initiated Update PDP Contexts

- RADIUS Change of Authorization Message

  The RADIUS Change of Authorization (CoA) message contains information for dynamically changing session authorizations. The CoA message is received on port 1700.

  The Cisco GGSN uses the base Cisco IOS AAA to support the RADIUS CoA message, as defined by RFC 3576. In addition, the Cisco GGSN also utilizes an additional 3GPP QoS attribute that indicates the updated QoS, and the Acct-Session-ID that identifies 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). The Accounting-session-id is a string that uses the standard attribute type 44.

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

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

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

- Downloadable QoS Profile

  The Cisco GGSN supports QoS profiles to be downloaded from an AAA server.

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

  In the access-accept from RADIUS, user-specific attributes such as session and idle timeout values can be downloaded and applied to the PDP context. In addition, the QoS profile can be downloaded via the QoS VSA (as defined by 3GPP TS 24.0008). If a 3GPP QoS profile attribute is received in an access-accept from an AAA server, 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, it 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.

- PPP-Regeneration Scalability—The Cisco GGSN permits PDPs regenerated to a PPP session to run on software interface description blocks (IDBs). Permitting PPP sessions to run on software IDBs, increases the maximum number of supported sessions.

- Anonymous User Access for PPP-Regeneration

  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 cannot send a name and password.

  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, the anonymous user configuration under that APN is sent to the LNS for authentication. 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.

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.

  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:

```
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

  The direct tunnel feature 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. It handles both signaling traffic (to keep track of the location of mobile devices), and the actual data packets being exchanged between a mobile device and the Internet.

  Before Cisco GGSN Release 8.0, a tunnel could only exist between the GGSN and SGSN, and between the SGSN and RNC. With this tunnel configuration, all data packets must pass through the SGSN. The SGSN 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 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 tunnel processing is as follows:

  a. 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

     - GGSN updates the RNC user traffic address and Data TEID. The GGSN uses the updated information when sending G-PDUs for the MS.

b. If the GGSN receives an Error Indication message from the RNC user traffic address, it initiates an Update PDP Context request. The Update PDP Context request includes the Direct Tunnel Flags IE with the Error Indication bit set.

c. Until the Update PDP Context response is received from the SGSN, the GGSN drops subsequent packets to the MS address.

d. 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. In addition, direct tunnel support does not apply to when the SGSN is asked by a prepaid system to count the traffic flow.